CONTRIBUŢII LA ÎMBUNĂTĂŢIREA CALITĂŢII TRANSMISIEI VOCII ÎN REŢELELE FĂRĂ FIR BAZATE PE STANDARDUL IEEE 802.11

Teză destinată obţinerii
titlului ştiinţific de doctor inginer
la
Universitatea „Politehnica” din Timişoara
în domeniul INGINERIE ELECTRONICĂ ŞI TELECOMNICAŢII
de către

...Ing. Mirela-Laura Ioaneşiu

Conducător ştiinţific:	Prof.dr.ing.Corneliu I. Toma
Referenţi ştiinţifici:	Prof.dr. ing.Mircea Petrescu
	Prof.dr.ing. Gavril Toderean
	Prof.dr.ing. Miranda Monica Naforniţă

Ziua susţinerii tezei: 03.12.2010.....

Seriile Teze de doctorat ale UPT sunt:

1. Automatică
2. Chimie
3. Energetică
4. Ingineria Chimică
5. Inginerie Civilă
6. Inginerie Electrică
7. Inginerie Electronică şi Telecomunicaţii
8. Inginerie Industrială
9. Inginerie Mecanică
10. Ştiinţa Calculatoarelor
11. Ştiinţa şi Ingineria Materialelor

Universitatea „Politehnica" din Timişoara a iniţiat seriile de mai sus în scopul diseminării expertizei, cunoştinţelor şi rezultatelor cercetărilor întreprinse în cadrul şcolii doctorale a universităţii. Seriile conţin, potrivit H.B.Ex.S Nr. 14 / 14.07.2006, tezele de doctorat susţinute în universitate începând cu 1 octombrie 2006.

România, 300159 Timişoara, Bd. Republicii 9,
tel. 0256 403823, fax. 0256 403221
e-mail: editura@edipol.upt.ro

Cuvânt înainte

Teza de doctorat a fost elaborată pe parcursul activităţii mele în cadrul Departamentului de Comunicaţii al Universităţii „Politehnica” din Timişoara.

Lucrarea abordează o parte din condiţiile care trebuie să fie îndeplinite pentru asigurarea calităţii transmisiei vocii prin reţelele fără fir, bazate pe standardul IEEE 802.11. Au fost abordate probleme de securitate, reducere a timpilor de întârziere în iniţializarea sesiunii de apel vocal, a ratei de eroare, a jitter-ului. De asemenea a fost abordată sub forma unor cercetări şi transmiterea de mesaje către mai mulţi utilizatori cu mai multe salturi.

Teza îşi propune să demonstreze că un pachet criptografic OpenSource puternic, de uz general, cum este Cryptlib, modificat cu algoritmul de criptare propus de doctorand, asigură securitatea informaţiilor vocale într-un mod facil, fără a mai fi nevoie de scrierea a sute sau chiar mii de linii de cod care să facă acelaşi lucru.

Scopul utilizării lui îl constituie posibilitatea unei optimizări foarte bune, funcţie de cerinţele sistemelor VoIP şi utilizarea avantajelor oferite de protocolul IAX (Inter-Asterisc eXchange) faţă de H.323 şi SIP pentru traficul de voce. De asemenea se asigură şi folosirea eficientă a lăţimii de bandă atât pentru sistemele de semnalizare cât şi pentru transferuri mass-media.

Cercetările efectuate au condus la realizarea unei aplicaţii cu operare în timp real care are capacitatea de a partaja un singur număr de port şi de a transfera toate datele printr-un port UDP cunoscut, cu asigurarea normelor de securitate ale acestora.

În vederea reducerii timpului aferent iniţializării unei sesiuni VoIP prin protocolul SIP, am propus un contor de timp adaptiv care este reglabil la dimensiunea pachetelor de semnalizare implicate în stabilirea unei sesiuni de apel vocal şi un algoritm pentru controlul apelurilor din lista de apeluri.

În încheiere doresc să aduc mulţumiri deosebite conducătorului de doctorat prof.dr.ing. Corneliu I.Toma şi doamnei Prof.dr.ing. Miranda Monica Naforniţă care prin supraveghere constantă şi sfaturi nepreţuite au contribuit la realizarea prezentei lucrări.

Timişoara, Mirela-Laura Ioaneşiu

Destinatarii dedicaţiei.

Ioaneşiu Mirela-Laura

Contribuţii la îmbunătăţirea calităţii transmisiei vocii în reţelele fără fir bazate pe standardul IEEE 802.11

Teze de doctorat ale UPT, Seria X, Nr. YY, Editura Politehnica, 2010, 158 pagini, 53 figuri, 15 tabele.

ISSN:uuuu-vvvv

ISBN (10): ……..; ISBN (13): ……

Cuvinte cheie:
Internet, VoIP, reţele IP, PBX, firewall, patch, puncte de acces, standardul IEEE 802.11, reţele fără fir

Rezumat:
Teza de doctorat este dedicată unei probleme de mare interes în transmiterea vocii prin Internet (VoIP). Calitatea transmisiei în reţelele fără fir bazate pe standardul IEEE 802.11 impune respectarea unor factori cum ar fi securitatea, reducerea timpului de iniţializare a sesiunii, a ratei erorilor, jitter-ului, a mecanismelor de retransmitere. Într-o lume a sistemelor de transmisie a vocii prin INTERNET, centralele clasice de abonat, Private Branch Exchanges (PBX) sunt înlocuite de IP PBX bazate pe servere ce rulează pe sistemele de operare Microsoft, Linux sau unul care este propriu producătorului. Astfel de sisteme de management al apelurilor folosite atât pentru a deservi serviciile VoIP cât şi pentru administrarea apelurilor sunt expuse atacurilor viruşilor şi hackerilor. În lucrarea de doctorat s-au evidenţiat breşele din mecanismele de securitate generate de punctele de acces (AP) ale reţelelor fără fir bazate pe standardul IEEE 802.11. Teza propune un soft pentru securitatea şi mobilitatea aplicaţiilor VoIP care are la bază un sistem propriu de criptare pentru iniţializarea şi securitatea protocolului IAX în reţelele fără fir. Performanţele softului bazat pe algoritmul de criptare implementat au fost evaluate prin experimente efectuate comparativ cu algoritmii utilizaţi în prezent. Pe baza rezultatelor experimentale s-a demonstrat eficacitatea acestuia în contextul securităţii transmisiilor VoIP.

În vederea reducerii timpului aferent iniţializării unei sesiuni VoIP prin protocolul SIP, am propus un contor adaptiv pentru retransmisie care este reglabil la dimensiunea pachetelor de semnalizare implicate în stabilirea unei sesiuni de apel vocal şi un algoritm pentru controlul apelurilor din lista interogare şi invitare la emisie.

De asemenea, în teză au fost abordate, sub forma unui studiu şi întărzierile survenite la distribuţia mesajelor către mai mulţi utilizatori prin staţii intermediare. Concluzia este ca numărul maxim de staţii pe care le poate parcurge un apel vocal este 4, după care acesta nu mai poate fi recuperat.

CUPRINS

LISTĂ DE TABELE

LISTĂ DE FIGURI

LISTĂ ABREVIERI

183-Session progress message
200 OK-Final confirmation messages in SIP transactions
AAA-Authentication, Authorization, Accounting
ACK-Acknowledgement Response in SIP transactions
ACL Access Control List
AES-Advanced Encryption Standard
AP-Access Point
ARQ-Automatic Repeat Request
ATM-Asynchronous Transfer Mode
BSA-Basic Service Area
CBC-Cipher Block Chaining
CBR-Constant Bit Rate
CC-CSRC-Count CSRC
CFB-Cipher Feedback
CFP-Contention Free Period
CP-Contention Period
CSCF-Call Session Control Function
CSCR-Contributing source ID
CSMA/CA-Carrier Sense Multiple Access with Collision Detection
CTI- Complete Timing Information
CW-Contention Window
DCF-Distributed Coordination Function
DES-Data Encryption Standard
DHCP-Dynamic Host Configuration Protocol
DIFS-Distributed coordination function Inter-Frame Space
EAP-Extensible Authentication Protocol
EAPoW-Extensible Authentication Protocol over Wireless
ECC-Error Correcting Codes
FEC-Forward Error Correction
FER-Frame Error Rate
IAX-Inter-Asterisk eXchange
I-CSCF-Interrogating Call Session Control Function
IDEA-International Data Encryption Algorithm
IFS-Inter-Frame Space
IP PBX- IP Private Branch eXchange
IP-IMS Multimedia Sub-Systems
ISAKMP–Internet Security Association and Key Management Protocol
LAN-Rețea locală
MAC-Media Access Control
MD5-Message-Digest Algorithm 5
MIB-Management Information Base
MIMO-Multiple Input Multiple Output-
MSDU-MAC Service Data Unit
MWM-Maximum Weighted Matching
NAK-Not Acknowledgment
NAT-Network Address Translation
NTI-Null Timing Information

PCF-Point Coordination Function
PCM-Pulse Code Modulation
P-CSCF-Proxy Call Session Control Function
PHY-Physical Layer
PHY-Physical Layer
PIFS-Point coordination function IFS
PKI-Public Key Infrastructure
PRACK-Provisional Response Acknowledgment
RADIUS-Remote Authentication Dial In User Service
RAT-Reverse Address Translation
RC4-Rivest Cipher 4
RLP-Radio Link Protocol
RTCP-Real Time Control Protocol
RTP-Real Time Transport Protocol
RTT-Round Trip Time
S-CSCF-Serving Call Session Control Function
SDES-Session Description Protocol Security
SDP-183 Session Description Protocol
SDP-Session Description Protocol
SIFS-Short Inter-Frame Space
SIP-Session Initiation Protocol
SSID-Service Set Identifiers
SSL-Secure Sockets Layer
SSRC-Synchronization source identifier
TCP-Transmission Control Protocol
TLS-Transport Layer Security
TLS-Transport Layer Security
UAC-User Agent Client
UAS-User Agent Server
UDP-User Datagram Protocol
VBR-Variable Bit Rate
VoIP-Voice over IP
WEP-Wired Equivalent Privacy
WLAN-Wireless Local Area Network
WLAN-Wireless Local Area Network
WPA-Wi-Fi Protected Access
ZRTP-Zimmermann Real Time Protocol
FHSS-Frequency Hopping Spread Spectrum
DSSS-Direct Sequence Spread Spectrum
IR-Infra Red-
Mickey-Multimedia Internet KEYing
IBSS-Independent Basic Service Set
BSS- Basic Service Set

1. MOTIVAŢIE

Capitolul introductiv al tezei face o prezentare a problemelor legate de asigurarea calităţii transmisiei în reţelele fără fir, cu accent pe probleme de securitate, iniţializare apeluri şi distribuţie multiplă. Din punct de vedere al securităţii reţelele fără fir sunt relativ mai puţin sigure decât cele cablate. Persoanele neautorizate, aflate în zonele de acoperire ale punctelor de acces pot profita de această structură de reţea şi le pot accesa fraudulos. Reţelele fără fir au prevăzute, încă de la implementare, diferite bariere care formează aşa numita securitate de bază şi care împiedică accesul neautorizat în reţea. Pentru persoane rău intenţionate, cu bună pregătire în domeniu, de tipul hackerilor, securitatea acestor reţele, ca de altfel şi a altora, este discutabilă.

1.1. Consideraţii generale privind securitatea VoIP în reţelele fără fir

O reţea de calculatoare este o structură deschisă la care se pot conecta diferite tipuri de echipamente. Acest lucru conduce la o lărgire necontrolată a cercului utilizatorilor cu acces la resursele reţelei. Vulnerabilitatea reţelelor se manifestă pe două planuri:

- posibilitatea modificării sau distrugerii informaţiei, adică atacul la integritatea ei fizică;
- posibilitatea folosirii neautorizate a informaţiilor, adică scurgerea lor din cercul de utilizatori stabilit.

Trebuie avute în vedere, cu prioritate, două aspecte legate de securitate:

- integritatea resurselor unei reţele, adică disponibilitatea lor indiferent de defectele de funcţionare, hard sau soft, de încercările ilegale de sustragere a informaţiilor precum şi de încercările de modificare a informaţiilor;
- caracterul privat, adică dreptul individual de a controla sau influenţa o informaţie referitoare la o persoană, poate fi memorată în fişiere sau baze de date şi cine are acces la aceste date.

O reţea sigură este aceea în ale cărei componente (resurse şi operaţii) se poate avea încredere, adică furnizează servicii de calitate şi corecte. Deoarece o reţea este alcătuită din componente diferite ea reprezintă o zonă convenabilă pentru diferite atacuri sau operaţii ilegale, lucru care conduce la concluzia că protecţia a devenit unul din aspectele operaţionale vitale ale unei reţele.

Securitatea şi în special caracterul privat trebuie să constituie obiectul unei analize atente în cazul reţelelor. Reţelele sunt ansambluri complexe de calculatoare. Este foarte dificil să se obţină o schemă completă a tuturor entităţilor şi operaţiilor existente la un moment dat, astfel încât reţelele sunt vulnerabile la diferite tipuri de atacuri sau abuzuri. Complexitatea este generată de dispersarea geografică naţională şi internaţională a componentelor (nodurilor) reţelei, implicarea mai multor organizaţii în administrarea unei singure reţele, existenţa unor tipuri diferite de calculatoare şi sisteme de operare, existenţa unui număr mare de entităţi. Fără o reţea de calculatoare bine concepută şi protejată nici o firmă nu îşi poate desfăşura activitatea.

De funcţionarea lor corectă depinde activitatea guvernamentală, comercială, industrială şi chiar personală. Pe măsură ce calculatoarele personale pot fi conectate de acasă în reţele, o serie de activităţi pot fi făcute de persoane particulare. Trebuie avute în vedere tipurile de date pe care persoanele le pot citi, care sunt celelalte persoane cu care pot comunica, la ce programe au acces. Tot mai multe informaţii memorate în fişiere devin posibil de accesat prin intermediul reţelelor. Această asociere de fişiere privind persoanele poate avea consecinţe nefaste asupra caracterului privat individual. Informaţia este vulnerabilă în faţa unui atac în orice punct al unei reţele, de la introducerea ei până la destinaţia finală. În particular, informaţia este mai susceptibilă la atac atunci când trece prin liniile de comunicaţii.

Telefonia VoIP sau telefonia IP este transportul vocii prin Internet cu ajutorul protocolului IP (Internet Protocol). Internet-ul este o interconectare între reţelele care folosesc acest protocol. Pe parcursul anilor Internet-ul a devenit o bază pentru aplicaţii şi servicii, fapt ce nu a fost luat în calcul de la început. Astfel s-a dezvoltat o piaţă cu un mare potenţial pentru servicii, în special pentru telefonia IP. Aceasta se datorează următoarelor trei cauze:

1. telefonia este o afacere cu câştiguri mari şi cu mulţi clienţi;
2. tot mai mulţi oameni utilizează Internet-ul zilnic;
3. Internet-ul, datorită flexibilităţii, dezvoltării rapide şi deschiderii sale, generează tot mai multe servicii noi.

O cerinţă majoră a Internet-ului este asigurarea securităţii sale. O mulţime de incidente de securitate s-au petrecut în ultimii ani şi numărul lor este în creştere. Ca atare securitatea este o temă esenţială pentru sistemele de telefonie VoIP.

Fig.1.1 descrie arhitectura unui sistem VoIP. Componentele implicate sunt: punctele finale (endpoints-EP), dispozitivele care asigură interfaţa între punctele finale şi reţea numite porţi (GK) şi serviciile finale (back-end-services-urile-BES), adică o suită de programe, interfeţe şi servicii care asigură comunicaţia cu sistemul pe care acesta este implementat. Punctele finale sunt echipamente care permit utilizatorilor sistemului să se apeleze între ei. Porţile administrează punctele şi serviciile finale, memorează informaţiile importante care permit unei porţi să conecteze cele 2 părţi una cu alta. Protocolul utilizat este SIP (protocol pentru iniţializarea sesiunii), un standard pentru telefonia IP [66].

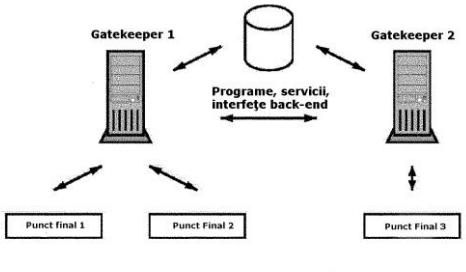


Fig.1.1. Arhitectura sistemului VoIP [65]

1.2. Structura unei reţele

Reţelele de calculatoare sunt nişte construcţii foarte complexe. Conectivitatea calculatoarelor necesită un software complicat. Programele care doresc să acceseze

funcţiile reţelei fac aceasta printr-o interfaţă. Arhitectura reţelei este structurată pe niveluri (layere). Fiecare nivel reprezintă un aspect diferit al sistemului. Comunicaţia cu alte niveluri se face prin interfeţe [66], [69].

Nivelul aplicaţie
Nivelul prezentare
Nivelul sesiune
Nivelul transport
Nivelul reţea
Nivelul legăturii de date
Nivelul fizic

Fig.1.2. Modelul de reţea OSI [69]

Fig.1.2 descrie modelul OSI al unei reţele. Nivelul cel mai de jos este cel fizic. Este baza pentru reţelele de calculatoare. Tot ce se conectează la hardware aparţine acestui nivel. Următorul nivel asigură conectivitatea între gazde. La acest nivel sunt implementate protocoalele de comunicaţie şi modul de trimitere a datelor între două calculatoare. Asigură o interfaţă de acces la servicii şi utilizează nivelul fizic pentru operaţii. Comunicaţia între două aplicaţii, aflate pe gazde diferite, necesită un anumit tip de canal între procesele aplicaţiilor. Această funcţionalitate este asigurată de un alt nivel, care utilizează conexiunea dintre gazde şi oferă funcţiile sale aplicaţiilor aflate pe nivelul superior al acestei arhitecturi.

Sunt stabilite două modele pentru arhitectura reţelelor de calculatoare. Modelul standard pentru protocoalele de reţea şi aplicaţiile distribuite este cel definit de OSI. Internet-ul utilizează însă suita de protocoale TCP/IP, un model în care avem doar 4 niveluri în loc de 7 [13], [15], [18].

1.2.1. Modelul TCP/IP

Modelul TCP/IP este modelul de arhitectură de reţea pentru Internet şi este ilustrat de Fig.1.3. Straturile sale nu sunt atât de strict delimitate ca în modelul OSI. Aplicaţiile pot însă accesa serviciile fiecărui nivel. Cel mai de jos nivel este cel al legăturii de date şi conţine mai multe protocoale de reţea. O comparaţie cu modelul OSI arată că funcţionalitatea nivelului reţea în modelul TCP/IP corespunde cu nivelul fizic şi cel al legăturii de date. El descrie necesarul de hardware şi software atât pentru reţea cât şi pentru adaptoarele de reţea, împreună cu driverele aferente. Nivelul doi cuprinde protocolul IP. El corespunde nivelului de reţea al modelului OSI. Funcţia lui este de a asigura o reţea transparentă cu o singură interfaţă, subreţelele pot avea însă tehnologii şi protocoale diferite. Al treilea nivel al modelului TCP/IP este echivalent nivelului patru din modelul OSI. Sunt două protocoale diferite care formează acest strat: Protocolul Datagramelor Utilizatorilor (UDP-User Datagram Protocol) şi Protocolul de Control al Transmisiei (TCP-Transmission Control Protocol). Ele furnizează alternativ canale logice aplicaţiilor. Protocolul de Control al Transmisiei oferă o conexiune sigură, spre deosebire de Protocolul Datagramelor Utilizatorilor unde serviciul de datagramă nu e sigur. Octeţii trimişi printr-un flux TCP ajung la celălalt capăt în ordinea în care au fost trimişi. Aplicaţia nu trebuie să urmărească pachetele pierdute. Serviciul datagramă trimite datagrame (mesaje individuale) fără a garanta recepţionarea lor. Ultimul strat este cel al aplicaţiei şi conţine modurile de funcţionare ale acesteia [18].

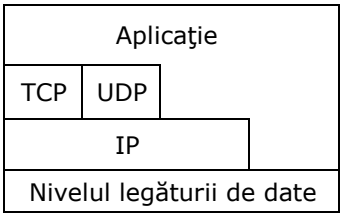


Fig.1.3. Modelul de arhitectură TCP/IP [18]

1.2.2. Încapsularea cadrelor

Încapsularea descrie procesul de construcţie al cadrului care este trimis prin reţea înainte ca o aplicaţie să transmită date. Sunt necesare informaţii suplimentare pentru trimiterea datelor unei aplicaţii altei gazde. Pentru a explica încapsularea se presupune că aceasta se află pe nivelul transport al suitei TCP/IP şi utilizează protocolul de transport TCP. Cadrul de pe nivelul legăturii de date este un cadru Ethernet. În Fig.1.4 se poate vedea un astfel de cadru încapsulat. După cum s-a menţionat în secţiunea anterioară aplicaţia poate să sară peste nivelul transport şi să acceseze direct serviciile oferite de nivelul legăturii de date.

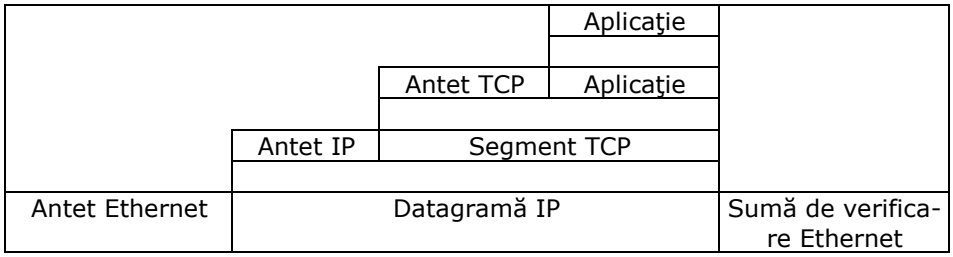


Fig.1.4. Date utilizator încapsulate într-un cadru Ethernet [17]

Datele trimise de aplicaţie trebuie să traverseze stiva de protocoale strat cu strat până la nivelul transport unde există o conexiune TCP. Nivelul transport adaugă la informaţia utilă, antetul TCP şi transmite mai departe nivelului IP. IP adaugă propriul antet la segmentul TCP pentru a forma datagrama IP şi îl transmite mai departe nivelului legăturii de date. Protocolul nivelului legăturii de date (aici Ethernet) construieşte cadrul final şi îl trimite la destinaţie [11], [17], [18].

1.2.3. Protocolul Internet

Protocolul principal din suita de protocoale TCP/IP este protocolul Internet (IP) [68]. IP este proiectat să fie utilizat în interconectarea reţelelor de calculatoare. Asigură un serviciu nesigur de livrare a pachetelor gazdă-la-gazdă. Termenul nesigur înseamnă că nu sunt garanţii că datagrama IP ajunge la destinaţie în ordinea corectă. Cele două caracteristici ale IP sunt adresarea şi fragmentarea. Informaţia necesară pentru a asigura un astfel de serviciu este memorată în antetul IP al datagramei. Fig.1.5 arată structura antetului IP. Mai multe detalii se pot găsi în [17], [69].

Versiune	Lungime	Tip de serviciu (ToS)	Lungimea totală	
Identificator			Steag	Deplasamentul fragmentului
Timp de viaţă (TTL)		Protocol	Suma de control a antetului	
Adresa IP sursa				
Adresa IP destinaţie				
Opţiuni (dacă sunt)				

Fig.1.5. Antetul IP [65]

Dezvoltarea rapidă a reţelei Internet a condus la necesitatea reorganizării sistemului de adrese IP. Cei 32 biţi rezervaţi pentru adrese ai standardului IPv4 s-au dovedit insuficienţi pentru asigurarea cererii de adrese alocate, în special pentru utilizatorii mobili. După numai 3 ani de la stabilirea direcţiilor prioritare în care trebuia acţionat, a apărut IPv6, versiunea "next generation" a standardului pentru IP. Principalele inovaţii de care beneficiază pachetul de protocoale IPv6 sunt [66], [78]:

- extinderea spaţiului alocat pentru adrese;
- posibilitatea de autoconfigurare a unei gazde (host) TCP/IP într-o adresă IP;
- suport pentru multimedia şi aplicaţii în timp real;
- creşterea gradului de securizare a datelor.

Prin extinderea dimensiunii adreselor cu un factor de ordinul 4, de la 32 la 128 biţi, se oferă un număr imens de adrese disponibile. În acelaşi timp, creşterea spaţiului de adrese conduce, în mod firesc, la implementarea unor proceduri de autoconfigurare. Structura de adrese de la IPv4 prevede o migrare uşoară şi gradată către reţelele bazate pe standardul IPv6. Într-o primă etapă se prevede transmisia datelor pe vechea infrastructură, prin încapsularea în pachete compatibile IPv4, între router-ele deja existente în reţea. Pe măsura dezvoltării tehnologice, noile routere IPv6 le vor înlocui pe cele din infrastructura actuală.

Noul protocol IPsec, poate asigura la ora actuală standardele de securitate pentru reţelele IPv6. Pachetul de protocoale IPv6 poate beneficia astfel de noi tehnologii de securizare a datelor, precum autentificarea, criptarea şi asigurarea integrităţii datelor care, aplicate la nivel de miez (kernel), pot asigura securitatea întregului sistem, a aplicaţiilor care rulează în cadrul acestuia şi a pachetelor de date transmise.

1.2.4. Protocolul UDP

Protocolul UDP se găseşte la nivelul transport şi utilizează IP ca protocol de nivel reţea [10], [16],[26], [66]. După cum s-a menţionat anterior protocolul IP utilizează adrese IP pentru a identifica gazdele. Presupunând că pe un anumit calculator rulează şapte aplicaţii, întrebarea este de unde va şti protocolul de transport cărei aplicaţii îi corespund pachetele. Răspunsul este numărul portului. Numărul portului este utilizat pentru a identifica diferitele aplicaţii ale server-ului de pe un calculator gazdă. Portul identifică sursa de la care datele sunt trimise şi destinaţia lor (Fig.1.6). Numele acestor porturi sunt port sursă şi port destinaţie.

Port sursă	Port destinaţie

Lungime	Suma de control

Fig.1.6. Structura unui antet UDP [17]

UDP este un serviciu datagramă orientat. Fiecare operaţie de ieşire produce o datagramă care este trimisă prin reţea. Ca şi IP, UDP nu este un serviciu sigur.

1.2.5. Protocolul TCP

TCP (Transmission Control Protocol) este al doilea protocol al nivelului transport din suita de protocoale TCP/IP [17], [69]. Asigură un serviciu full duplex nivelului aplicaţie, ceea ce înseamnă că datele se pot transmite simultan în ambele direcţii. Datele sunt trimise sub forma unui flux care va ajunge la destinaţie octet cu octet, în ordinea corectă. După cum se ştie IP nu garantează nici livrarea pachetelor, dar nici recepţionarea lor în ordinea corectă. De aceea TCP are propriul mecanism care asigură acest lucru. Fiecare pachet TCP este echipat cu o secvenţă numerică care permite recunoaşterea pachetelor lipsă, a pachetelor recepţionate în ordine greşită sau a duplicatelor. TCP împarte pachetele de date care urmează a fi trimise în segmente. Pentru fiecare segment recepţionat este trimis la expeditor un mesaj de confirmare a recepţiei pachetului. Dacă pachetul nu ajunge într-un anumit interval de timp (expeditorul nu primeşte mesajul de confirmare) atunci acesta este retransmis. Dacă pachetele nu ajung în ordinea corectă, ele pot fi reasamblate de către receptor pe baza numărului de secvenţă din fiecare pachet TCP. Tehnica care asigură o transmisie sigură este numită fereastră glisantă. O versiune simplificată este prezentată în Fig.1.7.

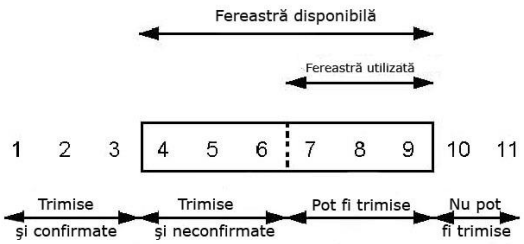


Fig.1.7. Vizualizare fereastră glisantă [16]

Emiţătorul menţine într-un buffer datele care au fost trimise dar nu a primit confirmarea de la receptor. Receptorul are un buffer pentru datele pe care le-a recepţionat. Datele citite sunt şterse din buffer. Pentru receptor nu are nici o importanţă dacă datele sosesc în ordine. Receptorul comunică emiţătorului câte date mai poate memora printr-un număr numit dimensiunea ferestrei. Astfel se evită o inundare a receptorului. În Fig.1.7 dimensiunea este şase. Astfel emiţătorul ştie câte cadre mai poate trimite receptorului fără ca acesta să le elimine. Dacă numărul de octeţi confirmaţi de receptor creşte, începutul ferestrei se mută spre dreapta şi fereastra se închide. Sfârşitul ferestrei se mută de asemenea spre dreapta dacă receptorul citeşte datele, le confirmă şi cere noi date. Acest procedeu este numit scalarea ferestrei.

1.2.6. Protocolul RTP

Protocolul de transport în timp real (Real Time Transport Protocol-RTP) asigură transmiterea end to end a pachetelor şi stă la baza protocoalelor pentru telefonia VoIP. Acest protocol are rolul de a transmite datele în timp real (de exemplu video sau voce) printr-o reţea de telecomunicaţii. Protocoalele de iniţializare a sesiunii (SIP-Session Initiation Protocol) şi H.323 îl folosesc pentru livrarea de date. Pentru a-şi atinge scopul RTP foloseşte serviciile aferente protocolului de la nivelul transport, de regulă cele ale UDP. Deoarece UDP nu are integrate mecanisme de reordonare a pachetelor sau de retransmitere a celor pierdute, nici RTP nu are această posibilitate. RTP permite însă reasamblarea pachetelor. La ora actuală RTP constă din două protocoale. Primul este RTP el însuşi, care transportă date în timp real. Al doilea protocol este Protocolul de Control în Timp Real (RTCP-Real Time Control Protocol), care monitorizează calitatea serviciului şi conţine informaţii de control despre participanţi. RTP şi RTCP utilizează porturi de transport consecutive când sunt încapsulate în pachete UDP [23], [26], [34], [35]. În plus, RTP defineşte pentru fiecare clasă de aplicaţii un profil şi unul sau mai multe formate. Un profil conţine informaţii pentru aplicaţii şi le ajută să înţeleagă sensul câmpurilor din antetul RTP.

1.2.7. Antetul RTP

În Fig.1.8 este prezentat antetul unui pachet RTP. Primele trei rânduri sunt întotdeauna prezente. Sursa informaţională este utilizată doar în circumstanţe speciale. Cazul general este acela în care un pachet de date RTP vine de la o sursă. Identificatorul acelei surse este numit sursă de sincronizare (SSRC). Un caz special este de exemplu un mixer care unifică mai multe fluxuri în unul singur pentru a salva lăţimea de bandă. În acel caz SSRC ar fi identificatorul mixerului (CSRC). Toate sursele care contribuie la acel flux vor apărea în câmpurile CSRC [34], [35].

<table>
<tr><td>Versiune V</td><td>Umplere (P)</td><td>Extensie (X)</td><td>CC Numărător CSRC</td><td>Marker (M)</td><td>Tipul de Informaţie (PT)</td><td>Număr secvenţă</td></tr>
<tr><td colspan="7">Timpul de transmitere</td></tr>
<tr><td colspan="7">Identificator sincronizare sursă (SSRC)</td></tr>
<tr><td colspan="7">Identificator sursă informaţională (CSRC)
.
.
.</td></tr>
<tr><td colspan="7">Extensie antet</td></tr>
</table>

Fig.1.8. Antet RTP [34]

Primii doi biţi (V) arată numărul de versiune al protocolului. Versiunea curentă este 2. Următorul bit este P (padding), un bit de umplere. Indică dacă informaţia utilă a fost încărcată, spre exemplu un algoritm de criptare care cere intrări de o anumită lungime. X (un bit) indică dacă sunt utilizate extensii ale protocolului în pachet. Este rar utilizat. CC (Count CSRC pe patru biţi) conţine numărul identificatorului CSRC care îi urmează antetului fix. M (marker pe un bit) este folosit la nivelul aplicaţie şi este definit în cadrul profilelor. Dacă este iniţializat, semnifică că datele curente au o semnificaţie specială pentru nivelul aplicaţie. Următorii şapte biţi aparţin câmpului PT (Payload Type), care specifică tipul de informaţie. Valoarea lui defineşte modul în care informaţia utilă va fi interpretată de aplicaţie. Numărul de secvenţă

este un număr pe 16 biţi. El defineşte în mod unic sursa unui flux RTP şi permite identificarea pachetelor pierdute sau care nu respectă ordinea. Este iniţializat printr-un număr aleator. Pentru fiecare pachet următor numărul de secvenţă este incrementat cu unu. Următorul câmp este cel al informaţiei de timp şi indică timpul de sincronizare al primului octet. Următorul câmp este pe 32 de biţi şi memorează o valoare unică. Următoarele câmpuri de la 0 la 15 sunt umplute cu identificatori unici de 32 de biţi.

1.2.8. Atacuri la securitatea unui sistem sau a unei reţele de calculatoare

Printr-un atac la securitatea informaţiei pe care o organizaţie o deţine se înţelege orice acţiune care compromite securitatea acestei informaţii. Atacurile se constituie din concretizări ale potenţialelor ameninţări care pot să planeze asupra securităţii unui sistem sau a unei reţele. În [31], [33] sunt amintite patru mari categorii de astfel de ameninţări: întreruperea, interceptarea, modificarea şi fabricarea. Atacurile sunt de două tipuri: pasive şi active.

Atacurile pasive sunt acele tipuri de atacuri în care atacatorul nu se implică în modificarea mesajului ci doar în citirea sa sau monitorizarea transmisiei. Avem astfel de a face cu atacuri la confidenţialitatea unei transmisii numite şi atacuri prin interceptare. Atacurile prin interceptare sunt de două tipuri:

1. **Dezvăluirea** (**Release of message content**) se manifestă prin aflarea conţinutului mesajului de către atacator prin simpla citire a datelor care se transmit prin sistem. Este un atac brut la confidenţialitatea datelor care duce la efecte nedorite pentru victima atacului. Aceste efecte pot varia de la unele neplăcute sau iritante în cazul în care este un simplu e-mail până la unele catastrofale în cazul în care este vorba despre un mesaj militar sau economic secret. Acest atac este încununat de succes în general doar dacă datele se transmit în clar pe canalul de transmisie (sau sunt criptate folosind algoritmi simpli, uşor de spart);
2. **Analiza de trafic** este un tip de atac mult mai subtil decât cel precedent şi se aplică în cazul în care datele au fost criptate folosind un algoritm puternic. În aceste condiţii, atacatorul chiar dacă a intrat în posesia datelor transmise nu le poate înţelege şi valorifica. Informaţiile pe care le-ar putea obţine un eventual atacator care foloseşte acest tip de atac ar fi sursa mesajului, destinaţia lui şi eventual frecvenţa transmisiei de mesaje între diferite site-uri. Chiar şi aşa, în timp, un agresor perseverent ar putea să observe unele tipare sau regularităţi în mesajele trimise de către un utilizator care nu îşi schimbă regulat cheile de criptare, regularităţi pe care le poate studia şi exploata prin alte tipuri de atacuri [2], [7].

Atacurile pasive sunt caracterizate prin faptul că detecţia lor este foarte dificilă. Neexistând modificări fizice ale datelor, atacurile nu pot fi descoperite în loguri şi astfel cei atacaţi nu sunt conştienţi de ele. Totuşi, prevenirea acestor atacuri este facilă dacă se folosesc algoritmi puternici de criptare şi se respectă nişte protocoale de securitate stricte.

Din punctul de vedere al unui sistem informatic, securitatea este o parte a capacităţii acestuia de a asigura siguranţa sistemului, dar nu este suficientă. Sunt patru părţi care contribuie la acest deziderat [32], [66]:

- **disponibilitatea**: o măsură pentru ca sistemul să fie funcţional la un anumit moment. O pierdere de disponibilitate este adesea menţionată ca Denial of

Service (DoS). O disponibilitate ridicată este de multe ori realizată prin intermediul unor sisteme hardware redundante;

- **fiabilitatea**: probabilitatea ca un sistem să-şi îndeplinească funcţiile sale pentru o anumită perioadă de timp. Fiabilitatea este diferită de disponibilitate, deoarece este măsurată pe o perioadă de timp şi corespunde continuităţii unui serviciu;
- **siguranţa**: indică dacă un sistem îşi exercită funcţiile sale în mod corect sau semnalizează o eroare în aşa fel încât să nu apară consecinţe catastrofale;
- **securitatea**: presupune protecţia tuturor resurselor de sistem.

Un sistem informatic, trebuie să fie disponibil tot timpul. Nu trebuie nici să piardă, dar nici să permită divulgarea unor informaţii. Datele trebuie să îşi păstreze caracterul de confidenţialitate şi integritate. Una dintre primele probleme care se pun este aceea a nivelului din modelul de referinţă TCP/IP la care trebuie aplicate măsurile de securitate. În continuare sunt prezentate câteva tipuri de atacuri mai des întâlnite.

1.2.9. Atacuri criptanalitice

Atacurile criptanalitice asupra unui algoritm au ca şi scop obţinerea textului în clar din textul cifrat fără a se cunoaşte cheia sau chiar aflarea cheii secrete care va putea fi folosită după aceea pentru descifrarea tuturor mesajelor viitoare. Există mai multe tipuri de astfel de atacuri după cum urmează ([30], [33], [45]):

- **Atacul bazat doar pe textul cifrat** (ciphertext-only attack)-este cazul în care criptanalistul are la dispoziţie pentru a efectua atacul doar textul cifrat în forma în care l-a interceptat de pe canalul de comunicaţie. Acesta este cel mai dificil tip de atac şi algoritmii care nu rezistă la aceste atacuri sunt consideraţi complet nesiguri.
- **Atacul bazat pe text în clar cunoscut** (known-plaintext attack)-este cazul în care atacatorul are la dispoziţie mai multe perechi (text în clar-text cifrat) înainte de a începe criptanaliza şi trebuie să afle cheia de criptare pentru a descifra transmisiile viitoare.
- **Atacul bazat pe text în clar ales** (chosen–plaintext attack)-spre deosebire de cazul anterior, atacatorul are posibilitatea să aleagă de multe ori el însuşi textul în clar şi obţine criptograma acestuia.
- **Atacul adaptiv bazat pe text în clar ales** (adaptive chosen-plaintext attack)-este o variantă a atacului bazat pe text în clar ales doar că criptanalistul nu va trebui să îşi planifice dinainte textul în clar pe care îl va alege spre a fi criptat ci poate să îşi modifice textul în clar în funcţie de rezultatele preliminarii ale atacului.
- **Atacul bazat pe text cifrat ales** (chosen–ciphertext attack)-acest atac este echivalent cu cel bazat pe text în clar ales doar că se aplică în general la partea de decriptare şi atacatorul are posibilitatea să aleagă criptograma pe care doreşte să o descifreze.
- **Atacul adaptiv bazat pe text cifrat ales** (adaptive chosen-ciphertext attack)-similar cu atacul adaptiv bazat pe text în clar ales dar folosit în general la descifrare (vezi descrierea atacului precedent).
- **Atacul bazat pe alegerea cheii** (chosen-key attack)-atac care se bazează pe relaţiile care pot exista în funcţie de diferitele chei.
- **Atacul prin forţă brută** (brute force attack) este atacul prin care se încearcă spargerea unui cod prin iterarea şi testarea tuturor valorilor din spaţiul cheilor, cu alte cuvinte în acest caz se vor testa toate variantele posibile până se va găsi cea

dorită. De exemplu, în cazul în care avem un algoritm care se bazează pe existenţa unei chei secrete de 128 de biţi, atacul prin forţă brută asupra acestui algoritm presupune testarea tuturor cheilor posibile până la găsirea celei corecte (maximum 2^{128} variante).

Totuşi există şi nişte condiţii în care atacul prin forţă brută se poate folosi şi anume:

- când algoritmii de criptare şi decriptare sunt cunoscuţi;
- când spaţiul cheilor posibile este suficient de mic;
- când limbajul folosit în cadrul textului în clar este cunoscut şi uşor de recunoscut.

1.2.10. Soluţii de securitate la nivelul reţea

Avantajul aplicării soluţiilor de securitate la nivelul reţea îl constituie faptul că această abordare le face invizibile nivelelor superioare, acestea fiind eliberate de o sarcină suplimentară.

Până în prezent sunt menţionate două mecanisme de securitate care pot fi folosite atât separat cât şi în conjuncţie şi un protocol de gestiune a cheilor la nivelul IP [45], [47]:

Antetul de autentificare (AH-Authentication Antet)-asigură integritatea datelor şi autentificarea acestora şi a emiţătorului lor. Este independent de algoritmii folosiţi.

Învelişul de securitate (ESP-Encapsulating Security Payload)-nu se impun algoritmii care se vor folosi şi se asigură confidenţialitatea, autentificarea şi integritatea datelor.

Protocolul de gestiune a cheilor (ISAKMP–Internet Security Association and Key Management Protocol)-este un protocol venit să rezolve la acest nivel problema distribuţiei cheilor pe baza unui algoritm asemănător cu Diffie-Hellman.

1.2.11. Soluţii de securitate la nivelul transport

La nivelul transport se pot menţiona două protocoale şi anume Nivel de Securitate Soclu (SSL-Secure Sockets Layer) şi Nivel Securitate Transport (TLS-Transport Layer Security). Dacă ar fi să plasăm aceste protocoale în modelul de referinţă OSI, locul acestora ar fi la nivelul sesiune pentru că ele oferă servicii de securitate deasupra protocoalelor de nivel transport cum ar fi TCP. Microsoft a propus de asemenea un protocol la acest nivel asemănător cu SSL pe care l-a denumit PCT (Private Communication Technology) [69].

Soluţiile de la nivelul aplicaţie pot fi protocoale independente sau protocoale care se bazează pe alte protocoale de acest nivel existente, ale căror performanţe le îmbunătăţesc. După natura aplicaţiilor lor, protocoalele de securitate pot fi referitoare la serviciul terminal (SSH–Secure Shell), la poşta electronică (PEM-Privacy Enhanced Mail, PGP-Pretty Good Privacy, S/MIME–Secure Multipurpose Internet Mail Extensions, MOSS-MIME Object Security Services) sau la aplicaţiile Web (S-HTTP–Secure HTTP).

Protocolul SSL (Secure Sockets Layer) a fost propus iniţial de către firma Netscape şi a devenit între timp specificaţie publică Internet ajunsă la versiunea 3.0. Este un protocol la nivel transport situat imediat deasupra protocolului TCP şi sub protocoalele de nivel aplicaţie. Acest lucru îl face să poată sta la baza oricărei aplicaţii Internet indiferent dacă aceasta este de tip TELNET, FTP sau Web. În cazul utilizării

SSL se criptează întreaga sesiune şi nu mesajele separate. Cele două concepte fundamentale care stau la baza comunicaţiei SSL sunt cele de sesiune şi conexiune.

Sesiunea SSL este o asociere între un server şi un client şi se creează în urma algoritmului de negociere (SSL Hand-shaking Protocol). De-a lungul unei sesiuni vor exista mai multe conexiuni. Conform specificaţiilor SSL, starea unei sesiuni este definită de următorii parametrii:

- Identificatorul sesiunii-un identificator unic generat de către server şi păstrat doar în cazul sesiunilor care mai sunt încă active sau mai pot fi repornite;
- Certificatul digital al partenerului-formatul certificatului este X.509 şi poate lipsi pe partea de server în cazul în care nu se cere autentificarea clientului;
- Metoda de compresie-identificatorul algoritmului de compresie ce se va folosi;
- Algoritmii folosiţi-se vor preciza algoritmul criptografic simetric ce se va folosi la criptarea datelor şi funcţia hash-code utilizată la calcularea codului de autentificare a mesajelor (MAC–Message Authentication Code);
- Cheia principală-cheia secretă comună serverului şi clientului;
- Indicatorul de repornire-are o valoare booleană şi indică dacă se mai pot crea sau nu conexiuni în sesiunea curentă.

Conexiunea SSL este o relaţie capăt-la-capăt între server şi client care oferă un anumit nivel de securitate ales. Conexiunile sunt temporare şi nu pot exista independent de o sesiune. Starea unei conexiuni este definită de:

- Secvenţa aleatoare-o secvenţă aleatoare de biţi aleasă de către server şi client pentru fiecare sesiune;
- Cheia secretă a server-ului de scriere a MAC–cheia secretă folosită de către server în operaţii legate de codurile de autentificare a mesajelor (MAC);
- Cheia secretă a clientului de scriere a MAC-corespondenta în cazul clientului cheii de mai sus;
- Cheia de scriere a serverului-cheia secretă ce se foloseşte în criptarea mesajelor de către server şi decriptarea de către client;
- Cheia de scriere a clientului-cheia secretă ce se foloseşte în criptarea mesajelor de către client şi decriptarea de către server;
- Vectorii de iniţializare-se folosesc de către algoritmii simetrici utilizaţi;
- Numerele de secvenţă-în cazul fiecărei conexiuni, atât severul cât şi clientul păstrează un număr de secvenţă care se tot incrementează cu fiecare operaţie efectuată.

SSL este compus din 4 subprotocoale: cel de înregistrare, de negociere, de alertare şi de schimbare a specificaţiilor cifrului care vor fi prezentate pe scurt în continuare. Pentru detalii suplimentare cu privire la SSL se recomandă [66], [69].

Protocolul de înregistrare SSL (SSL Record Protocol) este protocolul prin care mesajul iniţial este adus în forma în care va fi trimis pe canal către partener. Acelaşi protocol dar urmărind paşii în ordinea inversă va fi utilizat pentru a reface apoi la destinaţie mesajul în clar. Asupra unui mesaj se efectuează următoarele operaţii înainte de a fi transmis pe canal:

- Fragmentare-mesajul iniţial se va fragmenta în blocuri mai mici sau egale ca şi dimensiune decât 2^{14} octeţi;
- Compresie-se aplică o compresie fără pierderi care n-are voie să crească dimensiunea blocului cu mai mult decât 1 kB;
- Adăugarea MAC-se adaugă la final codul de autentificare al mesajului;
- Criptare-se foloseşte la criptare unul dintre următorii algoritmi simetrici: IDEA, RC2, DES, T-DES, RC4 sau Fortezza [11], [16], [18];
- Adăugare antet SSL-ca şi un ultim pas se va adăuga un antet ce va conţine identificatorul protocolului de nivel aplicaţie ce se aplică peste SSL, versiunea

majoră şi minoră a protocolului SSL folosit la prelucrare şi dimensiunea unui bloc.

Protocolul de negociere SSL (SSL Hand-shaking Protocol) este cel care urmează de fiecare dată când o sesiune este creată. Prin acesta server-ul şi clientul se vor autentifica şi vor cădea de acord asupra algoritmilor şi cheilor care vor fi folosite în schimbul propriu-zis de date. Acest protocol constă de fapt în 4 operaţii mari care vor fi efectuate în ordinea următoare:

- Stabilirea capabilităţilor criptografice-în această etapă atât clientul cât şi serverul prezintă partenerului algoritmii care sunt capabili să-i folosească şi se va cădea de acord asupra acelora dintre aceştia care vor fi folosiţi în continuare;
- Autentificarea serverului şi schimbul de chei: serverul îşi va trimite certificatul digital şi va avea loc schimbul de chei;
- Autentificarea clientului şi schimbul de chei: acest pas este facultativ şi prin el clientul va trimite propriul certificat digital pentru a fi autentificat;
- Finalizarea protocolului:în urma acestui pas se va crea sesiunea şi o conexiune sigură între client şi server.

Protocolul de schimbare a specificaţiilor cifrului SSL (SSL Change Cipher Specification Protocol) este cel mai simplu protocol din suita SSL. Constă în retransmiterea unui simplu octet cu valoarea 1 în urma căruia se vor schimba specificaţiile cifrului care se foloseşte în prezent şi se vor reseta numerele de secvenţă ale conexiunii curente [21], [26].

Protocolul de alertare SSL (SSL Alert Protocol)l se foloseşte pentru a alerta interlocutorul cu privire la apariţia unei erori în fluxul normal al SSL. Mesajele vor indica în primul octet dacă este vorba despre un simplu avertisment sau o eroare fatală. În cazul de pe urmă conexiunea curentă va fi imediat întreruptă.

Protocolul TLS (Transport Layer Security) reprezintă o variantă uşor modificată a protocolului SSL 3.0 care a fost standardizată de către IETF. Deosebirile apar în modul de generarea a codurilor de autentificare a mesajelor (MAC), în definirea unei ordini mai stricte a mesajelor şi în numărul mai mare de alerte. Astfel, singura modificare în protocolul de înregistrare faţă de SSL este schimbarea numărului de versiune minoră din antetul care se adaugă în ultimul pas. Ca urmare a acestei modificări versiunea va fi 3.1 în loc de 3.0. În protocolul de alertare pe lângă numărul mai mare de mesaje de alertă se va modifica şi nivelul de gravitate a unora dintre cele existente ele devenind din avertismente erori fatale.

Protocolul S-HTTP (Secure HTTP) a fost propus de către EIT (Enterprise Integration Technologies) şi este de fapt o variantă a clasicului protocol HTTP (Hyper-Text Transfer Protocol) care stă la baza www [65]. Această variantă oferă în sfârşit HTTP nivelul de securitate cerut în ziua de astăzi.

Dacă SSL şi TLS care au fost amintite anterior erau protocoale de nivel transport, S-HTTP acţionează la nivelul aplicaţie putând fi teoretic folosit împreună cu oricare dintre acestea. De asemenea, dacă SSL criptează întreaga sesiune, prin intermediul S-HTTP se criptează mesajele individuale ceea ce constituie un avantaj.

Criptările simetrice se pot face folosind unul dintre algoritmii DES, T-DES cu 2 sau 3 chei, DES-X, IDEA, RC2 sau CDMF (Commercial Data Masking Facility–varianta comercială cu cheie redusă a DES). Modul de operare va fi CBC (Cipher Block Chaining) în cazul mesajelor propriu-zise şi ECB (Electronic Codebook) în cazul antetelor.

Distribuţia cheii se poate face folosind metodele cunoscute din criptografia asimetrică, tichetele Kerberos dar se pot folosi şi chei distribuite în prealabil prin alte metode independente de protocol. Mai multe detalii despre S-HTTP pot fi găsite în [47], [61].

1.2.12. Securitatea prin firewall

Un firewall nu este un simplu ruter sau un calculator gazdă care asigură securitatea unei reţele. În linii mari, un firewall (numit uneori şi pasarelă de securitate) este un sistem care impune o politică de control al accesului între două reţele. Un firewall reprezintă implementarea acestei politici în termeni de configurare a reţelei, unul sau mai multe sisteme gazdă şi router-e cu funcţiuni speciale, autentificarea prin metode criptografice a clienţilor [47].

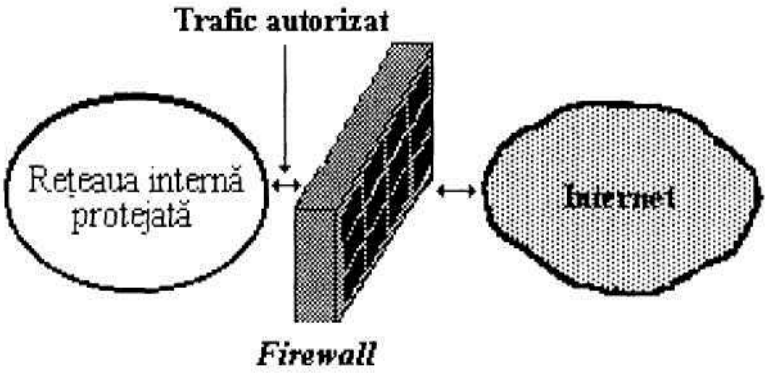


Fig.1.9. Dispunerea unui firewall [47]

Un firewall, Fig.1.9, este un mecanism folosit pentru a proteja o reţea sigură din punctul de vedere al securităţii de una nesigură, în care nu putem avea încredere.

În mod tipic, o reţea sigură este cea internă, a unei organizaţii, în timp ce cealaltă, nesigură, este Internet-ul (în care nu avem încredere din punctul de vedere al securităţii). Ultimele statistici referitoare la Internet arată că în compunerea sa intră peste 50.000 de reţele, cu un total de peste 2,5 milioane de sisteme gazdă, creşterea fiind estimată la 4.000 de noi domenii şi 150.000 de noi sisteme gazdă pe lună. Dat fiind numărul şi mai mare de utilizatori mulţi dintre aceştia având, din nefericire, statutul de hacker (cracker sau vandal) folosirea unui firewall are sens, deoarece probabilitatea "izbucnirii unui foc" undeva în internet este foarte mare.

Deşi cele mai multe firewall-uri sunt, în mod curent, interpuse între reţelele interne şi Internet, conceptul de firewall nu vizează numai acest aspect, existând suficiente motive pentru folosirea firewall-urilor în oricare reţea, inclusiv în reţelele cu arie largă (WAN) ale diferitelor companii. Deoarece un firewall este dispus la intersecţia dintre două reţele, acesta poate fi folosit şi în alte scopuri decât acela de control al accesului:

- pentru a monitoriza comunicaţiile dintre o reţea internă şi o reţea externă. De exemplu, un firewall poate jurnaliza (monitoriza, înregistra)

  serviciile folosite şi cantitatea de date transferată prin conexiuni TCP/IP între propria organizaţie şi lumea exterioară;
- un firewall poate fi folosit pentru interceptarea şi înregistrarea tuturor comu-

nicaţiilor dintre reţeaua internă şi exterior. O linie închiriată, care permite viteze de până la 128 Kbps, în condiţiile în care ar fi folosită 100% din timp, ar transfera zilnic circa 1,4 GB, ceea ce ar permite ca traficul pe câteva zile să încapă pe o singură bandă magnetică digitală de 8 mm;

- dacă o organizaţie are mai multe reţele, separate din punct de vedere geografic, fiecare având câte un firewall, există posibilitatea programării acestor firewall-uri pentru a cripta automat conţinutul pachetelor transmise între-treele. în acest fel, pe suportul internet, organizaţia îşi poate realiza propria reţea virtuală privată [2], [12].

Teza este legată de analiza protocoalelor utilizate în telefonia IP, identificarea slăbiciunilor şi propunerea soluţiilor de îmbunătăţire a sistemului de securitate. De asemenea urmăreşte şi reducerea întârzierilor la iniţializarea unei sesiuni de apel vocal bazat de protocolul SIP. Munca implică două părţi: una teoretică şi una practică. Partea teoretică explică tehnologia din spatele telefoniei IP şi a securităţii, analizează protocoalele aplicate în arhitectura VoIP şi propune un cadru de securitate. Partea practică constă în implementarea rezultatelor într-un centru de telefonie VoIP.

1.3. Actualitatea temei

Reţelele de telefonie IP PBX (Private Branch eXchange) sunt din ce în ce mai frecvent folosite în cadrul companiilor de dimensiuni medii şi mari. Printre motivele răspândirii acestora merită amintite costurile mult diminuate comparativ cu, conectarea fiecărui aparat telefonic din companie la o linie externa precum şi folosirea în comun de către sute de utilizatori a câtorva linii externe pentru efectuarea de apeluri în afara companiei. În plus, comunicarea internă este mai facilă deoarece numerele sunt formate din 3 sau 4 cifre.

Analiştii estimează că până la sfârşitul anului 2009, o cotă de 90% din piaţa va aparţine reţelelor IP PBX. Totuşi, înainte de a implementa o reţea VoIP, trebuie cunoscute riscurile la care acestea sunt expuse şi măsurile care pot fi luate pentru a le contracara**.**

Prin implementarea şi supravegherea politicilor de securitate se doreşte evitarea unor incidente de genul:

- Sniffing: folosirea unor programe care monitorizează traficul efectuat într-o reţea în scopul sustragerii de informaţii. Aceste programe sunt aproape imposibil de detectat şi se pot insera în orice punct;
- Folosirea neautorizată a serviciului prin intermediul unui computer şi/sau a altor dispozitive care pot induce în eroare un sistem de telefonie în scopul efectuării de apeluri gratuite sau care să fie taxate unui alt utilizator;
- Spam prin telefonie internet (SPIT) presupune transmiterea de apeluri nedorite către căsuţele vocale ale utilizatorilor;
- Troieni cu acces de la distanţă (Remote acces trojan) oferă atacatorului acces în sistemul afectat pentru a sustrage informaţii stocate pe acesta sau pentru a lansa atacuri asupra altor sisteme;
- Flux de distribuţie (Broadcast storm) ce implică ocuparea întregii lăţimi de bandă prin transmiterea simultană a unui mare număr de mesaje prin reţea şi care solicită dispozitivelor receptoare transmiterea ca răspuns a altor mesaje similare;
- Falsificarea certificărilor Wi-Fi (wireless fidelity) pentru accesul neautorizat în reţelele fără fir. Acestea sunt emise de Wi-Fi Alliance şi garantează că dispozitivele fără fir sunt interoperabile chiar daca provin de la producători diferiţi.

Astfel se poate obţine fraudulos accesul într-un punct de acces (Access Point-AP) la o staţie de bază care este conectată la reţelele fixe şi se oferă astfel acces de tip internet fără fir pe o raza de 50 m.

Utilizatorii VoIP sunt vulnerabili la atacurile îndreptate împotriva serviciilor tradiţionale de telefonie fixă sau mobilă, care au ca scop obţinerea de informaţii, furtul de identitate sau comiterea unor fraude. Centralele VoIP, responsabile de procesarea apelurilor, a numerelor şi a datelor de autentificare, utilizează sisteme de operare, protocoale internet, aplicaţii şi interfeţe de configurare care sunt vulnerabile la viruşi, viermi, spyware, tentative de acces neautorizat sau atacuri de tipul refuzului serviciului (Denial of Service-DoS).

VoIP utilizează Protocolul de Iniţializare Sesiune (SIP-Session Initiation Protocol) şi Protocolul în Timp Real (RTP-Real-time Transport Protocol) pentru transmiterea mesajelor vocale. Acestea nu asigură identificarea corespunzătoare a participanţilor la apel, nu protejează confidenţialitatea şi integritatea datelor trans-mise şi recepţionate pentru iniţierea apelurilor şi transmiterea datelor (spre deosebire de fluxurile media ce conţin semnal audio comprimat şi criptat). Până când aceste cerinţe de securitate vor fi implementate atacatorii ar putea identifica numeroase vulnerabilităţi care pot fi exploatate.

Deoarece protocoalele SIP şi RTP nu criptează apelul şi fluxurile de semnal audio (voce), atributele de identificare (nume/parola) şi numerele de telefon SIP ale utilizatorilor pot fi interceptate prin reţele locale fără fir folosind sniffer-e. Un atacator poate folosi informaţiile sustrase pentru a contacta un reprezentant al furnizorului de servicii VoIP (prezentându-se drept utilizator legitim) sau pentru a accesa interfaţa de configurare web şi a modifica setările pentru a permite apeluri la numere cu taxare specială sau în străinătate, pentru a accesa mesageria vocală a clientului sau pentru a schimba numărul de telefon spre care sunt direcţionate apelurile nepreluate. Furtul de identitate în aceste cazuri este folosit pentru a efectua apeluri costisitoare la mare distanţă sau pentru a obţine informaţii sensibile de natură financiară sau personală.

Supraîncărcarea prin inundare a reţelelor VoIP cu mesaje SIP (prin simularea diverselor faze ale apelurilor iniţiere, încheiere sau transmiterea de fluxuri de date media RTP) pot diminua calitatea serviciului, pot provoca întreruperea apelurilor sau pot forţa echipamentele să nu mai proceseze toate apelurile primite. Echipamentele VoIP sunt de asemenea vulnerabile la atacuri TCP SYN sau ping of death. Sistemele de operare şi comunicaţiile TCP/IP folosite de echipamentele VoIP sunt vulnerabile la atacuri ce vizează încetarea funcţionării lor sau preluarea controlului de la distanţă. Transmiterea şi execuţia de cod arbitrar prin intermediul aplicaţiilor softphone poate afecta calculatoarele şi dispozitivele mobile (laptop, PDA) pe care acestea sunt instalate. Prin spam de multe ori sunt transmise aplicaţii spyware sau de control de la distanţă sau mesaje de publicitate nedorite. Din aceste motive este necesar ca înainte de implementarea VoIP să fie evaluate riscurile pe care o astfel de iniţiativă le presupune şi să fie elaborată o strategie de combatere a acestora.

Transmisiunile de voce constituie sursa principală de venit a companiilor de telefonie tradiţionale, o piaţă în plină dezvoltare pentru furnizorii de servicii VoIP şi un serviciu absolut necesar desfăşurării activităţii de afaceri. Din acest motiv, principalul risc pe care trebuie să îl înfrunte operatorii VoIP este întreruperea serviciului. Clienţii se aşteaptă la aceeaşi disponibilitate pe care o oferă furnizorii tradiţionali de servicii de telefonie fixă şi mobilă. Planul de implementare a VoIP trebuie să conţină măsuri de combatere a atacurilor de tip Denial of Service (DOS), care vizează încetarea funcţionării echipamentelor [20], [26].

O altă prioritate o constituie prevenirea furtului de identitate şi a folosirii abuzive de către atacatori a conturilor clienţilor. Operatorii VoIP sunt confruntaţi cu ameninţări mai grave decât furnizorii de servicii de telefonie fixă sau mobilă deoarece adresele IP de provenienţă ale mesajelor nu sunt verificate în centralele VoIP şi încă nu au fost adoptate la scara largă metode de certificare coordonată între furnizori şi de verificare a validităţii identităţilor SIP. Prin urmare operatorii trebuie să fie precauţi în colaborarea cu alţi furnizori VoIP şi să nu stabilească relaţii cu aceştia fără să se asigure în prealabil că sunt respectate procedurile de validare a identităţii şi a integrităţii centralelor VoIP prin care sunt vehiculate apelurile.

Atacurile interne sunt în general mai frecvente decât cele din afara organizaţiei. Operatorii VoIP trebuie să ia în considerare posibilitatea furtului de identitate chiar şi atunci când îşi desfăşoară activitatea izolat de alţi furnizori. Din acest motiv managerii companiilor VoIP trebuie să pună la punct metode de combatere a furtului de identitate şi să monitorizeze metodele de audit intern pentru depistarea abuzurilor şi identificarea celor responsabili. De asemenea, în comparaţie cu reţelele publice, reţelele private VoIP vor fi vizate mai frecvent de acţiuni de culegere de informaţii legate de activităţile de afaceri.

Furtul de identitate în scopul utilizării frauduloase sau abuzive a serviciilor VoIP (efectuarea de apeluri costisitoare în detrimentul unor clienţi) sunt probleme foarte serioase cu care serviciul de relaţii cu clienţii se poate confrunta. Rezolvarea reclamaţiilor şi continuarea asigurării serviciilor pentru clienţii care au căzut victime ale unor astfel de atacuri vor solicita intens resursele companiei şi vor afecta negativ productivitatea. Efectele negative pe care incidentele le au asupra consumatorilor, utilizatorilor, managementului sau chiar a încrederii propriilor acţionari pot fi de lungă durată [33], [61].

În teza de doctorat s-a studiat de asemenea şi posibilitatea reducerii sesiunii de iniţializare a protocolului SIP prin introducerea unui contor adaptiv pentru retransmisie cu rolul de a reduce cozile de aşteptare prin ajustarea mărimii pachetelor de semnalizare implicate în iniţierea unei apel VoIP. De asemenea a fost studiată şi propusă o soluţie bazată pe reducerea timpului de transmitere a datelor prin controlul numărului de apeluri admise în lista de interogare a punctelor de acces (AP). A fost făcut un studiu experimental al întârzierilor în reţelele fără fir, pentru situaţia unei distribuţii multiple (multicasting). Pentru acest caz rata maximă de transfer care poate fi atinsă este de 1.78 Mbps, pentru reţelele cu trafic de 2 Mbps. Suplimentar trebuiesc implementate mecanisme de reducere a pierderilor cadrelor la nivelul MAC.

Majoritatea serviciilor VoIP sunt găzduite de sisteme de operare comerciale instalate pe servere. Întărirea securităţii acestora şi implementarea unor aplicaţii profesionale de detectare a intruşilor vor diminua considerabil şansele de succes ale atacurilor la care sunt expuse. În teză a fost propusă o nouă soluţie de securitate bazată pe conceptul de client-server. Studiul este motivat de faptul că nivelul de control al accesului al mediu (MAC-Medium Access Control) al standardului IEEE 802.11 suportă retransmiteri ale pachetelor, impuse de erorile de transmisie ale celor două moduri, PFC şi DCF, în care operează acest standard [41]. În urma unui studiu comparativ al performanţelor protocoalelor de semnalizare SIP, H.323 şi IAX, am optat pentru IAX, un protocol de tip open source, uşor de utilizat şi modificat. Prezintă avantajul că foloseşte lăţime de bandă minimă atât pentru transferul datelor cât şi pentru semnalizare şi are suport nativ pentru translatarea adreselor de reţea.

Dintre măsurile de securitate a server-elor aplicabile şi celor care deservesc reţelele VoIP enumerăm:

- Actualizarea permanentă a sistemelor de operare şi a programelor VoIP cu ultimele aplicaţii corectoare de tip patch lansate de producători;

- Menţinerea pe server doar a aplicaţiilor necesare derulării în bune condiţii a serviciilor VoIP;
- Reguli de autentificare solide pentru accesul administratorilor şi a utilizatorilor pe server garantarea accesului pe server pentru un număr minim de conturi de utilizator necesare asigurării întreţinerii şi funcţionării în bune condiţii a acestuia;
- Implementarea de proceduri de autentificare complexe pentru a preveni accesul neautorizat la serviciile VoIP sau la datele de identificare ale clienţilor;
- Derularea de activităţi de audit intern privind operaţiile desfăşurate de administratori şi utilizatori;
- Instalarea şi întreţinerea programelor firewall şi a aplicaţiilor antivirus pentru a combate atacurile de tip refuz al serviciului (DOS);
- Configurarea corespunzătoare a aplicaţiilor VoIP, spre exemplu utilizarea unei liste a codurilor de ţară apelabile, poate evita unele tentative de utilizare neautorizată sau abuzivă a serviciilor.

1.4. Structura tezei de doctorat

C**apitolul 1 „Motivaţie**" prezintă o privire de ansamblu a problemelor securităţii reţelelor fără fir care sunt relativ mai puţin sigure decât cele cablate, datorită accesului mai facil la reţea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. Totodată sunt prezentate pe scurt structura unei reţele, protocolul de transport al Internet-ului şi diverse soluţii de securitate implementate până în prezent. Tot în cadrul acestui capitol sunt prezentate motivele care au condus la tratarea acestei teme de cercetare ce face obiectul tezei.

Capitolul 2 „Stadiul actual al securităţii VoIP în reţelele fără fir bazate pe standardul IEEE 802.11" prezintă stadiul actual privind măsurile adoptate pentru asigurarea securităţii aplicaţiilor VoIP. Este făcută o evaluare a riscurilor utilizării VoIP din perspectiva furnizorilor şi utilizatorilor de servicii de voce prin reţelele fără fir. Sunt menţionate tipurile de atacuri şi algoritmii de criptare utilizaţi pentru a asigura securitatea comunicaţiilor fără fir. De asemenea sunt prezentate măsurile de securitate a server-elor care deservesc reţelele VoIP.

Capitolul 3 „Modalităţi de reducerea a întârzierilor la iniţializarea unei sesiunui bazate pe protocolul SIP în reţelele fără fir" are caracter de noutate şi prezintă un contor adaptiv pentru retransmitere, menit să optimizeze performanţele protocoalelor de semnalizare din sesiunea de iniţializare. În acest capitol se prezintă:

- întârzierile din sesiunea de iniţializare SIP;
- protocoalele de transport TCP, UDP şi RLP;
- analiza semnalizărilor SIP din legăturile fără fir;
- rezultatele numerice şi relevanţa contorului adaptiv pentru retransmitere;
- suportul pentru serviciile VoIP, arhitectura, întârzierile survenite în transmiterea şi recepţia datelor, precum şi soluţia propusă;
- descrierea rezultatelor numerice;
- analiza erorilor.

Capitolul 4 „Soluţii pentru asigurarea securităţii în reţelele fără fir" are de asemenea un caracter de noutate şi prezintă două contribuţii personale, una descrie un prototip de software pentru securitatea şi mobilitatea sistemelor VoIP, iar

cea de-a doua implementează un sistem criptografic pentru o comunicaţie sigură client-server. Acest capitol descrie:

- standardul IEEE 802.11. Este prezentată o imagine de ansamblu a securităţii lui şi a extinderii mecanismelor de control al accesului;
- expunerea motivelor alegerii IAX ca şi protocol pentru o transmisie sigură VoIP;
- Un sistem care utilizează diverse moduri de criptare pentru a determina care este cel mai adecvat pentru a asigura atât calitatea apelului cât şi utilizarea cât mai redusă a procesorului.

Acest capitol prezintă de asemenea un studiu experimental al performanţei şi fiabilităţii transmisiei cu destinaţii multiple în subnivelul de acces la mediu al reţelelor fără fir bazate pe standardul IEEE 802.11. În multe cazuri, distribuţia multiplă permite o utilizare mult mai eficientă a reţelelor, deoarece elimină nevoia de a trimite mai multe pachete identice la destinaţii diferite. Acest studiu experimental are ca scop determinarea gradului de utilizare a distribuţiei multiple a vocii la nivelul substratului de control al accesului la mediu (MAC) pentru două situaţii. Prima situaţie este utilizarea distribuţiei multiple pentru fluxurile de voce din link-ul de coborâre (downlink) şi este destinată mai mult celor aflaţi în aceeaşi celulă a unei reţele fără fir, cum ar fi teleconferinţele, emisiuni audio în întreprinderi sau situaţii de urgenţă. A doua situaţie este utilizarea în regim de walkie-talkie unde numai unul din participanţi are permisiunea de a accesa reţeaua la un moment dat.

Capitolul 5 face o sinteză a principalelor contribuţii teoretice şi a rezultatelor experimentale obţinute în cadrul cercetării expuse în teză.

1.5 Lucrări publicate de doctorand

Soluţiile şi metodele noi dezvoltate în cadrul acestei teze au fost publicate în următoarele articole:

1. Ioaneşiu M., *An Experimental Analysis of Performance of MAC Multicast Distribution in 802.11 Networks for VoIP Traffic*, Lucrările sesiunii de comunicări ştiinţifice „Doctor Etc 2009", Timişoara, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, pp.49-54, ISSN 2066-883X, Timişoara, September 2009.
2. Ioaneşiu M., Toma C.I., *Optimization of SIP session setup delay for VOIP in 3G wireless networks*, Proceedings of the 4th International Conference on Engineering Technologies–ICET 2009, pp. 367-375, ISBN 978-86-7892-227-5, Novi Sad, Serbia, April 2009.
3. Ioaneşiu M., Toma C.I., *Support of Voice services in IEEE 802.11 wireless LANs*, Proceedings of the 4th International Conference on Engineering Technologies–ICET 2009, pp. 379-385, ISBN 978-86-7892-227-5, Novi Sad, Serbia, April, 2009.
4. Ioaneşiu M., *Security of Mobile VoIP*, International Symposium on Electronics and Telecommunications, ETC 2008, Eight Editions, Buletinul Ştiinţific al Universităţii „Politehnica" din Timişoara, Tom 53 (67), Fascicola 2, 2008, pp. 36-41, ISSN 1583-3380, Seria Electronică şi Telecomunicaţii, Timişoara, September 2008.
5. Ioaneşiu M., *The security in wireless networks based on 802.11 standards. Problems and solutions. Developments of 802.11 standards in connection with security problems* , Lucrările sesiunii de comunicări ştiinţifice „Doctor Etc 2007 ", Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, pp. 88–93, ISBN 978–973–625–494-9, Timişoara, September, 2007.
6. Ioaneşiu M., *Securitatea datelor prin criptare,* Referatul 3 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2006.
7. Ioaneşiu M.**,** *Stadiul actual şi de perspectivă al securităţii reţelelor de calculatoare,* Referatul 2 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2005.
8. Ioaneşiu M., *VPN şi securitatea datelor***,** Referatul 1 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2004.

2. STADIUL ACTUAL AL CALITĂŢII TRANSMISIEI VOCII ÎN REŢELELE FĂRĂ FIR BAZATE PE STANDARDUL IEEE. 802.11

Acest capitol este structurat pe 9 subcapitole şi urmăreşte prezentarea stadiului actual al calităţii serviciilor VoIP în reţelele fără fir bazate pe standardul IEEE 802.11. În primul paragraf sunt prezentate şi discutate deficienţele legate de securitatea transmisiei vocii prin Internet utilizând protocolul IP. În paragrafele 2.2-2.5 se prezintă structura reţelelor fără fir, protocoalele utilizate, factorii care afectează performanţa VoIP şi straturile protocolului. În paragraful 2.6 sunt prezentate tipurile de atacuri asupra protocolului SIP. Mecanismele de securitate existente în reţelele fără fir sunt prezentate în paragraful 2.7. Metodele propuse în teză, de îmbunătăţire a calităţii transmisiei vocii în reţelele fără fir sunt prezentate în paragraful 2.8. Paragraful final face o trecere în revistă a concluziilor rezultate din studiul prezentat în acest capitol.

2.1. Consideraţii generale

Standardul IEEE 802.11 al reţelelor fără fir (Wireless Local Area Network-WLAN) acoperă substratul de control al accesului la mediu (Media Access Control-MAC) şi stratul fizic (PHY-Physical Layer), din suita de straturi de reţea definită de sistemul de interconectare deschis (OSI) [15], [46], [65].

Comunicaţiile fără fir prezintă un risc mai mare de atac în comparaţie cu cele efectuate prin cablu, fapt ce a impus aplicarea unor măsuri de securitate speciale, conform protocolului AAA (authentication, authorization, accounting). Sistemul de autentificare al standardului IEEE 802.11 are definite trei componente: solicitantul, autentificatorul şi server-ul de autentificare. Multiplele aplicaţii care folosesc acest mediu, au anumite constrângeri legate de asigurarea calităţii. Aceste constrângeri sunt pentru majoritatea aplicaţiilor cerinţele legate de rata de transfer, de întârziere şi de livrarea pachetelor. Pe măsură ce tot mai multe dispozitive de genul telefoanelor fără fir şi bluetooth accesează acelaşi canal nelicenţiat ca şi reţelele fără fir, nu se mai pune problema neglijării pierderii pachetelor [32].

Complexitatea serviciului de transmitere a vocii prin Internet (VoIP) creează un număr mare de vulnerabilităţi care afectează trei mari domenii de securitate a informaţiilor: confidenţialitatea, integritatea şi disponibilitatea [1], [2].

S-au efectuat studii privind robusteţea protocoalelor de securitate pe diverse niveluri ale modelului OSI şi s-a ajuns la concluzia că unele sunt mai robuste pentru o mobilitate mai redusă a reţelei, faţă de cazul în care mobilitatea creşte [1], [3], [9], [15], [20], [22].

Comunicarea într-un mediu fără fir se face prin staţii client, care utilizează modemuri radio pentru a comunica cu punctele de acces, AP. Staţiile client sunt echipate în general cu plăci de reţea pentru mediul fără fir care au în componenţă un emiţător-receptor radio şi logică pentru a permite interacţiunea dintre hardware şi software. Punctele de acces conţin în esenţă acelaşi emiţător-receptor şi în plus, o

punte (bridge) conectată la nucleul reţelei cablate. Punctul de acces este un dispozitiv staţionar care face parte din reţeaua locală-LAN şi este similar unei celule (staţie de bază) din comunicaţiile celulare. Toate comunicaţiile dintre staţiile client şi dintre clienţi şi reţelele cablate trec printr-un punct de acces Fig.2.1 [1].

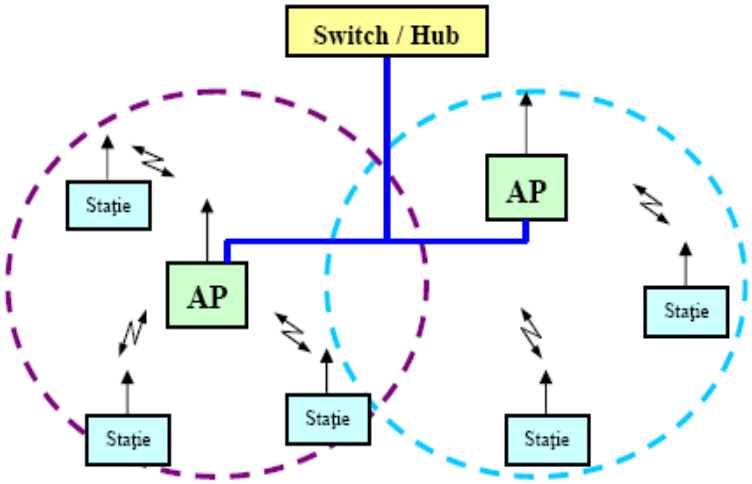


Fig.2.1 Topologia fundamentală a unei reţele fără fir 802.11 [1].

Viteza este aspectul cel mai important al comunicaţiilor VoIP. Foarte puţine reţele îşi pot permite întârzieri datorită congestiei traficului, iar furnizarea de lăţime de bandă suficientă nu este de multe ori soluţia. Bianchi [9], Cheriton, Faria [21], Rughiniş [67] au semnalat faptul că în numeroase reţele VoIP apare problema asigurării unei translaţii corecte a adresei la graniţa dintre reţele (Network Address Translation-NAT) şi au recomandat rutarea prin cât mai puţine noduri.

Aplicaţiile actuale, folosite pentru transmiterea vocii în reţelele fără fir, nu utilizează întotdeauna, în mod eficient, resursele acestora. Datorită supraîncărcării pachetelor mici ce se transmit într-o reţea fără fir (WLAN), lăţimea de bandă disponibilă pentru traficul VoIP este mult sub rata maximă de transfer a datelor, de 11 Mbps pe care în mod normal o suportă o reţea de fără fir. Această supraîncărcare se datorează transmiterii de octeţi suplimentari, adăugaţi la parcurgerea diferitelor straturi ale reţelei (antetele pachetelor) şi întârzierilor impuse de cele două variante de organizare a reţelelor fără fir (Funcţia de Coordonare Distribuită-DCF şi Funcţia de Coordonare prin Punct-PCF).

În prezent, noul standard are posibilitatea unor intrări şi ieşiri multiple (Multiple Input Multiple Output-MIMO), fapt ce permite o rată maximă de transfer de 600 Mbps, îmbunătăţirea transmisiei datelor prin utilizarea mai multor antene, a unor mecanisme de codare care să asigure securitatea datelor şi să poată transmite punctelor de acces informaţii referitoare la datele conţinute atât pe link-ul de upstream cât şi pe cel de downstream [64].

2.2. Structura reţelelor fără fir

Pentru reducerea ratei erorilor pe canalele reţelelor fără fir au fost şi sunt elaborate în continuare seturi de servicii care să asigure calitatea transmisiei. Pentru a veni în sprijinul traficului care se desfăşoară atât în timp real cât şi în timp nereal, Hong Hou, Borkar şi Kumar [32], au studiat problema asigurării calităţii în reţelele fără fir, iar în lucrarea lor sunt amintite:

1. studiile efectuate de Johnsson şi Cocs care au propus o politică de reducere a timpului de întârziere a pachetelor concomitent cu mărirea ratei de transfer la utilizator;
2. sistemul proiectat de Dua şi Bambos care face un compromis între corectitudinea datelor la utilizator şi performanţa sistemului;
3. studiile făcute de Stolyar şi Ramanan vizează oferirea de garanţii de calitate serviciilor implementate la client. Acest tip de abordare oferă însă un optim numai pentru o perioadă mare de timp.

Hong Hou, Borkar şi Kumar [32], s-au concentrat mai mult pe probleme de punere în aplicare şi consolidare a calităţii transmisiei pentru mecanismele aferente standardului IEEE 802.11. Simulările lor au fost efectuate într-un mediu controlat, în cazul în care pierderile de pachete sunt rare. Comparativ cu politicile de scanare reţea, care au fost mai mult studiate, există mai puţine studii analitice privind controlul admisiei în reţelele fără fir. Garg, Zhai, Shin şi Schulzrinne [69] au folosit diferite metrici pentru a prevedea, din punct de vedere statistic, performanţele reţelei. Au propus controlul admisiei pe bază de algoritmi pentru a garanta o anumită lăţime de bandă pentru fiecare utilizator, fără a lua în considerare latenţa.

Practic, intervalul de timp necesar asamblării pachetelor spre a fi transmise este considerat a fi factorul determinant în calitatea transmiterii datelor prin reţelele fără fir. În plus, supraîncărcarea impusă de cele două variante de organizare a reţelelor fără fir nu este fixă, ci creşte, pe măsură ce numărul de staţii care doresc acces la mediu creşte.

Acceptarea unui apel suplimentar, faţă de numărul maxim de apeluri acceptate, în curs de desfăşurare, poate avea consecinţe dezastruoase dacă se depăşeşte lăţimea de bandă disponibilă. Prin experimente cu diverse codec-uri şi sisteme de încapsulare a pachetelor, s-au stabilit relaţii între calitatea convorbirilor şi resursele reţelelor fără fir utilizate. În cazul în care lăţimea de bandă efectiv disponibilă este aproape de zero, calitatea convorbirii poate deveni inacceptabilă pentru toate apelurile în curs de desfăşurare. Utilizarea resurselor poate fi monitorizată de programe (sniffer-e) care urmăresc pasiv pachetele din trafic, la nivelul stratului 2 (L2/MAC) al mediului fără fir şi furnizează informaţii despre cele trei componente care consumă lăţimea de bandă (încărcarea, accesul şi eliberarea mediului). Informaţiile oferite de programele mai sus amintite sunt necesare pentru asigurarea calităţii transmisiei şi recepţiei datelor.

În prezent reţelele fără fir folosesc un sistem criptografic cu o variabilă permanentă fixă sau o cheie de criptare sau nici un fel de criptare. Acest lucru, cuplat cu faptul că pot oferi puncte de acces la reţea pentru orice intrus (dincolo de nivelul fizic şi dincolo de controalele de securitate ale organizaţiei) creează probleme de securitate. Legat de acest aspect este faptul că accesul la mecanismele de control al punctelor de acces conţin erori, creând o breşă pentru orice adversar [1].

În contextul reţelelor fără fir, solicitantul este de obicei un nod mobil având implementat clientul standardului IEEE 802.11. Punctul de acces, AP, joacă rolul de autentificator. Chen Ling, Jian de Lu, [19], folosesc pentru server-ele de autentificare, autorizare şi taxare-AAA (authentication, authorization and accounting) proto-

colul RADIUS (Remote Authentication Dial In User Service). Puteau opta şi pentru succesorul acestuia, DIAMETER.

În prezent, sunt implementate scheme de tip open-source, cunoscute sub denumirea de Xsupplicant, pentru Linux şi WIRE1x, pentru Windows. Una dintre problemele comune constă în faptul că aceste scheme sunt concepute numai pentru Linux sau Windows, neacordând suficientă atenţie protocolului de extensie a autorizării pentru reţelele fără fir (Extensible Authentication Protocol over Wireless EAPoW) şi taxării, Chang Chin Cheng [17], Chen Ling [19].

În reţelele fără fir, datorită mediului prin care se propagă informaţia, nu se poate şti dacă un telefon VoIP sau un calculator transmit date pe legătura (link-ul) de upstream sau downstream. Pentru link-ul de upstream nu se pot aplica măsuri de calitate a serviciului. Conform Ross Rehart [66], singura posibilitate rămâne pentru cel de downstream, prin introducerea unor porţi (gateway) sau routere de încredere care să analizeze pachetele recepţionate, ca în Fig.2.2.

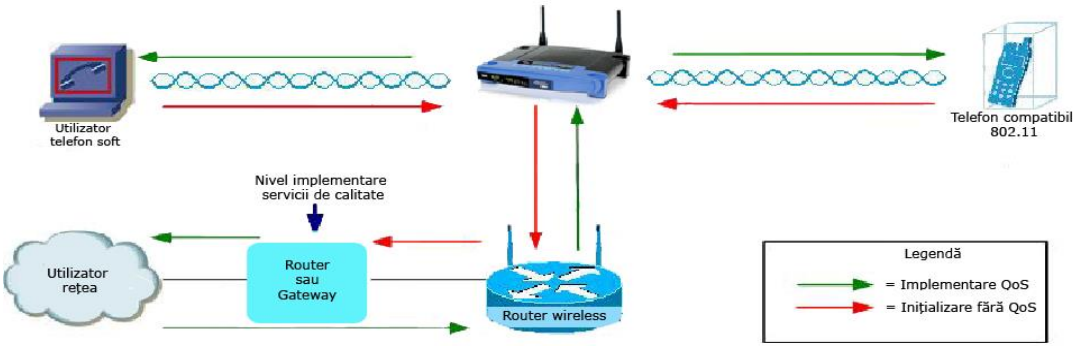


Fig.2.2 Arhitectură pentru implementarea serviciilor de calitate(QoS) [66]

Agarwal, Wang [1] şi Albers&Co [2] au efectuat experimente care arată influenţa protocoalelor de securitate asupra parametrilor de calitate, QoS. De exemplu, dacă timpul de autentificare, cuprins între 0,11 s şi 6,28 s, nu este asigurat, se poate ajunge la o pierdere dramatică de pachete. De asemenea, pentru acelaşi protocol de transfer de securitate, în afara serviciului de roaming, timpul alocat pentru el poate fi de până la două ori mai mare decât în roaming.

În [19] este descrisă arhitectura unei multiplatforme integrate (IMEWAS-A Integrate Multiplatform EAPoW-based WLAN AAA Solution) care se bazează pe standardul IEEE 802.11, pe protocolul de autentificare extins (EAP) şi un server de tip AAA, ce foloseşte protocolul RADIUS. Acesta utilizează bibliotecile WinPcap /Libpcap pentru Windows respectiv Linx, ca suport de bază pentru interacţiunea dintre cadrele de autentificare ale standardului IEEE 802.11 şi porturile de control al acce-sului în punctele de acces AP [19].

Platforma IMEWAS este o platformă flexibilă, sigură şi poate fi modulată. Este o structură la care se pot adăuga servicii şi poate fi uşor depanată.

Protocolul de autentificare extensibil pentru reţele fără fir, WLAN-EAP, permite implementarea mai multor metode de autentificare cum ar fi funcţia de autentificare hash MD5 (bazată pe algoritmul Message-Digest Algorithm 5) sau protocolul pentru securitatea stratului de transport-TLS (Transport Layer Security).

Prin utilizarea bibliotecilor WinPcap/Libpcap şi Libnet se asigură rularea pe mai multe platforme. În plus, parola utilizatorului şi sesiunea sunt securizate prin certificate de autentificare datorate protocoalelor utilizate [18].

Substratul MAC (Media Access Control) al standardului 802.11 oferă funcţii de control al accesului la mediul fără fir, cum ar fi coordonarea, adresarea sau trimiterea de secvenţe de cadre de verificare. Substratul MAC defineşte două funcţii de acces la mediu pentru a rezolva problemele legate de transmisie [1], [65]:

1. **Funcţia de bază, de coordonare distribuită** (Distributed Coordination Function DCF) care este similară organizării din reţelele cu, comutare de pachete şi este destinată transferului asincron de date;
2. **Funcţia de coordonare prin puncte** (Point Coordination Function-PCF) care se bazează pe interogări controlate de punctele de acces (**AP**) şi care este destinată transmisiunilor sensibile la întârzieri.

Conform standardului IEEE 802.11 se disting două tipuri de reţele locale:

1. **reţele ad-hoc;**
2. **reţele infrastructurale**.

O reţea ad-hoc este o grupare a staţiilor într-o singură arie de bază (Basic Service Area-BSA) cu scopul comunicării inter-reţele fără ajutorul unei reţele infrastructurale.

Orice staţie poate stabili o sesiune de comunicaţie directă cu altă staţie fără a fi necesară direcţionarea traficului printr-un punct de acces (AP) centralizat.

În opoziţie cu reţelele ad-hoc, reţelele infrastructurale au scopul de a servi utilizatorii cu servicii specifice şi de a permite extinderea zonei. Aceste reţele se constituie utilizându-se un punct de acces (AP).

În reţele fără fir cauza principală pentru scăderea numărului de apeluri este coliziunea. Evitarea pierderilor de pachete datorită acestui fapt se poate face dacă nu se lucrează în modul saturaţie când probabilitatea unor coliziuni este foarte mare în acest caz.

2.3. Protocoale utilizate la transmiterea vocii prin Internet

În prezent sunt utilizate mai multe protocoale menite să rezolve problemele de securitate [1], [2], [8]:

1. Confidenţialitatea echivalentă cu cea din reţelele cablate (Wired Equivalent Privacy-WEP);
2. Portul pentru control al accesului în reţelele fără fir care are înglobat Protocolul de Autentificare Extensibil (EAP);
3. Protocolul pentru Iniţializarea Sesiunii (SIP-Session Initiation Protocol);
4. Protocolul pentru Transport în Timp Real (Real Time Transport Protocol-RTP);
5. Protocolul H.323;
6. Protocolul Internet Securizat (IPsec) utilizat în reţelele cablate este de asemenea considerat ca alternativă pentru reţelele fără fir [2].

Aceste protocoale nu asigură identificarea corespunzătoare a participanţilor la apel, nu protejează confidenţialitatea şi integritatea datelor transmise şi recepţionate pentru iniţierea şi transmiterea apelurilor, respectiv datelor [14], [15], [21], [33], [34], [59].

Datorită faptului că protocoalele SIP şi RTP nu criptează apelul şi fluxurile de semnal audio (voce), atributele de identificare (nume/parolă) şi numerele de telefon SIP ale utilizatorilor pot fi interceptate prin LAN sau wireless LAN folosind programe de interceptare (sniffer-e) potrivit Cheriton şi Faria [21].

Un atacator poate oricând să folosească informaţiile sustrase pentru a contacta un reprezentant al furnizorului de servicii VoIP (prezentându-se drept utilizator legitim) sau pentru a accesa interfaţa de configurare web şi a modifica setările. În felul acesta poate efectua apeluri la numere cu taxare speciala sau în străinătate, poate accesa mesageria vocală a clientului sau poate schimba numărul de telefon spre care sunt direcţionate apelurile nepreluate. Furtul de identitate în aceste cazuri este folosit pentru a efectua apeluri costisitoare la mare distanţă sau pentru a obţine informaţii sensibile de natura financiară sau personală potrivit Agarwal [1], Wang, Lin, Liu [78].

Protocolul H.323 a fost cel mai răspândit şi utilizat protocol, însă datorită problemelor care apar la utilizarea lui între diferite reţele (rutare prin NAT, probleme cu firewall-uri, etc.), acest protocol a cedat primul loc protocolului SIP (Session Initiation Protocol). Protocolul SIP se adaptează mult mai bine cerinţelor şi problemelor diferiţilor utilizatori casnici, motiv pentru care se bucură de o răspândire tot mai largă. Protocolul H.323 este folosit acolo unde totul este sub control şi supraveghere, ca de exemplu în cadrul reţelelor de voce a diferitelor companii care furnizează servicii VoIP. În ultimul timp, îmbunătăţirile aduse protocolului H.323 (care de fapt este o umbrelă peste mai multe protocoale ca H.225.0, H.245, H.450, H.235, H.239), reduc problemele întâmpinate de H.323 la traversarea diferitelor reţele, ceea ce ar putea readuce utilizarea acestui protocol în prim plan, conform celor spuse de Kuhn [50] şi Wright [81].

2.4. Factori care afectează performanţa VoIP

Există mai mulţi factori majori care afectează calitatea serviciilor de voce transmise prin reţelele cu comutare de pachete. Aceştia sunt:

1. întârzierea;
2. latenţa întârziera dată de un pachet (funcţie de dimensiune) pentru a parcurge distanţa de la emiţător la receptor şi retur. ;
3. jitter-ul (întârzierea variabilă între pachete);
4. bruiajul;
5. limitări ale benzii de frecvenţă;
6. pierderea de pachete;
7. inundarea.

1. În sistemele VoIP întârzierea este dată în principal de timpii de prelucrare a semnalului: timpii de eşantionare, acumulare şi codare de la transmisie, apoi timpii de aşteptare în cozile ruterelor de pe traseu şi timpii de procesare la recepţie. Întârzierea între 2 puncte terminale (end-to-end) nu afectează în mod direct calitatea vocii, ci fluxul de date transmise, ducând astfel la suprapuneri ale convorbirilor. Recomandarea ITU-T G.114 [50] prevede limitări de timp pentru transmiterea într-o direcţie (one-way transmission time). Dacă întârzierea prin reţea este mai mică de 150 ms, utilizatorii nu vor fi afectaţi. Atunci când întârzierea este cuprinsă între 150 ms şi 400 ms, se percep întreruperi frecvente ale conversaţiei. Dacă întârzierea depăşeşte 400 ms conversaţia devine practic imposibilă [20], [22], [50].

Într-o reţea fără fir, utilizatorii concură pentru accesarea mediului de transport partajat. În timp ce legăturile (link-urile) se interferează reciproc, în timpul transmisiei, stratul de acces la mediu (MAC) trebuie să programeze cu atenţie accesarea acestora pentru ca pachetele să poată fi transmise cu coliziuni minime. Au fost studiate multe politici de planificare la nivelul substratului MAC, cu scopul de a maximiza productivitatea. Aceste sisteme sunt deseori numite scheme de programare pentru productivitatea optimă.

Pentru determinarea limitelor superioare şi inferioare ale întârzierii a fost propusă o schemă pentru estimarea exactă a întârzierii numită adaptarea maximă ponderată (Maximum Weighted Matching-MWM). În acest caz s-au luat în calcul reţele de tip ad-hoc cu un singur nod (hop). Gupta [29] a pornit de la premiza că pachetele sunt generate de o sursă externă şi a căutat reducerea cozilor de aşteptare pentru legături.

În reţelele fără fir s-au obţinut valori mari ale întârzierilor datorită interacţiunilor complexe dintre sosirea pachetelor, serviciile de reţea, up-link şi down-link. S-a demonstrat faptul că adaptarea ponderată maximă (MWM) este optimă în regim de trafic intens [29], [30], [49], [50]. Rezultatele nu oferă însă nici o estimare a întârzierii. De asemenea nu se ştie dacă aceste politici continuă să fie optime pentru o încărcare arbitrară.

Diverse modele de mobilitate au fost studiate în literatura de specialitate de Kuhn [50], Le Boudec [51], Lewis [52], Schulzrinne[69], pentru a determina relaţia între întârziere şi capacitate. Rezultatele indică faptul că există disensiuni între întârziere şi capacitate, iar natura acestor compromisuri este puternic influenţată de alegerea modelului de mobilitate.

Pentru a putea stabili un compromis între capacitate şi întârziere a fost introdusă noţiunea de întârziere critică. Scopul a fost de a se putea studia cât de mult trebuie să fie tolerată întârzierea pentru o anumită formă de mobilitate a nodului reţelei fără fir pentru a duce la îmbunătăţirea capacităţii acesteia. În literatură sunt propuse două clase diferite de modele de mobilitate şi s-a arătat că ambele prezintă întârzieri critice care sunt de fapt situaţii extreme. Întârzierea critică este invers proporţională cu lungimea căii caracteristice, care este definită ca distanţa între noduri. Aceste rezultate, oferă o înţelegere clară a motivului pentru care întârzierea critică este mai mare decât întârzierea critică aflată sub modelul punctului de mobilitate aleatoare. În realitate, este de aşteptat ca numărul de noduri sau densitatea de noduri să aibă o influenţă mică sau de loc asupra mişcării nodurilor. Corespunzător, ar fi de aşteptat ca şi lungimea caracteristică să aibă o dependenţă destul de slabă sau deloc asupra numărului de noduri sau densităţii acestora [29], [63], [71], [72], [76].

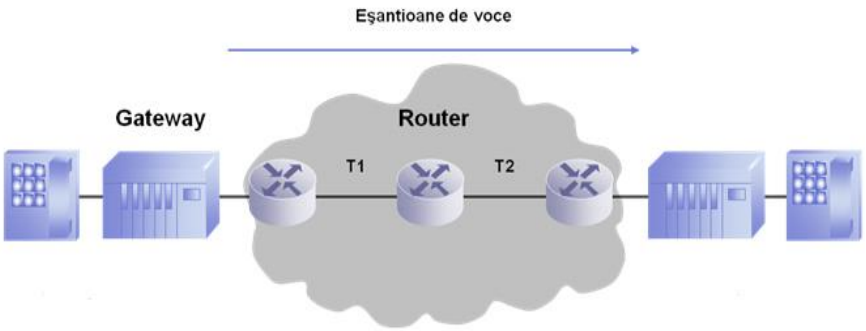


Fig.2.3 Punctele dintr-o reţea unde se produc întârzieri [50]

Întârzierile în reţelele VoIP se datorează algoritmilor de încapsulare a pachetelor, a serializării lor, a propagării lor prin reţea, a componentelor hardware ale reţelei, a aşteptării, retransmisiei şi a procesării în momentul recepţionării lor, Fig.2.3 [50]. De asemenea se poate observa din Fig.2.3 că şi multiplexările de la 1.544 Mbit/s (T1) la 6.312 Mbit/s (T2) sunt o posibilă sursă de întârzieri.

Prelucrarea semnalului analogic în formatul codec-ului utilizat se face pe blocuri a căror lungime poate varia între 10 ms şi 30 ms, în funcţie de codec-ul folosit. De exemplu, în cadrul codec-ului G.729 lungimea blocului este de 10 ms, faţă de cazul codec-ului G.723.1, care foloseşte lungimi de 30 ms. La blocuri mai mari de 30 ms, întârzierea introdusă de codec poate deveni sesizabilă şi chiar supărătoare la ascultător.

Wei Liu, Wenjing Lou, Yuguang Fang [79], au făcut o clasificare a întârzierilor din reţea în două mari categorii:

1. **întârzieri fixe**-din această categorie fac parte întârzierile codorului datorită prelucrării semnalelor pe cadre, întârzierile datorate împachetării informaţiei în pachete IP, (ţinând cont că un pachet poate conţine mai mult decât un cadru), întârzierile necesare compensării jitter-ului, întârzierea introdusă de decodor (mult mai mică decât cea introdusă de codor).
2. **întârzieri variabile**-din această categorie fac parte: întârzierea de propagare între nodurile reţelei, întârzierea datorată aşteptărilor în cozile de aşteptare a nodurilor reţelei şi întârzierile de comutaţie.

Întârzierile fixe nu sunt atât de periculoase ca şi cele variabile, cu toate că valoarea acestora este semnificativ mai mare decât a celor variabile, datorită faptului că o decalare a momentului de început al convorbirii, la ascultător, de câteva secunde, este insesizabilă. Pe de altă parte o variaţie a întârzierii cu câteva sutimi de secundă poate deveni deranjantă.

Dacă sunt cunoscute, întârzierile lanţului de comunicaţie pot fi controlate, iar dacă se ţine cont de aceste întârzieri în timpul proiectării reţelei şi aplicaţiilor, efectele acestora pot fi înlăturate sau micşorate până la limita observabilităţii.

2. Latenţa definită ca timpul necesar unui pachet de a ajunge la receptor şi înapoi la emiţător, este un alt factor generator de întârzieri. Este nevoie de mai putin de 150 ms de latenţă pentru o bună calitate, iar tipurile de conexiuni existente in prezent nu ating încă această medie. În cazul unei reţele VoIP, orice latenţă mai mare de 150-200 ms, un bruiaj mai mare de 20-40 milisecunde vor determina o rată de pierdere a pachetelor mai mare de 1-3%, afectând astfel calitatea semnalului vocal.

3. Jitter-ul este abaterea întârzierii (pozitivă sau negativă) la transmiterea pachetelor de voce. Apare în primul rând datorită modului de transfer al pachetelor pe diferite rute, fiind cauzat de cozile de aşteptare din nodurile reţelei şi de serializare.

Prin instituirea unor discipline de control a cozilor de aşteptare, prin prioritizarea pachetelor de voce, prin rezervarea benzii de frecvenţe şi prin dezvoltarea unor legături (link-uri) de mare viteză, cum ar fi SDH şi E3/T3 se poate controla jitter-ul îmbunătăţindu-se astfel calitatea serviciului (QoS).

Jitter-ul poate fi redus, prin utilizarea unor buffer-e la punctele terminale. Buffer–ele jitter-ului reţin astfel pachetele un timp suficient de lung pentru a permite şi celui mai lent pachet să ajungă la timp şi să poată fi reasamblat în ordinea corectă. Lungimea acestui buffer influenţează direct întârzierea dus-întors (deci mărimea bufferului nu poate fi foarte mare). De aceea jitterul trebuie să fie mic astfel încât redarea sunetului la recepţie să rămână lină.

4. Bruiajul apare datorită unor interferenţe nedorite ale semnalelor din banda de frecvenţă, producând întârzieri care pot varia foarte mult în reţelele fără fir. Dacă nivelul de bruiaj creşte dincolo de ceea ce un tampon de bruiaj este proiectat să suporte, semnalul audio va fi redat fără pachetele care nu au sosit. Astfel, rezultatele unui bruiaj excesiv pentru voce este similar cu cel ce afectează pierderea de pachete. Deoarece nu există nici o dimensiune maximă a buffer-ului tampon, nu poate fi specificat un nivel maxim de bruiaj pentru toate sistemele.

5. **Limitările de bandă** pot avea un efect sever asupra calităţii vocale într-un sistem [75]. Lăţimea de bandă, necesară pentru transmisia de voce într-o reţea IP depinde de codec-ul audio folosit. În plus, faţă de informaţiile de voce, diverse informaţii din antet cresc cerinţele de lăţime de bandă [33], [34], [35], [75].

Codec-ul ITU-T G.711, denumit PCM, este cel mai frecvent codec utilizat în prezent de sistemele telefonice. Există două variante ale metodelor de codificare: μ-law, utilizate în SUA şi în Japonia şi a-law utilizat în celelalte ţări. Fiecare din aceste metode transmit 8000 de eşantioane pe secundă, ceea ce înseamnă că un total de 64000 biţi pot fi transmiși pe secundă. Prin urmare, pentru a transmite semnal vocal codat digital, se folosește codec-ul G.711, cu o lăţime de bandă disponibilă de 64 kbps. În utilizarea reală există o încărcare suplimentară, în afară de traficul de voce, ceea ce duce la o lăţime de bandă reală utilizată de 87.2 kbps. Această lăţime de bandă este utilizată în ambele direcţii. Aceasta înseamnă că un minim de 128 Kbps pe canalul este necesar pentru acest codec să funcţioneze normal.

6. Pierderea de pachete se răsfrânge are de asemenea un efect negativ asupra calităţii vocii recepţionate. Un procent relativ scăzut (5-10%) al pachetelor de date pierdute va provoca o scădere a calităţii vocii. În cazul în care procentul de pierderi de pachete se ridică la 10 %, calitatea va deveni inacceptabilă [33], [64]. Pierderea pachetelor trebuie să fie mică, deoarece fluxul de voce este sensibil la pierderea de pachete (pierderea unor pachete duce la pierderea unor bucăţi din semnalul primit de la microfonului transmiţătorului şi astfel redarea la recepţie se face cu întreruperi.) Din păcate pierderea de pachete în reţelele IP este corelată, deoarece pierderile apar în timpul congestiilor şi aceste pierderi continue de pachete reduc substanţial inteligibilitatea vocii.

7. Inundarea este o tehnică ce permite unui atacator să trimită un număr mare de pachete, pe care ţinta le acceptă şi încearcă să le proceseze, întârzie sau să întrerupă traficul, rezultând astfel refuzul serviciului (Denial of Service-DoS).

Primul pas într-o încercare reuşită de a ataca o reţea VoIP este colectarea de informaţii şi profile. După descoperirea dispozitivelor SIP prezente în reţea, prin scanare, enumerare şi amprentare, se pot face o varietate de teste de securitate cum ar fi: inundarea UDP cu mesaje de tip INVITE pentru a ataca sesiunea, a intercepta traficul sau a asculta [52], [53].

Colectarea de informaţii se poate face prin detectarea online a gazdelor, iar apoi se determină care dintre ele utilizează protocolul SIP.

Toate protocoalele SIP suportă protocoale de tip datagramă (User Datagram Protocol-UDP), astfel că atacurile de inundare prin intermediul acestui protocol au o probabilitate ridicată de apariţie. Inundarea se face prin solicitările de mesaje INVITE ulterioare, astfel că SIP va interpreta fiecare dintre ele ca apeluri independente şi va iniţia un dialog pentru fiecare. Deoarece este un atac specific SIP, inundarea prin mesaje INVITE se consideră o metodă de atac la nivel de sesiune şi aplicaţie [1], [60].

Manipularea semnalizărilor SIP poate duce la unele forme foarte periculoase de încălcare a securităţii. Un atacator poate folosi astfel mesaje de înregistrare false (REGISTER), putând adăuga sau substitui utilizatori falşi. În SIP, cererile de mesaje BYE trimise între telefoane SIP anunţă terminarea convorbirii. Dacă un atacator va trimite un mesaj de BYE unui telefon SIP angajat într-o conversaţie, acesta va determina întreruperea ei imediată [3], [5].

Protocoalele SIP sunt vulnerabile de asemenea la atacuri de tip media în timp real, mesajele audio se pot insera în convorbiri şi pot fi ascultate simultan de mai mulţi utilizatori de telefoane SIP.

Mediul SIP este vulnerabil de asemenea la atacuri de interceptare. Fluxul de date poate fi interceptat în timp real şi pot fi extrase informaţiile audio (eavesdropping).

Inundare (flood) reţelelor VoIP cu mesaje SIP (prin simularea diverselor faze ale apelurilor de iniţiere, încheiere sau transmiterea de fluxuri de date media RTP) poate diminua calitatea serviciului, poate provoca întreruperea apelurilor sau poate forţa echipamentele să nu mai proceseze toate apelurile primite.

Echipamentele VoIP sunt de asemenea vulnerabile la atacuri de tip TCP-SYN sau ping-ul morţii, un tip de comenzi ping modificate în scopul de a compromite conversaţia (Ping of Death) [52].

Sistemele de operare şi comunicaţiile TCP/IP folosite de echipamentele VoIP sunt vulnerabile la atacuri ce vizează încetarea funcţionării lor sau preluarea controlului de la distanţă.

Transmiterea şi execuţia de instrucţiuni modificate de diverşi intruşi, prin intermediul aplicaţiilor softphone, pot afecta calculatoarele şi dispozitivele mobile (laptop, PDA) pe care acestea sunt instalate. Prin trimiterea de mesaje nesolicitate (spam) de multe ori sunt transmise aplicaţii de spionare (spyware) sau de control de la distanţa sau mesaje de publicitate nedorite [77].

Algoritmii de criptare, interferenţa frecvenţelor radio (RFI) şi limitările de infrastructură influenţează şi ei calitatea vocii în reţelele fără fir, Wu & Co [81].

2.5. Straturile protocolului VoIP

Reţelele IP care transmit pachetele de voce ca datagrame, sunt tot mai des utilizate ca o alternativă la reţeaua clasică de telefonie. Deoarece conversaţiile private sunt efectuate prin reţele publice nesigure, securitatea comunicaţiilor VoIP este tot mai importantă. În [16], se prezintă componentele stivei protocolului cu ajutorul căruia se transmite vocea prin Internet. Ele sunt:

1. Protocolul pentru Iniţializarea Sesiunii (SIP-Session Initiation Protocol SIP);
2. protocolul pentru descrierea sesiunii (SDP);
3. cheia de criptare (SDES, Mikey şi ZRTP);
4. protocolul de securitate pentru transportul în timp real (SRTP) Fig.2.4 [30].

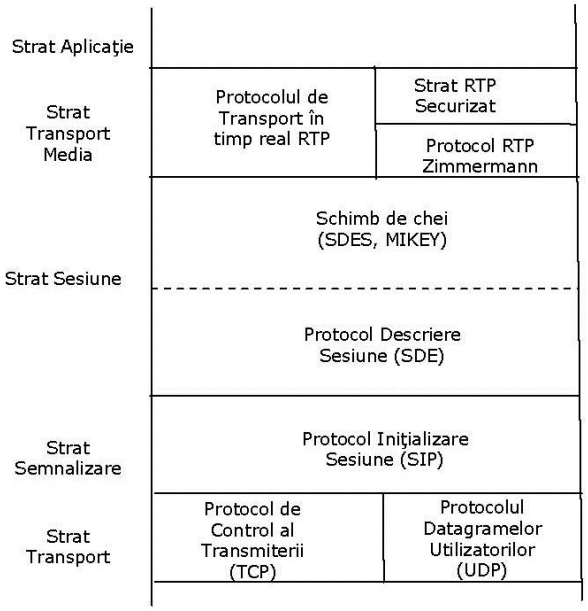


Fig.2.4. Setul de protocoale implicate în transmiterea vocii prin Internet [30]

Majoritatea breşelor de securitate ale stivei protocolului VoIP sunt cauzate de faptul că între protocoalele din diferitele straturi ale stivei nu se transmit informaţii suficiente referitoare la starea lor [14].

Traficul de media este transportat de către mai puţin sigurul protocol UDP şi include 2 protocoale definite de ITU-T în RFC 1889: Protocolul în timp real-RTP (Real Time Protocol) care transportă chiar informaţia şi protocolul de control în timp real-RTCP (Real Time Control Protocol) care transmite mesaje periodice de control şi de stare. Informaţia este transportată de protocolul UDP deoarece nu ar avea sens să fie retransmisă (aşa cum ar proceda TCP de exemplu). Dacă un fragment de sunet, pierdut, ar fi retransmis, probabil ar ajunge prea târziu şi nu ar mai putea fi folosit la reconstruirea vocii. Mesajele RTP sunt transmise prin porturile UDP impare, iar cele RTCP prin cele pare, imediat alăturate.

RTCP permite schimbul periodic de informaţie între participanţi privind calitatea legăturii şi se foloseşte pentru detecţia şi eventual corecţia erorilor care apar pe parcursul convorbirii.

2.6. Tipuri de atacuri asupra SIP

Refuzul Serviciului (Denial of Service-DoS). Acest tip de atac se focalizează pe transmiterea ca indisponibil a unui anumit serviciu de reţea, de obicei direcţionând spre el un volum mare de trafic. Prin aceasta clienţii legitimi îşi pierd încrederea în el. Un refuz al unui serviciu distribuit permite unui singur utilizator să provoace inundarea gazdelor ţintă de către reţele gazdă multiple, Herculea [55].

Arhitectura SIP permite deosebit de uşor distribuţia unui serviciu de tipul DoS. Un atacator poate pune adresa IP a victimei în antetul unui router de mani-

pulare (spoofed Router) care o trimite apoi unor routere intermediare de bifurcare (forking proxies), amplificând astfel numărul de mesaje returnate către victimă.

Reflecţia este o altă modalitate de a refuza un serviciu. Un atacator poate trimite cereri modificate (spoofed request) de la un număr mare de elemente SIP şi servere intermediare (proxy-uri), punând adresa IP a victimei în câmpul sursă. Fiecare dintre beneficiari va genera un răspuns, copleşind astfel victima [55].

O protecţie limitată împotriva solicitărilor SIP falsificate poate fi asigurată de IPsec. Implementarea IPsec end-to-end, într-un mediu tipic VoIP, unde punctele finale sunt dinamice nu este încă bine pusă la punct. Nu reiese clar din specificaţiile pentru protocolul SIP modul de inter-operare cu protocolul IPsec [1], [2], [26], [27], [48], [55], [65].

Autentificarea şi autorizarea sunt alte vulnerabilităţi importante în SIP. Cererile BYE, de terminare sesiune, nu sunt autentificate, până nu sunt confirmate. În schimb, o cerere BYE este implicit autentificată în cazul în care este primită de la acelaşi element de reţea (pe aceeaşi cale) ca şi cererea de INVITE anterioară. Un atacator poate determina, prin ascultare, (eavesdropping), parametrii unui mesaj INVITE şi apoi poate introduce o cerere de BYE în sesiune. Odată ce, cererea BYE este primită de către ţintă, sesiunea se va termina. Atacuri asemănătoare pot fi lansate şi pentru mesajele de re-INVITE utilizate pentru schimbarea parametrilor sesiunii [30].

O mare varietate de atacuri de negare a serviciului, pot fi posibile în cazul în care cererile de înregistrare nu sunt autentificate şi autorizate de către server-ul de înregistrare. Dacă un utilizator rău intenţionat este capabil să anuleze o parte sau pe toţi ceilalţi utilizatori din reţea şi să îşi înregistreze propriul dispozitiv în numele lor, el poate refuza cu uşurinţă accesul oricăruia dintre acei utilizatori/servicii. Atacatorii pot încerca de asemenea, să epuizeze resursele de stocare ale server-ului de înregistrare prin crearea unui număr foarte mare de legături [30], [76], [77].

Autentificarea este destul de dificil de realizat în cazul protocolului SIP, deoarece sunt un număr de elemente intermediare cum ar fi server-ele proxy care pot modifica conţinutul unui mesaj înainte ca acesta să ajungă la destinaţie. Toate aceste elemente intermediare trebuie securizate potrivit Gupta, [30].

Înregistrările SIP nu cer câmpului **From Field** al unui mesaj să fie la fel ca şi antetul header-ului cîmpului **TO** al cererii, permiţând astfel unei a treia părţi să schimbe, în numele altui utilizator, adresa ataşată înregistrării.

În cazul în care atacatorul poate modifica utilizatorii, în numele unuia autorizat, fără a fi identificat, el poate modifica astfel, în mod arbitrar, adresa înregistrărilor asociate câmpului TO al mesajului SIP. Deoarece autentificarea SIP se bazează pe autentificarea server-ului şi a celor intermediare (proxy), atacatorul, dacă nu este depistat la timp, poate produce daune arbitrare, inclusiv refuzul serviciului pentru client sau lansarea unui atac de tipul refuzului de servicii distribuite. Acest lucru necesită existenţa unor metodologii de autentificare a server-ului şi/sau proxy-urilor pentru clienţi. Din păcate în documentaţia RFC (Request for Comment) pentru SIP nu e specificat nici un mecanism în acest sens.

SIP este o platformă foarte accesibilă şi prin definiţie deschisă pentru toată lumea, fiind un protocol al cărui potenţial poate fi uşor exploatat de către operatorii de botnet (colecţie software, de cele mai multe ori asociat cu cel al atacatorilor) [8]. În ansamblu, dezvoltarea unei aplicaţii SIP de tipul botnet este greu de depistat. În cel mai rău caz poate fi detectată de către sistemele de protecţie ca un atac prin inundare [8].

Omul în mijlocul atacului (Man in the Middle Attack MitM) este un alt tip de ameninţare. Atacatorul sau o persoană nedorită poate trage cu urechea la conversaţie [14], [15]. Un atac de acest tip asupra protocolului în timp real-RTP, permite

ataca-torului să convingă părţile care comunică că au pierdut cheia secretă comună. Dacă sunt folosite dispozitive VoIP fără ecran de afişare nu se poate executa autentificarea "umană", acestea fiind obligate să comunice nesecurizat sau să nu comunice de loc. Astfel apare un atac de negare al serviciului (DoS) [30].

Repudierea este într-un fel similară cu modificarea atacului deoarece ambele afectează integritatea şi responsabilitatea sistemului. Repudierea se produce atunci când cineva declină faptul că s-a întâmplat ceva sau trimite informaţii falsificate despre ce s-a întâmplat [13], [14].

2.7 Mecanisme de securitate

Reţelele fără fir sunt relativ mai puţin sigure decât cele cablate, datorită accesului mai facil la reţea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. Există implicit în implementarea reţelelor fără fir diferite bariere care formează aşa numita securitate de bază a reţelelor fără fir şi care împiedică accesul neintenţionat al persoanelor străine de reţea, aflate în aria de acoperire a unui punct de acces. Barierele de securitate (securitatea de bază) care au fost prevăzute în protocoalele reţelelor fără fir (Wireless Fidelity-Wi-Fi) asigură un nivel relativ scăzut al securităţii acestor reţele, ceea ce le-a frânat întrucâtva dezvoltarea. Securitatea de bază a acestor reţelelor este asigurată de următoarele funcţii implementate:

1. Identificatori ai Setul de Servicii (Service Set Identifiers-SSID);
2. Confidenţialitatea echivalentă cu cea din reţelele cablate (Wired Equivalent Privacy-WEP);
3. Verificarea adresei controlului de acces la mediu (Media Acces Control-MAC).

Toate dispozitivele fără fir (wireless) care vor să comunice într-o reţea trebuie să aibă un identificator propriu (SSID), setat la aceeaşi valoare cu valoarea identificatorului (SSID) punctului de acces, pentru a se realiza conectivitatea. În mod normal un punct de acces îşi transmite identificatorul (SSID-ul) la fiecare câteva secunde. Acest mod de lucru poate fi stopat, astfel încât o persoană neautorizată să nu poată descoperi automat SSID-ul şi punctul de acces. SSID-ul este inclus în pachetele de date transmise continuu de un punct de acces pentru a-şi face cunoscută prezenţa şi pentru a asigura managementul reţelei (beacon-ul). Astfel este uşor pentru un hacker dotat cu echipament de monitorizare să-i descopere valoarea SSID-ului şi să se lege în reţea [46], [47].

Algoritmul de securitate al standardului IEEE 802.11, confidenţialitatea echivalentă cu cea din reţelele cablate-WEP, poate fi folosit pentru a ameliora problema transmiterii continue a SSID-ului prin criptarea traficului dintre clienţii reţelelor fără fir şi punctul de acces. Se realizează prin aceasta o autentificare printr-o cheie partajată (shared-key authentication). Punctul de acces transmite clientului wireless o provocare pe care acesta trebuie s-o returneze criptată. Dacă punctul de acces poate decripta răspunsul clientului, are dovada că acesta posedă cheia validă şi are dreptul de a intra în reţea. WEP dispune de două posibilităţi de criptare-cu cheie de 64 de biţi sau de 128 de biţi.

Desigur, WEP nu asigură o securitate prea mare. Hacker-ul dotat cu echipament de monitorizare poate recepţiona şi înregistra întâi provocarea plecată de la punctul de acces apoi răspunsul criptat al clientului şi pe baza unor procesări se poate determina cheia pe care apoi o poate folosi pentru a intra în reţea.

Verificarea adresei plăcilor de reţea, MAC, poate spori securitatea reţelei, dacă administratorul de reţea utilizează filtrarea adreselor MAC, adică punctul de acces este configurat cu adresele MAC ale clienţilor cărora le este permis accesul în reţea.

Din nefericire, nici această metodă nu asigură o securitate prea mare. Un hacker poate să înregistreze secvenţe din trafic şi în urma unor analize, poate să extragă o adresă MAC pe care ulterior o poate folosi pentru a intra în reţea [49].

Comunitatea internaţională Internet Engineering Task Force-IETF a sugerat unele mecanisme, bazate fie pe HTTP Digest sau S/MIME (Secure/Multipurpose Internet Mail Extensions) pentru asigurarea unei securităţi selective la nivelul protocolului SIP. Ambele mecanisme nu garantează însă un nivel ridicat al acestuia, doar primul prevede un mecanism de autentificare pentru agentul utilizator (User Agent) atât în faza de înregistrare (spre un proxy) cât şi în faza de comunicare (faţă de un alt User Agent) [14], [25].

O altă soluţie interesantă propusă de IETF, se bazează pe provocarea/răspunsul protocolului de autentificare RADIUS (Remote Authetication Dial In User Service), care este folosit frecvent de către numeroşi furnizori de servicii Internet (ISP). Un server RADIUS este un al treilea element de încredere (Third Trusted Party) pentru toate componentele SIP care se autentifică reciproc înainte şi în timpul unei sesiuni SIP datorită unor secrete împărtăşite cu server-ul RADIUS. Acesta are rolul de gestiune a lor (ar putea fi considerat ca un centru de management al cheilor, o cale de altfel comună pentru a face faţă securităţii în infrastructurile distribuite) [14].

RADIUS este mai uşor de utilizat, foloseşte mecanisme mai simple pentru schimbul de parole ale utilizatorilor sau pentru parola de autentificare. Utilizează pentru criptarea mesajelor algoritmul de criptare MD5 [10]. Mai sunt şi alte alternative, cum ar fi utilizarea mecanismului Kerberos bazat pe Infrastructura de chei publice (Public Key Infrastructure-PKI), pentru furnizarea securităţii end-to-end clienţilor SIP. Odată ce clientul este autentificat şi cheia Kerberos este generată, clienţii SIP pot utiliza cheia furnizată pentru criptarea şi autentificarea unuia cu altul [14].

Pentru transmiterea în timp real a datelor, audio sau video, este utilizat de obicei protocolul de transmisie în timp real RTP, considerat a fi nesigur. O soluţie mai bună, este utilizarea variantei securizate, SRTP (Secure-RTP), pentru a face ca protocolul de transport în timp real (RTP) şi protocolul de control al transportului în timp real (RTCP) să fie mai sigure prin criptarea şi autentificarea fluxurilor şi furnizarea de mesaje de autentificare securizate. SRTP este foarte flexibil şi nu depinde de modul de gestionare al cheilor. Standardul avansat pentru criptare-AES (Advance Encriptyon Standard) este algoritmul utilizat implicit pentru criptare având cheia de criptare pe 128 de biţi [13], [67].

2.7.1 Asigurarea securităţii SIP în sistemele multimedia implementate sub diverse sisteme de operare

Analiza influenţei măsurilor de securitate asupra diverselor sisteme de operare Windows (Server 2003, Windows XP şi Windows Vista), Linux şi Unix, care rulează în reţelele fără fir este studiată în Kolahi & Co, [49]. S-au folosit diverse tehnici de criptare (WEP-64, WEP şi WPA-128), pentru ambele protocoale TCP şi UDP. Capacitatea de transfer şi timpul de răspuns sunt doi parametri influenţaţi de mecanismele de securitate implementate [61], [62].

Fig.2.5 prezintă arhitectura unei reţele fără fir folosite pentru teste de invadare în două situaţii: când receptorul este în furcă, poziţia on hook şi după ce s-a terminat o convorbire. Este o schemă obişnuită pentru diverse simulări în reţele fără fir.

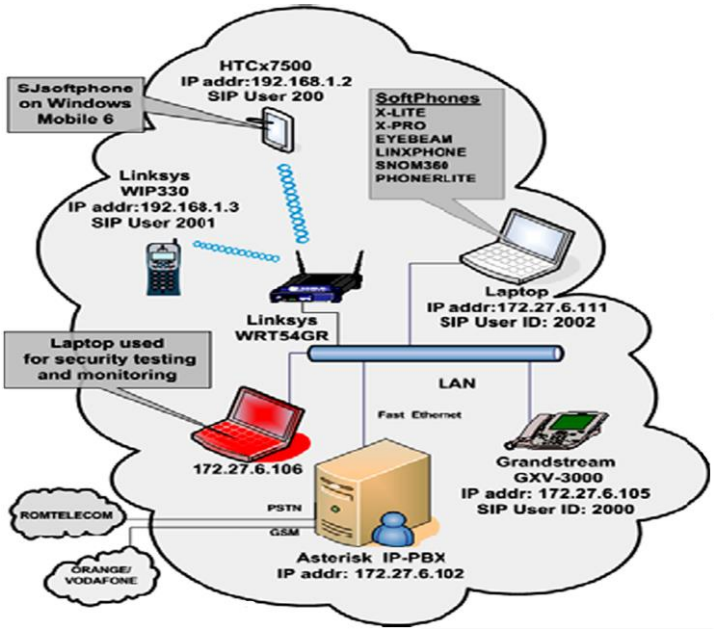


Fig.2.5. Arhitectură testare reţea fără fir [54]

Cu ajutorul programului de test, Wireshark, pachetele RTP au fost interceptate şi apoi procesate pentru a se extrage datele audio transmise între cele două puncte finale. Această metodă este utilă doar în cazul în care atacatorul are acces la reţea. Parametrii SRTP (chei de criptare, chei de autentificare) sunt trimişi prin mesaje INVITE cu mesaje de semnalizare SDP (Protocol Descriere Sesiune). Pentru Asterisk se poate instala un modul care conţine protocolul SRTP şi care va fi plasat în calea fluxului de comunicare mass-media, între clienţii SIP, ca nod intermediar [55].

Etapa de evaluare a securităţii a relevat faptul că cele mai periculoase atacuri sunt la nivelul aplicaţiilor. Inundarea cu mesaje de tip INVITE s-a dovedit devastatoare pentru clienţii SIP, precum şi pentru Asterisk, ducând la refuzul serviciului, DoS. Testarea reţelei bazate pe SIP are şi alte avantaje, deoarece furnizează informaţii despre terminalele care sunt cele mai fiabile în timpul atacurilor.

Utilizarea SRTP pentru traficul mass-media a îmbunătăţit problema confidenţialităţii, dar nu a rezolvat-o în totalitate. Un canal securizat de comunicare pentru semnalizare (cum ar fi TLS) este necesară. Programul Snort, un program ce oferă posibilitatea depistării intruşilor la nivel de reţea, oferă o îmbunătăţire a securităţii pentru alertarea sau blocarea unor tipuri de atacuri, în timp ce un număr de probleme rămân în continuare nesoluţionate (probleme cum ar fi alarmele false). Testele au arătat că mesajele SIP ilegale sunt greu de detectat datorită asemănării lor cu cele legitime. Soluţiile propuse reuşesc să ridice nivelul de securitate pentru arhitecturile SIP, dar nici una dintre tehnologii, instrumente sau metode utilizate nu oferă o soluţie completă.

Performanţele capacităţii de transfer a datelor şi întârzierea datorată traseului parcurs de semnal de la sursă la destinaţie şi înapoi (round trip time-RTT) depind de tehnica de criptare folosită, în special pentru cheia secretă similară cu cea din reţelele fixe (Wired Equivalent Privacy-WEP). După cum se ştie WEP adaugă valoarea iniţială

a cheii simetrice de criptare la datele pe care urmează să le trimită şi utilizează restul de biţi ai cheii pentru a iniţia un algoritm care să genereze un flux de chei pentru fluxul de date ce urmează a fi codificat şi trimis. Ca rezultat, WEP introduce o oarecare întârziere pentru trimiterea/primirea datelor şi pentru criptarea/decriptarea lor [81], [82], [83].

Testele au scos în evidenţă faptul că Windows Vista, nu are performanţe mai bune în ceea ce priveşte lăţimea de bandă şi timpul de răspuns dus-întors (Round Trip Time-RTT), faţă de predecesorii săi. Utilizarea algoritmului de criptare WEP-128 a avut cel mai mare impact pentru Windows Server 2003, în timp ce pentru Windows XP sau Vista a fost nesemnificativ. Windows 2003 a înregistrat cea mai mare lăţime de bandă, pentru atât TCP şi UDP, în toate sistemele de criptare studiate.

Pentru a face schimbări minime la infrastructura reţelelor fără fir existente, unele firme folosesc arhitectura reţelei cu translaţia inversă a adresei (RAT-Reverse Address Translation), utilizând adresa de translaţie reţea (Network Address Translation-NAT) [81]. În astfel de arhitecturi, un nod mobil se înregistrează la server-ul de înregistrare din reţeaua de domiciliu, după care se mută în reţeaua străină. Server-ul de înregistrare la rândul său, notifică dispozitivul RAT din reţeaua de domiciliu, care este responsabil pentru redirecţionarea pachetelor între nodul corespondent şi nodul mobil. Deoarece RAT este propusă ca o soluţie de tranziţie pentru migrarea către protocolul IP mobil, protocolul mesajelor RAT respectă protocolul IP mobil. Spre deosebire de metoda clasică de abordare unde nodul mobil trebuie să trimită în mod explicit un mesaj de înregistrare la server-ul din reţeaua de domiciliu, după schimbarea adresei IP, în [82], Wu&Co propune o arhitectură prin care mobilitatea nodului este detectată automat. Detecţia se face de către server-ul proxy, prin interceptarea mesajelor de atribuire adresă nodului mobil, de către protocolul de atribuire dinamică a adresei (Dynamic Host Configuration Protocol-DHCP). Acest prototip de arhitectură a fost propus în [81] pentru sprijinirea mobilităţii IP în campusurile universitare, centrele comerciale, etc. Într-o astfel de arhitectură de reţea timpul de întârziere este de aproximativ 1s. Acest lucru permite asigurarea unor servicii de calitate (Quality of Service QoS) unor aplicaţii sensibile la întârzieri cum ar fi VoIP şi aplicaţii multimedia.

Subsistemele IP multimedia (IMS) sunt considerate a fi principala soluţie pentru următoarea generaţie de comunicaţii multimedia. În [77] este prezentat un studiu al acestor subsisteme bazate de cozi de aşteptare Petri. Este un studiu pentru introducerea partiţiei de securitate cu examinări multiple (multi-view security partition) prin care se pot asigura servicii de securitate multistrat diverşilor utilizatori şi diverselor aplicaţii, asigurându-se cel mai bun compromis între cerinţele de securitate şi performanţele sistemelor [77].

În [17] este descrisă o implementare practică a securităţii VoIP utilizând Java şi sistemul de operare pentru dispozitive mobile Android. Au fost efectuate teste utilizând atât protocolul SIP cât şi H.323. Protocolul de semnalizare H.323 a fost creat pentru reţele LAN (Local Area Network) şi nu suportă un număr mare de adrese. Protocolul de semnalizare SIP, conceput pentru reţele de WAN (Wide Area Network), are capabilitatea unui număr mai mare de adrese. Din acest punct de vedere SIP este considerat mult mai scalabil decât H.323.

2.8 Soluţii de îmbunătăţire a calităţii transmisiei vocii prin reţelele fără fir propuse în cadrul tezei de doctorat

Soluţiile de îmbunătăţire a calităţii transmisiei în reţelele fără fir, propuse în această teză, se referă la cazul particular al aplicaţiilor de **transmitere a vocii prin Internet (VoIP)**. Am pornit de la faptul că până acum, în literatura de specialitate, s-a acordat o atenţie mult mai mare studiilor legate de asigurarea calităţii semnalului vocal şi în mai mică măsură reducerii timpului de iniţializare a sesiunii unui apel vocal VoIP transmis în reţelele fără fir. În lucrarea [38] eu am analizat factori precum întârzierile, pierderea pachetelor şi încărcarea server-elor SIP, în vederea optimizării întârzierilor sesiunii de iniţializare în reţelele fără fir. În prezent, sunt utilizate pentru semnalizarea sesiunii de iniţializare a unui apel vocal mai multe protocoale cum ar fi H.323, SIP, IAX. Spre deosebire de protocolul H.323, protocolul SIP este definit numai pentru reţele care utilizează protocolul Internet (IP). **În teza de doctorat am propus o soluţie nouă de optimizare a întârzierilor sesiunii de iniţializare a unui apel vocal prin Internet. Soluţia constă în realizarea şi implementarea unui contor adaptiv pentru retransmiterea datelor. Are rolul de ajustare, funcţie de timp, a tranzacţiilor SIP efectuate pentru iniţierea unei convorbiri. Soluţia este prezentată în capitolul 3, paragrafele 3.3 şi 3.4**. Tot în scopul reducerii întârzierilor din sesiunea de iniţialzare a unui apel vocal am studiat şi modalitatea optimă de transport a datelor. **În capitolul 3, paragrafele 3.3.2-3.3.5, am făcut un studiu comparativ al întârzierilor din sesiunea de iniţializare utilizând mai multe variante de transport a protocolului pentru iniţializarea sesiunii SIP: prin intermediul protocolului de control a transmisiei-TCP (Transmission Control Protocol), a protocolului utilizatorilor de datagrame-UDP (User Datagram Protocol) şi a protocolului legăturii prin unde radio-RLP (Radio Link Protocol)**. Pentru protocolul legăturii prin unde radio am luat în considerare două scheme RLP (1,1,1,1,1,1) şi RLP (1,2,3), pentru a determina care oferă cei mai buni timpi de transmisie. Factorii de care am ţinut cont sunt rata de eroare a cadrelor (FER), aferentă legăturii aeriene şi cozile de aşteptare a pachetelor, datorită încărcării diferite a server-elor SIP implicate în transferul acestora. Am calculat timpii de răspuns şi procentul cadrelor eronate care nu trebuie să depăşească 3%. Varianta cea mai bună pentru transport este cea prin intermediul protocolului RLP, bazat pe schema RLP(1,2,3) Contorul de timp are rolul de a ajusta mărimea pachetelor de semnalizare implicate în stabilirea sesiunii de iniţializare apel vocal, astfel încât să se reducă dimensiunea cozilor de aşteptare. Tot în scopul reducerii timpului aferent iniţializării sesiunii, se pot utiliza suplimentar algoritmi de comprimare a mesajelor SIP. Din păcate mesajul de INVITE al protocolului SIP, prin care se iniţiază o sesiune nu poate fi comprimat mai mult de 9%.

O abordare din alt punct de vedere a îmbunătăţirii calităţii transmisiei vocii prin reţelele fără fir, bazate pe standardul IEEE 802.11, este reducerea timpului de transmitere a datelor prin controlul numărului de apeluri admise în lista de interogare a punctelor de acces (AP). Substratul de control al accesului la mediu (Media Access Control-MAC), al standardului IEEE 802.11, are definite două funcţii de control, una de coordonare distribuită şi alta de coordonare prin punct. Am analizat capacitatea funcţiei de coordonare prin punct (PCF) de a suporta traficul de voce, datorită faptului că transmisia în acest caz se realizează prin comutarea de pachete. Acest fapt ar permite multiplexarea între ele a fragmentelor vocale, provenite de la convorbiri diferite, datorită perioadelor de pauză dintr-o convorbire. **Spre deosebire de alte publicaţii, în care s-au prezentat doar rezultatele simulărilor efectuate pentru**

optimizarea modului de interogare a staţiilor din lista ataşată punctului de acces, în teză am făcut o analiză a interogărilor şi am indicat modul în care trebuiesc setaţi parametrii pentru a suporta apeluri vocale. Descrierea analizei şi simulările au dus la concluzia că cel mai simplu mod de transfer al datelor, în modul de funcţionare cu coordonare prin puncte de acces, este cel cu rata de transfer constantă (Contant Bit Rate-CBR). În capitolul 3, paragrafele 3.5-3.7 am descris analitic şi am experimentat un nou algoritm, care să monitorizeze numărul maxim de apeluri admise în listă, pentru a evita coliziunile şi a asigura o întârziere garantată a reţelei care să fie luată în considerare la receptor.

La subnivelul controlului de acces la mediu (MAC-Medium Access Control) al standardului IEEE 802.11 sunt necesare retransmiteri ale pachetelor, pentru a putea acoperi erorile de transmisie ale celor două funcţii ale standardului IEEE 802.11 de coordonare prin punct (PFC) şi coordonare distribuită (DCF). În mod normal retransmiterile trebuiesc evitate pentru traficul în timp real datorită întârzierilor pe care le implică. **Datorită acestor retransmiteri am făcut un studiu, capitolul 3, paragraful 3.7,care a indică necesitatea corecţiei erorilor pentru traficul de voce. Am luat în calcul trei cazuri posibile legate de starea canalului la transmiterea unui pachet de voce şi de tranziţiile din timpul transmisiei. Experimentele au arătat că erorile sunt mari de 10^{-3}, deci ce impune necesitatea corecţiei lor.**

Lucrarea [37] conţine un studiu experimental al întârzierilor în reţelele fără fir, pentru situaţia utilizării controlului pentru accesul la mediu cu distribuţie multiplă (multicasting) în reţelele fără fir**. Trimiterea unui apel vocal spre mai mulţi utilizatori în reţelele fără fir a fost mai puţin studiată. Studiul, prezentat în teză, în capitolul 4, paragrafele 4.5-4.9, arată că pentru astfel de situaţii rata maximă de transfer care poate fi atinsă este de 1.78 Mbps, pentru reţele cu trafic de 2 Mbps. Experimentele arată că, deşi traficul VoIP tolerează unele pierderi, distribuţia multiplă poate, în general, să fie utilizată în reţelele fără fir bazate pe standardul IEEE 802.11 numai dacă vor fi implementate mecanisme suplimentare în straturile superioare ale reţelei pentru a atenua pierderile de cadre de la nivelul MAC.**

Standardul IEEE 802.11 oferă suport limitat de confidenţialitate, prin utilizarea protocolului Wired Equivalent Privacy (WEP), care nu a fost conceput să fie singurul mecanism de securitate din reţelele fără fir ci în asociere cu altele să asigure protecţia reţelelor fără fir [40], [41]. Multe din organizaţiile care utilizează reţelele fără fir folosesc fie un sistem criptografic cu o variabilă permanentă fixă sau o cheie de criptare sau nici un fel de criptare (util pentru destinaţii multiple când se face numai autentificarea).

Securitatea transmisiei datelor, deci implicit şi a vocii, în reţelele fără fir, este un alt parametru care trebuie asigurat pentru a îmbunătăţi calitatea unei convorbiri ce foloseşte ca infrastructură Internet-ul [40], [41], [42], [44]. **În teza de doctorat am pornit de la analizele efectuate în lucrările [40], [41], [44] şi am propus o nouă soluţie de securitate bazată pe conceptul de client-server.** Am făcut o comparaţie între protocoalele cel mai des utilizate în transmisiile VoIP: H.323, SIP şi IAX. **Am optat pentru IAX deoarece este un protocol de tip open source dedicat semnalizării, uşor de utilizat şi modificat. Prezintă avantajul că foloseşte lăţime de bandă minimă atât pentru transferul datelor cât şi pentru semnalizare şi are suport nativ pentru translatarea adreselor de reţea**. **În capitolul 4, paragraful 4.4 este prezentată propunerea mea pentru un client VoIP securizat, care utilizează protocolul de semnalizare IAX.** Pentru testare am folosit

un laptop. Utilizarea toolkit-ului Cryptlib a permis experimentarea diferitelor metode de criptare. Kiax este un telefon soft ce dispune de o interfaţă grafică, prin intermediul căreia am putut modifica setările. Am putut astfel modifica nucleul de securitate al protocolului IAX prin adăugarea unei etape suplimentare de codificare, criptare şi încapsulare a datelor înainte de a fi trimise, urmând ca la receptor ele să fie decodate. Prototipul care a fost creat pentru client poate fi utilizat cu succes în orice aplicaţie VoIP.

Un mecanism des folosit pentru a furniza securitate este şi utilizarea listelor de control al accesului pe baza adresei Ethernet a plăcii de reţea a clientului (MAC) [41]. Fiecare punct de acces poate limita clienţii reţelei la cei enumeraţi în listă. Dacă un client are adresa plăcii de reţea (MAC) pe listă, acesta are acces la reţea. Dacă adresa nu se regăseşte în listă, accesul la reţea este împiedicat.

O altă soluţie pentru asigurarea securităţii reţelelor fără fir este configurarea lor sub forma unor reţele virtuale private-VPN, blocând astfel interceptarea [44].

2.9. Concluzii rezultate din teză

În acest capitol am trecute în revistă principalele probleme legate de asigurarea calităţii transmiterii de semnal vocal prin reţelele fără fir bazate pe standardul IEEE 802.11. M-am oprit asupra unora din factorii care afectează calitatea transmisiei şi am argumentat necesitatea dezvoltării unor soluţii care să îmbunătăţească calitatea transmisiei vocii prin reţelele fără fir. Ca domeniu de aplicabilitate al acestor soluţii este asigurarea securităţii în reţelele fără fir, respectiv în punctele de acces, reducerea întârzierilor la sesiunea de iniţializare a apelurilor, la transmisia şi recepţia pachetelor de date şi corecţia erorilor pachetelor.

Având în vedere aceste lucruri am realizat următoarele contribuţii teoretice şi practice pe care nu le-am găsit în alte lucrări.

1. Am identificat întârzierile semnificative care afectează calitatea sesiunii de iniţializare a protocolului SIP în reţelele fără fir .Am analizat rata de eroare a cadrelor FER (frame error rate) funcţie de protocoalele de transport utilizate: TCP, UDP şi RLP. Întârzierile produse de fiecare dintre ele depind de mărimea pachetelor de semnalizare implicate în stabilirea sesiunii şi de numărul de server-e pe care acestea le traversează până la destinaţie. Pentru reducerea timpului de iniţializare a convorbirii am **propus un contor adaptiv pentru retransmitere.** Funcţie de numărul de cadre trimise şi confimate ca recepţionate, iniţial, contorul reduce timpul dintre cadre prin reducerea numărului şi a mărimii acestora. De asemenea întârzierile din cozile de aşteptare şi cele datorate Internet-ului influenţează sesiunea de iniţiere a unei apel VoIP [38]. În lucrarea [37] am făcut un studiu experimental al întârzierilor în reţelele fără fir, pentru situaţia unei distribuţii multiple (multicasting). Pentru acest caz rata maximă de transfer care poate fi atinsă este de 1.78 Mbps, pentru reţele cu trafic de 2 Mbps. Suplimentar trebuiesc implementate mecanisme de reducere a pierderilor cadrelor la nivelul MAC.
2. Tot în vederea îmbunătăţirii transmisiei vocii prin reţelele fără fir, bazate pe standardul IEEE 802.11, **am studiat şi am propus o soluţie bazată pe reducerea timpului de transmitere a datelor prin controlul numărului de apeluri admise în lista de interogare a punctelor de acces (AP)**. În lucrarea [39] am făcut o analiză a capacităţii funcţiei de coordonare prin punct (PCF) de a suporta traficul de voce. şi am indicat modul în care trebuiesc setaţi parametrii pentru a suporta apeluri vocale. Concluzia ce se desprinde este că, pentru o rată constantă de transmitere a biţilor (Contant Bit Rate-CBR),

cu toate că se limitează numărul de apeluri care pot fi admise, în realitate, prin limitarea jitter-ului şi prin aceasta a întârzierii maxime admise, modul CBR permite un număr rezonabil de apeluri care urmează să fie efectuate. În mod normal retransmiterile sunt evitate pentru traficul în timp real datorită întârzierilor pe care le implică. Numărul maxim de apeluri care pot fi admise este determinat de lungimea super-cadrului. Variind lungimea supercadrului, aceasta determină variaţii ale întârzierilor apelurilor, fapt ce trebuie evitat. Pentru aceasta am calculat numărul maxim de apeluri şi am determinat o întârziere implicită care se ia în calcul la receptor. Analiza erorilor pentru voce arată că e necesară şi o formă de corecţie a erorilor. Există trei opţiuni pentru aceasta: redirecţionarea corecţiei erorilor (forward error correction-FEC), retransmiterea şi livrarea pachetelor de eroare procesorului de semnal.

Prin redirecţionarea corecţiei erorilor-FEC, la emisie se codează informaţia cu coduri corectoare de erori, ECC (Error Correcting Codes) şi se transmite forma codată (cu biţii redundanţi rezultaţi) pentru a permite receptorului să regăsească informaţia iniţială. Informaţia se codează anterior transmisiei. Corecţia se face datorită ECC. La schemele ARQ (Automatic Repeat Request) codarea se face cu coduri detectoare de erori şi corecţia se face prin retransmitere. Se mai numesc ”backward error correction”.

3. **Am propus o nouă soluţie de securitate bazată pe conceptul de client-server**, care este publicată în lucrarea [40]. Studiul este motivat de faptul că nivelul MAC (Medium Access Control) al standardului IEEE 802.11 suportă retrans miteri ale pachetelor, impuse de erorile de transmisie ale celor două moduri, PFC şi DCF, în care operează acest standard. În urma unui studiu comparativ al performanţelor protocoalelor de semnalizare SIP, H.323 şi IAX, am optat pentru IAX, un protocol de tip open source, uşor de utilizat şi modificat. Prezintă avantajul că foloseşte lăţime de bandă minimă atât pentru transferul datelor cât şi pentru semnalizare şi are suport nativ pentru translatarea adreselor de reţea. În capitolul 4, paragraful 4.4 este prezentată propunerea mea pentru un modul de program **software**, bazat pe protocolul de semnalizare IAX şi care răspunde următoarelor cerinţe :
   - permite alegerea a 5 metode diferite de criptare;
   - traversarea cu succes a NAT (Network Address Translation);
   - permite simularea de chei de schimb prin utilizarea cheilor de sesiune pre-partajate (pre-shared);
   - securitate foarte bună;
   - nici o modificare la cerinţele de lăţime de bandă;
   - cerinţe reduse pentru procesorul calculatorului utilizat [40].

3. MODALITĂŢI DE REDUCERE A ÎNTÂRZIERILOR LA INIŢIALIZAREA UNEI SESIUNI BAZATE PE PROTOCOLUL SIP ÎN REŢELELE FĂRĂ FIR

Faţă de reţelele fixe, reţelele fără fir prezintă avantajul că nu au nevoie de cablu pentru transmisia de date. Rata de transfer a datelor în cadrul unor astfel de reţele locale (LAN-uri) este de ordinul a 11 Mbps, ceea ce este considerabil mai mare decât cea a serviciilor de date oferite de telefonia mobilă.

La iniţializarea unei sesiuni VoIP, datorită infrastructurii (transmitera datelor prin Internet având ca suport reţele fără fir) apar întârzieri. În acest capitol aduc ca noutate două modalităţi de reducere a întârzierilor la iniţializarea unei sesiuni bazate pe protocolul SIP în reţelele fără fir.

Înainte ca un utilizator să poată iniţia un apel VoIP, trebuie să stabilească sesiunea folosind unul din protocoalele de semnalizare, H.323 sau SIP şi să negocieze parametrii mass-media. Intervalul de timp necesar pentru a iniţializa sesiunea se numeşte timp pentru iniţializarea sesiunii. Acesta este afectat de calitatea link-ului wireless, măsurat prin rata de eroare a cadrelor (FER). Acest lucru duce la re-transmisii de pachete pierdute şi prelungeşte timpul de iniţializare. Prin urmare, protocoalele trebuie să optimizeze timpul de iniţializare a sesiunii împotriva pierderilor. În această teză, m-am concentrat asupra întârzierii sesiunii de configurare a SIP şi am propus optimizarea acesteia prin implementarea unui contor adaptiv pentru retransmitere. Pentru a reduce rata de eroare a cadrelor am evaluat, de asemenea performanţele sesiunii de iniţializare SIP funcţie de diverse protocoale utilizate cum ar fi protocolul de control al transmisiei (TCP), protocolul utilizatorilor de datagrame (UDP) şi protocolul legăturii radio (RLP).

Protocolul accesului la mediu (MAC) al standardului IEEE 802.11 suportă două moduri de funcţionare, un mod cu acces aleator pentru aplicaţii care nu sunt în timp real şi un mod de funcţionare cu liste de interogare şi invitare la emisie pentru aplicaţii în timp real. În acest capitol am studiat şi implementat un sistem care utilizează liste de interogare şi invitare la emisie pentru traficul de voce interactiv. Cu perioade între listele de interogare şi invitare la emisie mai mari, mai multe apeluri de voce pot fi acceptate, dar acest lucru duce la creşterea timpului de iniţializare, deci implicit la întârzieri mai mari. Rezultatele de aici vor putea fi aplicate la orice schemă de interogare şi invitare la emisie. Am plecat pentru acest studiu de la faptul că modul de coordonare prin punct (PCF) se bazează pe comutarea de pachete orientată pe conexiune, "packet-switched connection-oriented", care este bine adaptată traficului telefonic şi am stabilit condiţiile în care poate suporta trafic de voce. Traficul telefonic s-a dovedit a avea perioade alternative de semnal şi pauză [66], [82]. Soluţia de tip comutaţie de pachete profită de pauzele dintr-un apel vocal şi permite multiplexarea pachetelor de date provenite şi de la alte apeluri. Se utilizează astfel, în mod mult mai eficient, lăţimea de bandă decât în cazul circuitelor comutate.

Capitolul este structurat în opt paragrafe. În primul paragraf 3.1, sunt prezentate succint principalele probleme ale VoIP, protocoalele existente şi măsurile de securitate care ar trebui luate pentru o comunicaţie sigură. Paragraful 3.2 descrie

întârzierile din sesiunea de iniţializare SIP. Sunt prezentate protocoalele de transport TCP, UDP şi RLP.

Analiza semnalizărilor SIP din legăturile fără fir este prezentată în paragraful 3.3. Rezultatele numerice şi relevanţa contorului adaptiv pentru retransmisie constituie subiectul paragrafului 3.4. O altă modalitate de reducere a timpului de iniţializare a unei sesiuni SIP este controlul numărului de apeluri acceptate în listele de interogare şi invitare la emisie aferente punctelor de acces. Fundametarea teortică şi soluţia propusă pentru sunt prezentate în paragraful 3.5. În paragraful 3.6 sunt descrise rezultatele numerice, iar în paragraful 3.7 este făcută o analiză a erorilor. Concluziile capitolului sunt incluse în paragraful final 3.8.

3.1.Protocolul pentru iniţializarea sesiunii (SIP) în subsistemele IP multimedia (IP Multimedia Sub-Systems-IMS)

Arhitectura de bază a protocolului SIP se bazează pe modelul client-server. Funcţiile principale ale protocolului SIP în reţelele IP multimedia (IP Multimedia Subsystems-IMS) sunt asigurate de servere SIP cu funcţii variate, unele de control a sesiunii de apel (Call Session Control Function-CSCF), iar altele pe post de porţi (gateway-uri). Prin funcţia de control a sesiunii de apel (CSCF) se supervizează sesiunea multimedia, funcţia de translatare a adresei, de negociere a coder-ului de voce pentru comunicaţiile audio şi de gestionare a profilului abonatului. CSCF are trei roluri: cea de server proxy CSCF (P-CSCF), care este primul punct de contact mobil în reţelele IP multimedia (IMS), cea de server de control al accesului (S-CSCF), responsabil de gestionarea sesiunii şi cea de interogare CSCF (I-CSCF), care este responsabilă pentru găsirea celui mai apropiat server S-CSCF, funcţie de încărcarea sau capacitatea acestuia.

Un agent utilizator sau un punct final (endpoint) SIP este de obicei identificat folosind un cont de e-mail cum ar fi adresa de utilizator@domeniu.

SIP lucrează împreună cu protocolul de descriere al sesiunii (SDP), care are sarcina de a descrie sesiunea care va fi deschisă. Mesajele SIP pot fi transportate de protocolul UDP sau TCP.

Atunci când transportul mesajelor este efectuat de către protocolul TCP, nivelul de transport oferă siguranţă. Atunci când mesajele SIP sunt transportate de către UDP, asigurarea securităţii este realizată de către SIP. UDP este protocolul de transport larg utilizat de către SIP.

SIP este un protocol tranzacţional, în sensul că o tranzacţie SIP este alcătuită dintr-o singură solicitare şi orice răspuns la această solicitare. Stabilirea unei sesiuni, folosind SIP constă din diferite tranzacţii. Fig.3.1 ilustrează iniţializarea sesiunii între doi agenţi utilizator.

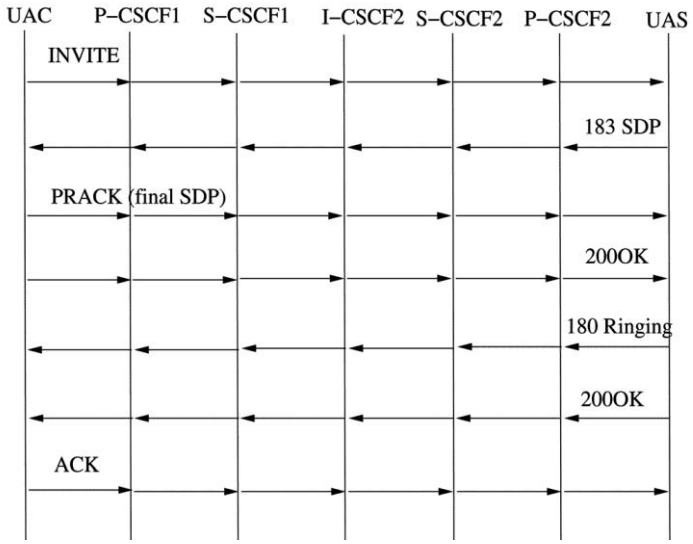


Fig.3.1. Iniţializarea sesiunii SIP [34]

Pentru a asigura un transfer sigur al cererilor şi răspunsurilor SIP, implicate în diverse tranzacţii, sunt necesare mecanisme de retransmisie atât la clientul agentului utilizator (User Agent Client-UAC) cât şi la server-ul agentului utilizator (User Agent Server-UAS). Scopul protocolului SIP este de a iniţializa legătura între cei doi agenţi. Agentul utilizator conţine atât o aplicaţie client care trimite cereri SIP cât şi o aplicaţie server care acceptă cererile. Clientul iniţiază tranzacţia trimiţând o cerere de INVITE şi primeşte ca răspuns mesajul 183 SDP (Session Progress with Session Description Protocol), adică cererea a ajuns la agentul utilizator al server-ului şi este în curs de procesare. Astfel agentul utilizator al clientului (User Agent Client) este conştient de transmiterea cu succes a cererii de INVITE de îndată ce a primit răspunsul 183 SDP. Agentul utilizator al clientului trimite un mesaj de confirmare provizorie (Provisional Respons Acknowledgement-PRACK) care îmbunătăţeşte fiabilitateai reţelei prin adăugarea unui sistem de confirmare a răspunsurilor provizorii de tipul 183 SDP. UAC trimite un răspuns 200 OK pentru rezervarea resurselor de-a lungul căii şi primeşte un sunet de apel, împreună cu răspunsul 180. Atunci când partea chemată decide să accepte apelul (de exemplu, ridică receptorul) este trimis un răspuns final 200 OK. Ultimul pas este de a confirma sesiunea, cu o cerere confirmare ACK. Apoi, sesiunea este stabilită.

Dacă pentru transmiterea mesajului SIP este folosit protocolul UDP, agentul utilizator al clientului retransmite cererea de INVITE, după un interval care durează Tr.(1) secunde şi care se dublează după fiecare retransmitere. Contorul de timp Tr.(1) estimează timpul necesar pachetului de date să străbată distanţa de la sursă la destinaţie şi înapoi şi are o valoare implicită de 500 ms, dar este recomandat să fie mai mare în cazul unei latenţe mari de acces a link–ului [34]. Retransmisiile încetează la recepţionarea unui răspuns de progers al sesiunii 183 SDP de către agentul clientului utilizator (UAC) sau după şapte transmisii de cerere de INVITE. Pentru protocoale de transport sigure, cum ar fi TCP, nu există nici un mecanism de retransmisie la nivelul aplicaţie. Aceasta cade în sarcina nivelului transport. Fiecare utilizator final

trebuie să confirme datele pe care le primeşte de la celălalt capăt. Pot să apară însă pierderi de date la nivel de segment de date sau de semnal de confirmare recepţie date. TCP tratează aceste pierderi prin iniţializarea unui contor de timp care se declanşează când se trimit date. În cazul în care timpul expiră şi nu se primeşte semnalul de confirmare recepţie date, retransmiterea datelor se reia [34]. Valoarea implicită pentru retransmisie este, de obicei între 1-1,5 secunde [35]. Indiferent de tipul de protocol de transport utilizat, retransmiterea cererilor încetează în cazul în care se depăşeşte o valoare de 2^6xTr.(1) secunde [35]. Pentru server, partea de tranzacţie constă în trimiterea de către agentul utilizator al server-ului UAS (User Agent Server) a semnalului 200 OK şi recepţionarea unui răspuns de confirmare ACK (Acknowledgement) .

3.2 Întârzierea sesiunii de iniţializare

În studiile legate de calitatea transmiterii vocii prin Internet s-a dat o mai mică atenţie întârzierilor care apar în sesiunea de iniţializare în reţelele fără fir.În această teză am investigat întârzierea sesiunii de iniţializare, definită ca perioada de timp în care agentul utilizator al clientului iniţiază sesiunea printr-un semnal de INVITE şi momentul în care semnalul de confirmare recepţie ACK, de la agentul utilizator al server-ului, ajunge la client. Întârzierea sesiunii de iniţializare depinde de un anumit număr de factori. Cei mai importanţi sunt următorii: întârzierea la transmiterea prin reţea, fapt ce poate produce pierderi şi cozile de aşteptare. Această întârziere poate fi cauzată de protocoalele de transport utilizate şi de erorile din strategiile de recuperare a datelor.

3.2.1. Protocoale de transport

Protocoalele de transport utilizate cel mai des pentru iniţializarea sesiunii sunt TCP şi UDP. Dacă pentru transportul mesajelor SIP este folosit protocolul UDP, este necesar doar un schimb de mesaje, ilustrate în Fig.3.1, pentru a iniţializa o sesiune VoIP. Retransmisiile sunt asigurate prin utilizarea unui contor de regresie exponenţial (de timp). Prin urmare, totalul timpului de întârziere pentru sesiunea de iniţializare pentru acest caz este timpul necesar tuturor mesajelor implicate în diverse tranzacţii să fie recepţionate cu succes atât de către UAC cât şi de UAS. Dacă mesajele SIP sunt transportate de protocolul TCP, conexiunea TCP ar trebui mai întâi să fie stabilită prin schimbul de semnale de sincronizare SYN/SYN-ACK/ACK. Apoi, mesajele SIP sunt schimbate, după cum este ilustrat în Fig.3.2.

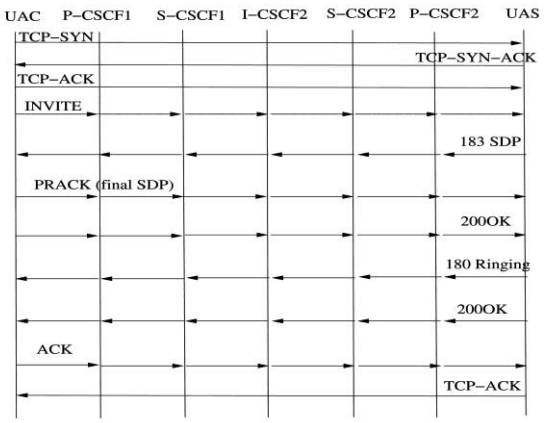


Fig.3.2 Iniţializarea sesiunii SIP prin utilizarea protocolului TCP [34]

Valoarea totală a întârzierii pentru sesiunea de iniţializare pentru mesajele SIP transportate de TCP se obţine prin suma dintre timpul de iniţializare al unei sesiuni TCP şi cel de transmitere cu succes a tuturor mesajelor necesare pentru stabilirea cu succes a unei sesiuni VoIP.

3.2.3. Protocol pentru Legături Radio (RLP-Radio Link Protocol)

Transportarea mesajelor SIP de către protocolul pentru legături prin unde radio RLP, poate reduce efectul ratei de eroare per cadru (FER-Frame Error Rate) din sesiunea de iniţializare şi poate creşte astfel fiabilitatea nivelului legăturii în reţelele fără fir [66].

RLP este un protocol care foloseşte tehnica ARQ la interfaţa cu legătura radio (wireless air interface). Majoritatea acestor interfeţe sunt reglate astfel încât să ofere pierderi de pachete de 1% şi respectiv vocoderele sunt astfel proiectate încât calitatea vocii sa fie bună la aceste pierderi. Dar pierderi de 1% sunt intolerabile pentru TCP şi trebuie luate măsuri de corectare. RLP detectează pierderile şi face retransmisii, astfel încât pierderile scad sub 0,1% sau chiar sub 0,001%, convenabile pentru aplicaţiile TCP/IP. De asemenea RLP fragmentează şi reasamblează fluxul şi uneori face o livrare ordonată. Noile forme de RLP fac cadrajul (adaugă cadrelor delimitatori de început şi sfârşit) şi compresia (acţiuni care mai de mult erau realizate de protocolul PPP-Point to Point Protocol). La transportul RLP, interfeţei radio nu i se poate pretinde o anumită dimensiune a încărcăturii utile (payload), dar planificatorul (scheduler) determină dimesiunea pachetului în funcţie de starea canalului şi emite un „upcall” RLP cu dimensiunea necesară a payload-ului, chiar înaintea transmisiei. Multe alte protocoale care fac fragmentarea (802.11b sau IP) folosesc dimensiunea payload-ului stabilită în nivelurile superioare şi apelează nivelul MAC care să creeze payload-ul de o anumită dimensiune. Aceste protocoale nu sunt atât de flexibile ca RLP şi eşuează în transmisii prin mediile afectate de fading (fluctuaţie) mare. Deoarece RLP-payload poate fi mic (11 octeţi) trebuie ca şi antetele RLP să fie mici-numere de secvenţă de pe 6 biţi (variable sequence number).

RLP se poate baza pe confirmări pozitive ACK şi negative NAK, dar de obicei se lucrează cu NAK pentru a reduce încărcarea legăturii pe retur (ineficientă spectral şi cu latenţă mare). Dacă legătura e „idle" (în repaos) se retransmite dublicatul ultimului NAK pentru a menţine rata de pierderi a pachetelor sub 0,1%. Acţiunea e controlată de un „flush timer" (contor de umplere), ce e pornit la 200-500 msec după ce canalul devine idle, Fig. 3.3.

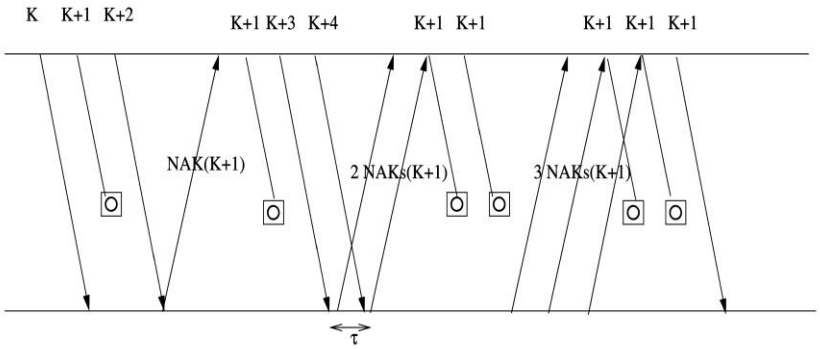


Fig.3.3 Schema RLP (1,2,3) [51]

RLP clasifică cadrele în trei clase de prioritate. Acestea sunt: cadre RLP de control (cum ar fi NAK), cadre de retransmitere date şi cadre noi de date. În scopul reducerii întârzierilor, în RLP, numărul de semnale NAK se aproximează astfel că numărul de mesaje NAK care pot fi trimise se poate alege. În această lucrare sunt investigate protocoalele RLP (1, 2, 3) şi RLP (1, 1, 1, 1, 1, 1). Numărul total de retransmisii pentru cele două scheme este aceleaşi (şase), cu diferenţa că (1, 2, 3) execută şase retransmisii cu trei aproximări, în timp ce RLP (1, 1, 1, 1, 1, 1) realizează acest lucru cu şase aproximări NAKs. Informaţii detaliate cu privire la RLP, se găsesc în [18].

3.3. Analiza semnalizărilor protocolului SIP la parcurgerea stratului legăturii de date al reţelelor fără fir

Pentru analiză, am luat în considerare un flux de mesaje SIP care se schimbă în mod normal la iniţierea unei sesiuni. Aceste mesaje sunt cele prezentate în Fig.3.1 pentru UDP şi Fig.3.2 pentru TCP. De asemenea am pornit de la următoarele ipoteze referitoare la o sesiune SIP end to end:

1. controlul admisiei, posibilele erori ale server-elor şi disponibilitatea conexiunii reţelei nu sunt luate în calcul;
2. protocolul TCP am presupus că operează într-un mod interactiv;
3. modul „întârzieri de confirmat" (delay acknowlegdement) de către TCP este dezactivat;
4. TCP răspunde cu un mesaj de timp expirat (time out) ori de câte ori un pachet se pierde. De exemplu un agent utilizator, după ce a transmis un mesaj SIP (INVITE) aşteaptă o confirmare (200 OK), înainte de a transmite următorul mesaj SIP (ACK).

3.3.1 Contor adaptiv pentru retransmisia mesajelor SIP de către protocolul UDP

Contorul de decrementare al protocolului SIP, după a i-a transmisie, dublează valoarea contorului Tr.(i). Astfel Tr (i) este dat de formula de mai jos :

$$Tr(i) = 2^{i-1}T(1) \tag{3.1}$$

Valoarea contorului iniţial de retransmisie Tr.(1) este un parametru crucial care trebuie optimizat, deoarece are un impact direct asupra întârzierii în sesiunea de iniţializare. Nu ar trebui să fie prea mic, deoarece pachetele vor fi retrimise în timp ce un răspuns este pe cale de a fi primit şi nu ar trebui să fie prea lung, pentru a evita creşterea în mod inutil a sesiunii de iniţializare, în caz că se produce o pierdere. Prin urmare, acesta trebuie să fie proporţional cu timpul de transmitere a mesajelor implicate în tranzacţie. Este în funcţie de numărul de cadre k cuprinse în diagrama UDP, de întârzierea D de propagare end to end, de timpul de transmisie dintre două cadre consecutive τ. Pentru partea de tranzacţie client transmiterea unei cereri INVITE (conţinând k_1 cadre) e confirmată de răspunsul 183 (conţinând k_2 cadre). **Prin urmare, contorul adaptiv pentru retransmisie, pe care îl propun pentru partea de client este:**

$$Tr(1) = D + (k_1 - 1)\cdot\tau + D + (k_2 - 1)\cdot\tau + \hat{I}ntârziere_{cozi\ asteptare/proces} \tag{3.2}$$

Pentru server valoarea lui Tr(1) se modifică, reflectând numărul de cadre conţinute de răspunsul 200 OK (k_2) şi de cel de confirmare ACK (k_3).

$$Tr(1) = D + (k_2 - 1)\cdot\tau + D + (k_3 - 1)\cdot\tau + \hat{I}ntârziere_{cozi\ asteptare/proces} \tag{3.3}$$

3.3.2. Întârzierea de transmitere fără Radio Link Protocol

Să presupunem că p este probabilitatea unui cadru de a fi eronat într-o legătură fără fir. Ca atare (1-p) este probabilitatea unui cadru de a nu fi eronat . Cu k cadre conţinute într-un pachet UDP, $((1-p)^k)$ este probabilitatea ca pachetele UDP să nu fie eronate. Prin urmare, rata de pierdere a pachetelor este $(1-(1-p)^k)$. Considerăm q probabilitatea ca o tranzacţie să eşueze. Aceasta înseamnă că primul pachet trimis (cererea de INVITE care conţine cadrul k_1) s-a pierdut sau că primul pachet s-a recepţionat dar răspunsul (183 care conţine cadre k_2) s-a pierdut. Prin urmare, probabilitatea de a avea o retransmisie a unei cereri INVITE în timpul unei tranzacţii la client este :

$$q = 1 - \left((1-p)^{k_1+k_2}\right) \tag{3.4}$$

Pentru partea de tranzacţie la server, valoarea q se schimbă, reflectând numărul de cadre conţinând răspunsuri 200 OK (k_2) şi ACK (k_3).

Fie N_m numărul maxim de transmisii (pentru SIP, N_m=7). Media întârzierilor pentru o tranzacţie cu succes este media întârzierilor pentru transmiterea cu succes a unei datagrame UDP care conţine un mesaj SIP şi a recepţionării cu succes a răspunsului de confirmare. Aceasta se datorează faptului că expeditorul (de exemplu, UAC)

ştie că pachetul expediat (de exemplu, INVITE) a fost recepţionat cu succes atunci când se primeşte mesajul 183.

Prin urmare, întârzierea de transmisie totală pentru iniţializarea sesiunii este suma întârzierilor pentru transmiterea tuturor mesajelor N necesare pentru a iniţializa o sesiune VoIP folosind transmiterea mesajelor SIP prin protocolul UDP. Media întârzierii sesiunii de iniţializare este dată de Tt_{UDP} şi este:

$$Tt(i)_{UDP} = D + (k-1)\tau - Tr(1) + \frac{(1-q)\left(1-(2q)^{Nm}\right)}{\left(1-q^{Nm}\right)(1-2q)} \cdot Tr(1) \tag{3.5}$$

$$Tt_{UDP} = \sum_{i=1}^{N} Tt(i)_{UDP} \tag{3.6}$$

unde $Tt(i)_{UDP}$ este întârzierea pentru transmiterea cu succes a celei de-a i-a datagrame UDP.

3.3.3. Întârzierea de transmitere prin protocolul RLP (1,2,3)

Protocolul legăturii radio (Radio Link Protocol-RLP) retransmite datele la nivel de cadru. Pentru prima încercare de retransmisie, un mesaj NAK este trimis la punctul final, care declanşează mecanismul de retransmitere al cadrului lipsă. În cea de-a doua încercare, sunt trimise două mesaje NAK şi fiecare din ele determină retransmiterea cadrului lipsă. În final, în cea de-a treia încercare, trei mesaje NAK sunt trimise şi declanşează trei retransmisii consecutive ale aceluiaşi cadru lipsă. Pentru această analiză, similar cu [18], trebuie să fie definiţi următorii termeni:

X_{ij}=al i-lea cadru retransmis la a j-a încercare şi recepţionat în mod corect la destinaţie;

Y_{ij}=al i lea –cadru NAK retransmis la a j-a încercare şi recepţionat în mod corect la sursă;

C_{ij}=primul cadru primit corect la destinaţie, care este al i–lea cadru retransmis la a j-a încercare de retransmisie;

A_j=cadrul lipsă nerecepţionat corect la a j -a încercare de retransmitere;

B_j= cadrul lipsă nerecepţionat corect până la sfârşitul celei de-a j -a încercare de retransmitere.

Presupunând că aceste cadre sunt independente unele de altele avem:

$$P(X_{ij})=P(Y_{ij})=1-p \tag{3.7}$$

unde p este rata de eroare/cadru FER (frame error rate). Astfel, în cazul în care un cadru nu este recepţionat corect la a j-a retransmisie, toate retransmisiile cuprinzând a j-a încercare se vor pierde şi atunci:

$$P\left(A_j\right) = \left((2-p)p\right)^j \tag{3.8}$$

În cazul în care după n încercări, retransmiterea cadrului eşuează, înseamnă că acest cadru nu a fost recepţionat corect, până la sfârşitul celui de-al n proces de retransmitere şi acest lucru este exprimat în următorii termeni:

$$P(B_n) = p((2-p)p)^{\frac{n(n+1)}{2}} \tag{3.9}$$

Dacă primul cadru recepţionat corespunde cu al i–lea cadru retransmis al încercării j, înseamnă că acel cadrul lipsă a fost pierdut până la a (j-1) încercare de retransmitere şi până la a (i-1) retransmitere din încercarea j.

$$P(C_{ij}) = p(1-p)^2 \cdot ((2-p)\cdot p)^{\frac{j(j+1)}{2}+i-1} \tag{3.10}$$

Prin urmare, probabilitatea de a transmite un cadru cu succes la nivelul stratului de control a legăturii radio (RLC) este dată de formula:

$$Pf = 1 - P(B_n) = 1 - p \cdot ((2-p)\cdot p)^{\frac{n(n+1)}{2}} \tag{3.11}$$

Retransmiterea la nivelul stratului legăturii de date măreşte durata de propagare a întârzierii de la D la D'. Dacă considerăm că dintr-un pachet care are k cadre, l cadre au fost recepţionate corect, obţinem următoarea întârziere D':

$$D' = \frac{1}{(1-P(B_n))^k}\left[\sum_{l=0}^{k}\left\{\binom{n}{k}(1-p)^{k-l}\left(\sum_{j=1}^{n}\sum_{i=1}^{j}P(C_{ij})\right)^{l}\left(D+(k-1)\tau+\frac{l}{1-P(B_n)}\left[\sum_{j=1}^{n}\sum_{i=1}^{j}P(C_{ij})\left((2j)D+\left(\frac{j(j+1)}{2}+i\right)\tau\right)\right]\right)\right\}\right] \tag{3.12}$$

Considerând că vor fi maxim trei încercări de retransmitere la nivelul protocolului legăturii radio, avem în acest caz n=3. Având în vedere că sunt tranzacţii SIP, contorul adaptiv al protocolului legăturii radio-RLP, se va modifica şi el pe partea de client:

$$\text{Tr}(1) = D`_1 + D`_2 + \hat{I}ntârziere_{cozi\,asteptare\backslash proces} \tag{3.13}$$

unde D_1´corespunde întârzierii pentru INVITE (cadre k1), iar D_2´pentru răspunsul 183 (cadre k_2). Întârzierile de tipul Cozi aşteptare\proces sunt calculate cu formula:

$$q = 1 - Pf^{k1+k2} \tag{3.14}$$

Pentru partea de server contorul este similar. Expresiile Tt(i) şi Tt rămân neschimbate.

3.3.4. Întârzierea de transmitere utilizând protocolul RLP (1,1,1,1,1,1)

RLP (1, 1, 1, 1, 1, 1) efectuează şase încercări de retransmitere şi fiecare din ele implică declanşarea unui NAK. Am presupus că:

$$P(X_{ij}) = P(Y_{ij}) = 1 - p \tag{3.15}$$

unde p este rata de eroare/cadru-FER. Probabilitatea ca un cadru să nu fie recepţionat corect la a j-a încercare de retransmitere este:

$$P(A_j) = ((2-p)p)^j \tag{3.16}$$

Dacă un cadru este abandonat (aborted) după a n–a încercare de retransmisie, acest lucru denotă faptul că până la sfârşitul celei de-a n-a retransmisii el nu a fost recepţionat corect. Modelul teoretic este exprimat de ecuaţia (3.17):

$$P(B_n) = p((2-p)p)^{\frac{n(n+1)}{2}} \tag{3.17}$$

Dacă primul cadru recepţionat corespunde retransmiterii cadrului corespunzător încercării j avem situaţia:

$$P(Cj) = p(1-p)^2 \cdot ((2-p)\cdot p)^{(j-1)} \tag{3.18}$$

Prin urmare, probabilitatea de a transmite cu succes un cadru la nivelul controlului legăturii radio este dată de :

$$Pf = 1 - P(B_n) = 1 - p\cdot((2-p)\cdot p)^n \tag{3.19}$$

Pentru protocolul RLP(1,2,3) întârzierea de propagare a cadrului creşte de la D la D’:

$$D' = \frac{1}{(1-P(B_n))^k}\left[\sum_{l=0}^{k}\left\{\binom{n}{k}(1-p)^{k-l}\left(\sum_{j=1}^{n}\sum_{i=1}^{j}P(C_{ij})\right)^l\left(D+(k-1)\tau+\frac{l}{1-P(B_n)}\left[\sum_{j=1}^{n}\sum_{i=1}^{j}P(C_{ij})\left((2j)D+\left(\frac{j(j+1)}{2}+i\tau\right)\right)\right]\right)\right\}\right] \tag{3.20}$$

Pentru studiu am limitat numărul maxim de încercări de retransmisie ale protocolului legăturii radio la n=6.

3.3.5. Întârzierea de transmitere a SIP utilizând protocolul TCP

Contorul adaptiv utilizat pentru retransmisa mesajelor în cazul protocolului TCP se bazează pe timpul necesar unui fragment de a parcurge distanţa de la emiţător la receptor şi înapoi. Pentru analiza protocolului TCP voi folosi un contor adaptiv similar cu cel folosit pentru protocolul UDP:

$$Tr(1) = 2D + (K_1 - 1)\cdot\tau + D + (K_2 - 1)\cdot\tau + Întârziere_{coziasteptare\phi proces} \tag{3.21}$$

K_1 este numărul de cadre conţinute în pachetele de date şi K_2 este numărul de cadre trimise receptorului împreună cu, confirmările de recepţie ale emiţătorului (de exemplu 183).

Dacă transmisia mesajelor SIP prin protocolul TCP se face fără a utiliza protocolul pentru legături radio, agentul utilizator al protocolului SIP va executa specificaţiile de retransmitere a mesajelor date de protocolul TCP până când va fi recepţionat un mesaj de confirmare. Segmentele TCP transportă mesajele SIP în câmpul de informaţie utilă. Valoarea totală a întârzierii sesiunii de iniţializare este dată de:

- întârzierea transmiterii mesajelor necesare pentru a stabili o sesiune TCP (SYN /SYN-ACK/ACK);
- întârzierea transmiterii mesajelor SIP nesecare iniţializării sesiunii VoIP.

Suma întârzierilor sesiunii de iniţializare este dată mai jos:

$$Tt_{TCP} = \sum_{i=1}^{N} Tt(i)_{TCP} \tag{3.22}$$

3.3.6 Întârzierile în cozile de aşteptare

În această secţiune voi determina întârzierile în cozile de aşteptare ale mesajelor SIP la terminalul utilizatorului, la server-ul intermediar de control al funcţiei de iniţiere sesiune (CSCF) şi la destinaţie. Pentru aceasta voi considera pentru terminalul sursă şi server-ul CSCF modelul M/M/1, al lui Markov, iar pentru destinaţie modelul M/G/1. Am ales aceste două modele ale lui Markov deoarece terminalul sursă şi server-ul execută operaţii prestabilite dar momentul de început e aleator, pe când la destinaţie se pot executa o varietate de operaţii non SIP cu un timp de serviciu de distribuţie general. De asemenea am presupus că mai multe terminale sursă sunt deservite de server-e cu funcţie de control al apelului. Astfel rata de sosire a mesajelor SIP la terminalul sursă, λ_M, este o fracţiune din rata de sosire a mesajelor la serverele de control a funcţiei de iniţiere apel, $\lambda:\lambda_M \le \lambda$.

Utilizând rezultatele din teoria cozilor de aşteptare [62], media întârzierii datorate cozilor de aşteptare, pentru agentul utilizator al clientului este dată de formula:

$$Tq_{ST} = \frac{1}{\mu - \lambda_M} \tag{3.23}$$

unde μ este rata de serviciu pentru mesajele SIP de la terminalul sursă. Media întârzierii în cozile de aşteptare pentru server-ele proxy, de interogare şi de servire ale funcţiei de apel sesiune (P/I/S-CSCF) definite pe parcursul capitolului este:

$$Tq_{P-CSCF} = Tq_{I-CSCF} = Tq_{S-CSCF} = \frac{\rho_S}{\lambda(1-\rho_S)} \tag{3.24}$$

unde ρ_s ($\rho=\lambda/\mu$) reprezintă destinaţia şi încărcarea server-elor CSCF. În final întârzierea cozilor de aşteptare la destinaţie se obţine utilizând rezultatul bazat pe modelul cozilor M/G/1 ale lui Markov. Pentru a evalua întârzierea mesajului SIP datorită cozii voi lua în considerare numai mesajele care au prioritate mai mare decât cele SIP şi voi ignora pe cele cu o prioritate mai scăzută. Întârziere de aşteptare la destinaţie este următoarea:

$$Tq_{DT} = \frac{\frac{1}{\mu_S}(1-\rho_0-\rho_S)+R}{(1-\rho_0)+(1-\rho_0-\rho_S)} \tag{3.25}$$

unde ρ_0 este sarcina de la destinaţie pentru mesaje non SIP, μ_s rata de serviciu pentru mesajele SIP de la destinaţie. Valoarea R este un răspuns al server-ului de la destinaţie ca urmare a unui mesaj anterior şi care determină trecerea lui aleatoare într-o stare nouă ce trebuie iarăşi evalută. Este egală cu:

$$R = \lambda_0 \overline{X_1^2} + \frac{\lambda_s \overline{X_s^2}}{2} \tag{3.26}$$

unde $\overline{X_1^2}$, $\overline{X_s^2}$ sunt momentele secundare ale lui μ_s şi respectiv rata de servire a mesajelor non SIP de la destinaţie.

3.3.7 Expresia întârzierii sesiunii de iniţializare

Întârzierea sesiunii de iniţializare este o sumă de întârzieri datorate transmisiei, cozilor de aşteptare şi Internetului. Astfel media sesiunii de iniţializare cu N mesaje este următoarea:

$$T_{sesiune} = N^* Tq_{ST} + Tt_{Transm} + N^* Tq_{P\text{-}CSCF} + N^* Tq_{I\text{-}CSCF} + N^* Tq_{S\text{-}CSCF} + N^* T_{Internet} + N^* Tq_{DT} \tag{3.27}$$

unde Tt_{Transm} variază, în funcţie de protocoalele de transport şi cel pentru legături radio folosite pentru a transmite mesaje SIP. $T_{Internet}$ este întârzierea dată de Internet. Întârzierea introdusă de Internet depinde de numărul de rutere şi de tipul de legături pe care le parcurge datagrama transmisă. Este foarte greu să se standar-dizeze astfel de transmisii heterogene şi să se calculeze întârzierile. Pentru acest mo-tiv întârzierea prin reţelele fixe este presupusă a fi constantă şi egală cu 100 ms [69].

3.4. Rezultate numerice obţinute ca urmare a experimentelor efectuate pentru studiul întârzierilor SIP

Această secţiune prezintă rezultatele experimentale ale studiului referitor la media întârzierilor sesiunii de iniţializare SIP utilizând protocoale de transport şi legătură radio. **Modelul introdus în paragraful precedent, 3.3., implică creşterea exponenţială a mediei întârzierilor sesiunii de iniţializare cu rata de eroare a cadrelor (FER). Numărul şi dimensiunea mesajelor schimbate afectează media întârzierilor din sesiunea de iniţializare**. Reducerea acestor factori con-duce la o diminuare a lor. Pentru evaluare, dimensiunea aproximativă pentru fiecare mesaj SIP am obţinut-o din pachetele capturate de analizorul de protocol Ethereal din testele experimentale. A fost nevoie de numărul de cadre, în fiecare caz şi de aceea au fost luate în considerare două tipuri de canale: 9.6 kbps şi 19.2 kbps . Durata fiecărui cadru radio am presupus a fi de 20 ms, ceea ce corespunde la 24 de octeţi într-un canal 9.6 kbps şi 48 de octeţi într-un canal de 19.2 kbps. Valorile întârzierii D de propagare end to end şi a intervalului de timp dintre cadre τ, sunt setate la 100 ms, respectiv 20 ms. Numărul maxim de transmisiuni N_m, stabilit în paragraful 3.3.2 este setat la şapte pentru mesaje SIP cu TCP respectiv UDP [69].

Referitor la întârzierile din cozile de aşteptare, am presupus că rata de sosire a mesajelor SIP (λ), rata de serviciu a server-elor intermediare şi cea de la destinaţie sunt la fel ($\mu_s=\mu$). Calculul întârzierilor pentru cozile de aşteptare de la destinaţie implică al doilea moment al ratei de servire. De asemenea am presupus că $\lambda_M=0{,}1\lambda$ şi

deviaţia standard σ, a acestor rate de servicii este de 5% din valoarea medie. Acum avem potrivit [62], relaţiile:

$$\overline{X}_1^2 = E[X_1]^2 \text{ şi } \overline{X}_S^2 = E[X_S]^2 \quad (3.28)$$

$$\text{unde } E[X_1]^2 = \sigma_1^2 + (E[X_1])^2 \text{ şi } E[X_S]^2 = \sigma_S^2 + (E[X_S])^2 \quad (3.29)$$

Înlocuind μ_s şi μ_0 în $E[X_1]$ şi $E[X_s]$, vom avea expresia

$$R=0{,}501\left[\rho_0^2 + \rho_S^2\right] \quad (3.30)$$

Pentru experimente am considerat prima dată rata de eroare a cadrelor (FER) variabilă şi am menţinut rata de sosire a mesajelor SIP la sursă λ_M=50 cereri/s. Menţinând acum rata de eroare a cadrelor constantă la 1%, am modificat valoarea lui λ_M. Pentru ceilalţi parametri ai sistemului avem următoarele valori:

$\mu=4*10^{-4}$s

$$\rho_S = \frac{\lambda}{\mu}$$

ρ_0=0,7

$T_{Internet}$=100ms

Tabelul 1 arată dimensiunea datagramelor UDP şi numărul de cadre per datagramă pentru ambele canale.

Tabelul 1. Mărimea mesajelor şi numărul de cadre pentru sesiunea de iniţializare SIP cu protocolul UDP

Mesaje	Mărime informaţie utilă (octeţi)	Mărime mesaj (octeţi)	Cadre (9.6kbps)	Cadre (19.2kbps)
SIP INVITE	700	728	37	19
SIP 183	835	863	44	23
SIP PRACK	558	586	30	16
SIP 200OK	545	573	29	15
SIP 180	349	377	19	10
SIP ACK	300	328	17	9

Am presupus că fiecare datagramă UDP este încapsulată într-un cadru IP de 28 octeţi (20 octeţi pentru header-ul IP şi 8 octeţi pentru header-ul UDP). Media întârzierilor sesiunii de configurare utilizând un contor adaptiv pentru retransmisia mesajelor este calculată pentru ambele canale şi este prezentată în fig.3.4.

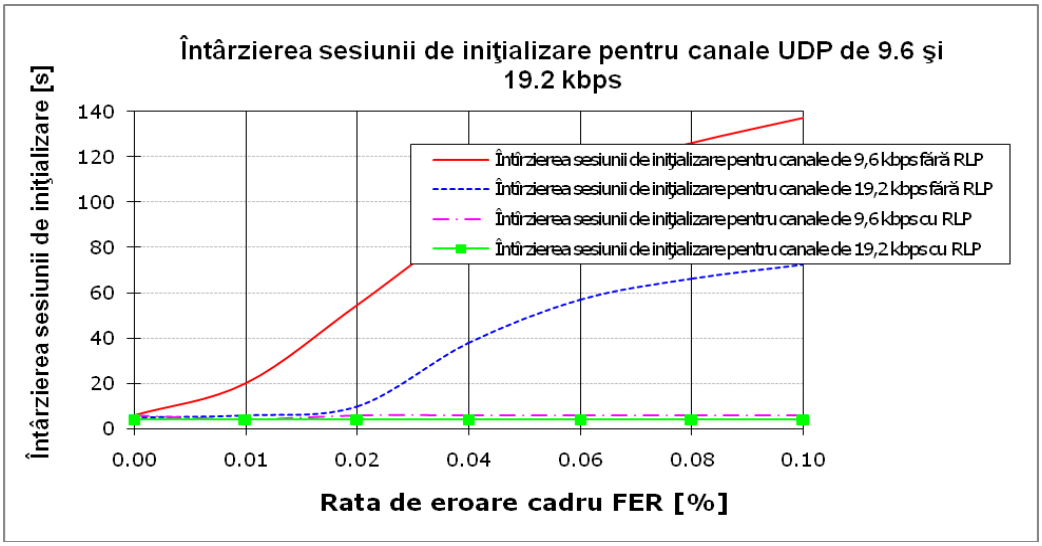


Fig.3.4. Media întârzierilor sesiunii de iniţializare SIP cu UDP pentru canale de 9.6 kbps şi 19.2 kbps cu/fără RLP (1,2,3)

Au fost luate în calcul cadre cu rate de erori variate, cuprinse între 0-10 %. Având în vedere că sesiunea este stabilită pentru VoIP, serviciile de voce sunt suportate pentru erori de ale cadrelor (FER) cuprinse între 1 şi 3%. Rezultatele pentru procentul de 1 % a ratei de eroare a cadrelor sunt prezentate în Tabelul 2.

Analizând valorile vedem că întârzierea unei sesiuni SIP este conformă cu recomandările ITU-T [34], dacă este utilizat protocolul pentru legături radio sau dacă lăţimea de bandă este mai mare de 19.2 kbps. În Fig.3.4 am făcut o evaluare a întârzierii sesiunii de iniţializare pentru mesaje SIP transmise prin protocolul UDP cu RLP (1, 2, 3) sau RLP (1, 1, 1, 1, 1, 1). Din figură rezultă faptul că prin utilizarea protocolului pentru legături radio se obţine cea mai mica întârziere a sesiunii de iniţializare. RLP permite configurarea numărului de runde NAK şi a confirmărilor NAK trimise într-o rundă, în scopul de a optimiza recuperarea erorilor.

Întârzierea datorată cozilor de aşteptare din sesiunea de iniţializare este relativ mică: 0,6136 s pentru mesaje SIP transmise prin protocolul UDP pentru ambele canale.

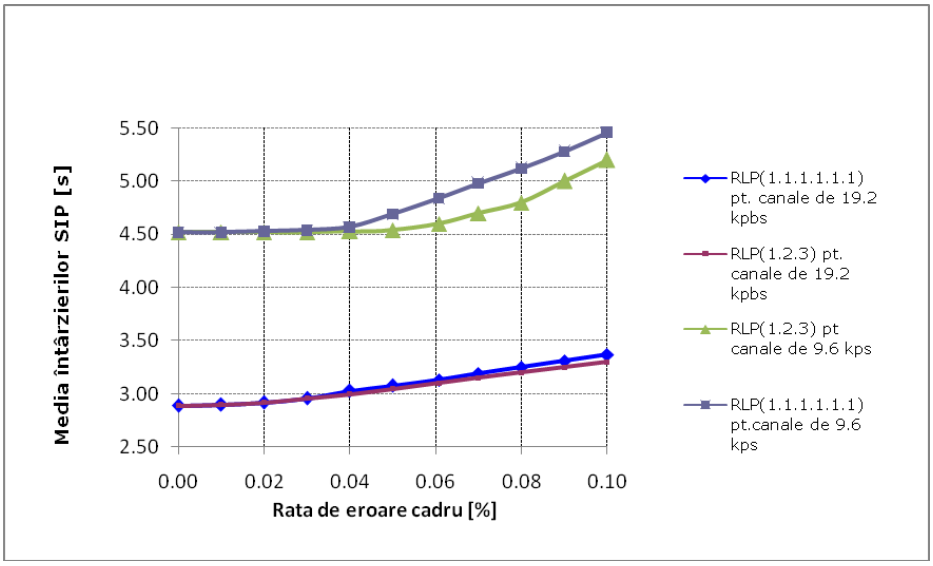


Fig.3.5 Media întârzierilor sesiunii de iniţializare pentru canale de 9,6 şi 19,2 kbps pentru mesaje SIP prin UDP şi RLP diferite

Fig. 3.5 compară schemele RLP(1, 2, 3) şi RLP(1, 1, 1, 1, 1, 1) pentru ambele canale. RLP (1, 2, 3) surclasează RLP (1, 1, 1, 1, 1, 1), pentru rate de erori ale cadrelor mai mari de 3 %, independent de lăţimea de bandă a canalului. Întârzierea sesiunii de iniţializare este cu până la 5 % mai mare în cazul protocolului RLP(1, 1, 1, 1, 1, 1) datorită timpului suplimentar de recuperare pentru confirmarea celor şase semnale NAK. Dublarea vitezei de transmisie a canalului, adică a debitului de la 9,6 la 19,2 kbps, reduce întârzierea cu 40 %. Cu toate acestea, reducerea este de 0,5 s, o diferenţă care nu este importantă pentru percepţia la utilizator. Utilizarea oricărei scheme de retransmisie prin protocolul RLP reduce considerabil întârzierea acolo unde rata de eroare a cadrelor (FER) este mai mare de 1 %. Se poate alege un sistem sau altul atâta timp cât diferenţa între scheme este de maxim 200 ms. Utilizarea oricăruia dintre protocoalele RLP optimizează întârzierea sesiunii de iniţializare şi este o soluţie mult mai bună decât creşterea lăţimii de bandă pentru erori ale cadrelor mai mari de 1 %.

Tabelul 2. Comparaţie între UDP şi TCP,pentru o rată de eroare a cadrului de 1%

Protocoale	Întârzierea sesiunii de iniţializare pentru canale de 9.6 kbps	Întârzierea sesiunii de iniţializare pentru canale de 19.2 kbps
UDP fără RLP	20.65	5.6
UDP cu RLP(1,2,3)	4.61	2.9
UDP cu RLP (1,1,1,1,1,1)	4.61	2.9
TCP fără RLP	23.8	6.9

Protocoale	Întârzierea sesiunii de iniţializare pentru canale de 9.6 kbps	Întârzierea sesiunii de iniţializare pentru canale de 19.2 kbps
TCP cu RLP(1,2,3)	5.9	3.9
TCP cu RLP(1,1,1,1,1,1)	5.9	3.9

3.4.1 Relevanţa contorului adaptiv pentru retransmisie

Contorul de timp iniţial, utilizat pentru retransmisia mesajelor SIP prin protocoalele UDP şi TCP, se comportă după modelul unei funcţii exponenţiale. Îşi dublează, după fiecare retrimitere de pachete valoarea. Este foarte important să se ia în considerare o valoare iniţială relevantă pentru contor.

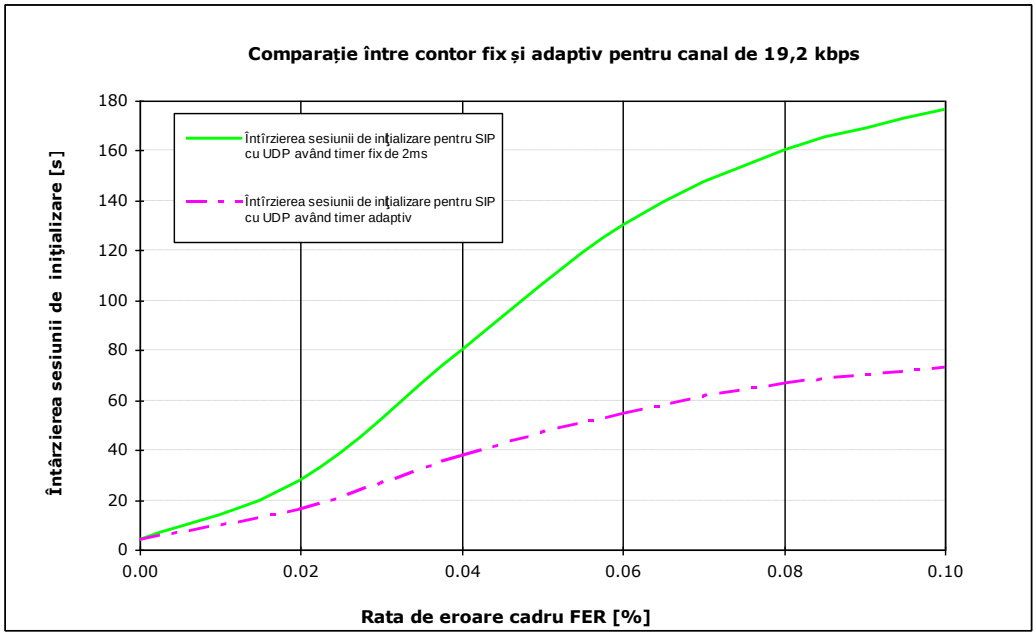


Fig.3.6 Comparaţia mediei sesiunii de iniţializare SIP cu UDP între contor adaptiv pentru retransmisie şi contor fix de 2s pentru canale de 19.2 kbps

Fig.3.6 arată rezultatele comparaţiei dintre întârzierea sesiunii de iniţializare cu un contor de timp fix de 2 ms şi un contor adaptiv pentru retransmisie. Contorul adaptiv pentru retransmisie reduce în timp întârzierile sesiunii de configurare cu o medie de 46%. Utilizarea contorului adaptiv pentru retransmisie este relevantă pentru minimizarea costurilor de întârziere pentru orice transmitere în general şi a sesiunii de iniţializare în special, deoarece aceasta din urmă afectează în mod direct cerinţele utilizatorilor.

Fig.3.7 ilustrează media valorilor întârzierilor sesiunii de iniţializare pentru cele două canale de 9,6 şi 19,2 kbps. Dublarea lăţimii de bandă a canalului reduce întârzierile în sesiunea de configurare cu o medie de 37%. Întârzierea sesiunii de confi-

gurare cauzate de cozile de aşteptare este mai mare pentru mesajele transmise prin protocolul TCP decât pentru UDP: este de 1.0227 s pentru ambele canale. Acest lucru se datorează numărului mare de mesaje implicate în iniţializarea unei sesiuni cu TCP şi a dimensiunii lor mai mari.

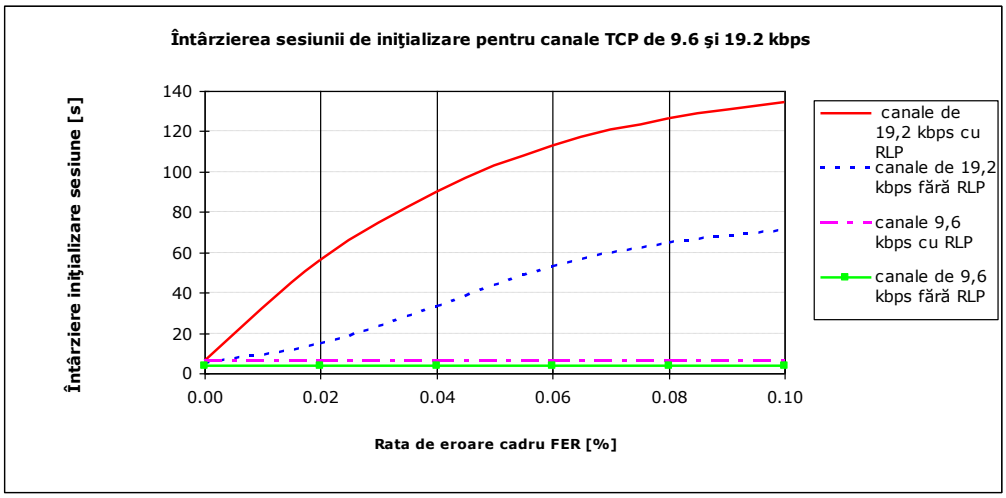


Fig.3.7. Întârzieri medii ale sesiunilor de configurare pentru canale de 9.6 şi 19.2 kbps pentru mesaje SIP încapsulate în protocolul TCP cu sau fără protocolul pentru legături radio RLP

În cazul în care rata de eroare a cadrelor este mai mică de 2 % întârzierea sesiunii de iniţializare a mesajelor SIP transmise prin protocolul TCP este sensibil egală cu cea pentru UDP. Acest lucru se datorează utilizării contorului adaptiv pentru retransmitere care ajustează dimensiunea mesajelor la cea a celor implicate în iniţializare, iar TCP trimite mesaje relativ mici pentru conexiunile de iniţializare.

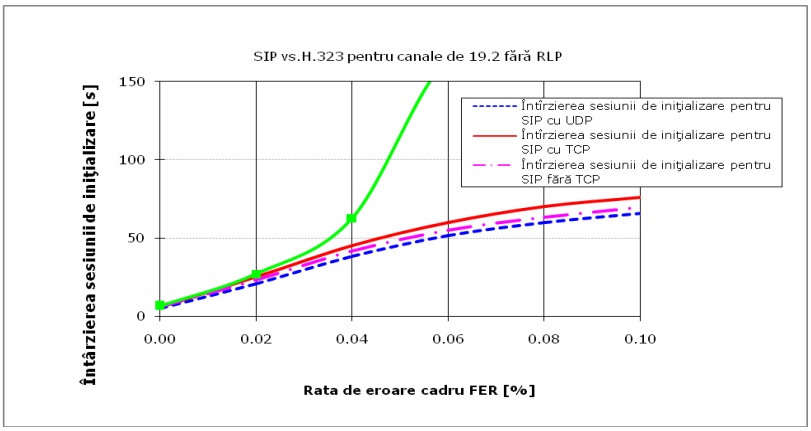


Fig.3.8. Întârzierile din sesiunea de iniţializare cu protocoale SIP şi H.323 pentru canale de 19.2 kbps prevăzute cu contor adaptiv pentru retransmitere

Protocolul H.323 este concurentul lui SIP pentru stabilirea sesiunilor VoIP. În Fig.3.8 am făcut o comparaţie a celor două protocoale pentru cazul utilizării contorului adaptiv pentru retransmisie şi a unei rate de eroare a cadrelor descrisă anterior. Mesajele H.323 sunt transmise prin protocoalele TCP şi IP. Testele le-am făcut pentru un număr maxim de 10 retransmisii. Pentru întârzierea sesiunii de iniţializare cu o rată de eroare a cadrelor (FER) mai mică de 2 % rezultatele sunt la fel. Dacă rata de eroare creşte peste 2 %, SIP surclasează H.323.

Aceste rezultate se datorează contorului adaptiv pentru retransmisie utilizat pentru stabilirea sesiunii H.323, care are 19 mesaje mai mici decât cele SIP. În plus, la H.323 întârzierea creşte exponenţial deoarece sunt permise 10 retransmisii în timp ce pentru SIP doar şapte. Această comparaţie arată o influenţă considerabilă a contorului de timp şi a numărului maxim de retransmisii permise asupra performanţelor întârzierilor din protocolul de semnalizare.

Pentru contorul de timp fix numai numărul de mesaje necesare pentru a iniţializa o sesiune influenţează întârzierea acesteia, pe când la contorul adaptiv pentru retransmitere, dimensiunea mesajelor este factorul cel mai semnificativ care o influenţează. Prin urmare, pentru a optimiza şi mai mult întârzierea sesiunii de iniţializare SIP, unele scheme de compresie ar putea utiliza compresia de semnalizare (SigComp) sau compresia bazată pe text. Compresia bazată pe text poate comprima între 30-50% din dimensiunea celor mai multe mesajele SIP prin eliminarea antetelor redundante şi a informaţiei utile. Cererea iniţială INVITE nu poate fi comprimată decât la circa 9% [20].

Numărul de utilizatori pot afecta de asemenea întârzierile din sesiunea de iniţializare: prin modul de admitere a unui utilizator într-o celulă şi disponibilitatea server-elor SIP. În această teză, disponibilitatea server-elor este legată de încărcarea lor şi de rata de sosire a mesajelor SIP. Controlul admisiei nu face obiectul de studiu al acestei lucrări. Rata de sosire afectează în mai mică măsură întârzierea sesiunii de iniţializare, independent de lăţimea de bandă a canalului. Este de ordinul a 10 ms pentru mesaje SIP, crescând o dată cu creşterea număului de cereri de la 50 cereri/s la 150 de cereri/s.

3.5. Suport pentru servicii VoIP

Conform standardului IEEE 802.11 se disting două tipuri de reţele fără fir:

- ad hoc;
- reţele infrastucturale cu punct de acces (AP) .

Punctele de acces (AP) au rolul unor punţi între staţiile fără fir (wireless), precum şi între staţiile fără fir şi cele fixe. Standardul IEEE 802.11 specifică două funcţii la nivelul controlului de acces la mediu (MAC), una de coordonare distribuită (DCF-Distributed Coordination Function) şi alta de coordonare prin punct (PCF-Point Coordination Function) şi trei opţiuni pentru nivelul fizic: spectru împrăştiat cu salt de frecvenţă (Frequency Hopping Spread Spectrum-FHSS), spectru împrăştiat cu secvenţă directă (Direct Sequence Spread Spectrum-DSSS) şi infra-roşu (Infra Red-IR) [39].

Prin funcţia de coordonare distribuită se asigură accesul la mediu din subnivelul MAC de control al accesului la mediul şi se bazează pe accesul multiplu cu detecţia purtătoarei (Carrier Sens Multiple Access cu evitarea coliziunii-CSMA/CA). Perioada de timp în care o reţea locală funcţionează în modul DCF este cunoscută sub numele de perioada concurenţială (Contention Period-CP) când îşi adjudecă accesul la mediul de transmisie. Priorităţile de acces la mediu sunt controlate prin utilizarea intervalului de timp dintre cadre (Inter-Frame Spaces-IFS). Există trei tipuri de perioa

de de timp între cadre: perioada scurtă (Short Interframe Space-SIFS), perioada funcţiei de coordonare prin punct a IFS (Point Coordination Function IFS-PIFS) şi perioada funcţiei de coordonare distribuită a IFS (Distributed Coordonation Function-DIFS).

Intervalul cel mai scurt dintre cadre (SIFS) este folosit pentru transmiterea de mesaje de confirmare. Staţiile răspund la interogările punctelor de acces şi între mesaje, dacă o unitate pentru date de serviciu (MAC Service Data Unit-MSDU) este fragmentată. Transmisiile care trebuie să aştepte doar un interval scurt au cea mai mare prioritate faţă de mediu. Transmisiile care trebuie să aştepte un interval de timp egal cu un cadru DIFS, au prioritatea cea mai scăzută de acces la mediu.

Funcţia de coordonare prin punct (PCF) asigură transferul cadrelor neconcurenţial şi perioada de timp în care o reţea locală (LAN) funcţionează în modul PCF este cunoscută sub numele de perioadă neconcurenţială (Contention Free Period-CFP). Punctele de acces, AP, îndeplinesc funcţia de punct coordonator, câştigând controlul asupra mediului la începutul unei perioade neconcurenţiale, după ce primeşte informaţia prin care i se comunică, că mediul urmează să fie inactiv pentru o perioadă scurtă de timp PIFS. În timpul perioadei inactive, staţiile care sunt incluse în listă pot răspunde la mesaje, pot fi chestionate de către punctele de acces-AP. La primirea unui mesaj staţia transmite datele sale după un interval scurt SIFS. În scopul de a sonda staţiile active, un punct de acces trebuie să menţină o listă a lor, care este dependentă de modul ei de implementare. Perioada de pauză trebuie să alterneze cu cea de dispută a accesului la mediu. Suma celor două perioade este numită "supercadru" şi este prezentată în Fig. 3.9. Se poate întâmpla ca o staţie să înceapă să transmită un cadru, chiar înainte de sfârşitul perioadei concurenţiale, CP, mărind astfel perioada supercadrului curent şi scurtând astfel următorul CFP aşa cum este arătat în Fig. 3.9:

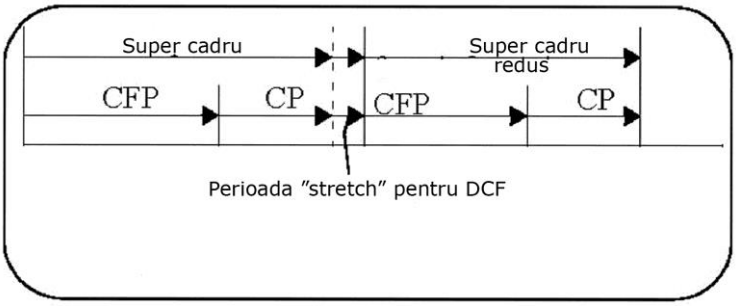


Fig.3.9. Diagrama de timp pentru transmisie supercadru [35]

Mărirea duratei supercadrului curent şi scurtarea următorului CFP este cunoscută sub denumirea de stretching. Pentru a înţelege efectul de stretching al CFP, ar trebui să admitem că, pentru unitatea pentru date de serviciu a substratului de acces la mediu (MAC Service Data Unit-MSDU), dimensiunea maximă a cadrului, de 2304 octeţi, să fie trimisă înainte de sfârşitul supercadrului. Dacă pragul de fragmentare (parametru setabil), nu este egal cu această dimensiune maximă, atunci depăşirea duratei va fi inevitabilă datorită fragmentării MSDU. Toate fragmentele unităţii de serviciu a mediului, MSDU, sunt trimise ca intervale scurte (SIFS), ceea ce înseamnă că un punct de acces, în aşteptarea unui interval PIFS, pentru a iniţia un CFP, nu poate accesa mediul între transmisia fragmentelor. Astfel, în cel mai rău caz, perioa-

da de stretching ar dura atâta timp cât ar fi necesar pentru a trimite 2304 de octeţi conţinând fragmente cu informaţii utile. Punctele de acces iniţiază perioade de neconcurenţialitate, CFP, prin transmiterea unui cadru de balizaj (beacon). Dacă traficul în timpul perioadei de neconcurenţialiate (CFP) este redus şi/sau un AP a finalizat de interogat toate staţiile din lista de acces, CFP se poate termina prin transmiterea unui cadru CF-End. Punctul de acces, AP, preia apoi controlul mediului şi începe interogarea staţiilor din listă. Retransmisiile sunt utilizate în standardul IEEE 802.11 pentru corectarea erorilor atât în modul DCF cât şi în modul PCF. Pentru a sprijini corectarea erorilor sunt folosite confirmări (ACKs). O confirmare a unui cadru este încapsulată în cadrul următor, chiar dacă aceasta din urmă nu este destinată aceleaşi staţii de către expeditorul din cadrul anterior. Nu există nici un mecanism pentru a opri retransmisiile în modul PCF sau de a folosi diferite contoare de reluare pentru modurile PCF şi DCF.

Mesajele de balizaj (beacon) sunt generate periodic, în funcţie de intervalul stabilit. Staţiile mobile ascultă mediul la anumite intervale, multipli ai intervalului de balizaj, pentru a detecta aceste mesaje. Un mesaj este trimis la începutul unei perioade neconcurenţiale-CFP, dar în cazul în care durata CFP este mai mare decât cea a mesajului, vor fi trimise mai multe mesaje în timpul unui CFP. Durata maximă a unei perioade neconcurenţiale (CFP MaxDuration) este de asemenea, setabilă şi indicată în mesajele de balizaj. Pentru semnalele de balizaj care sosesc în mijlocul unui CFP, durata rămasă indică de cât timp a fost iniţiată perioada de neconcurenţialitate. Astfel, dacă o staţie de telefonie mobilă e inactivă şi se trezeşte la intervalele ei de ascultare, acestea ar putea să nu coincidă cu începutul unei CFP, însă se poate stabili perioada scursă de când CFP–ul a fost iniţiat.

3.5.1. Soluţia propusă

Specificaţiile standardului IEEE 802.11 nu prevăd o metodă pentru crearea şi menţinerea listelor de interogare şi invitare la emisie (polling lists). Această teză aduce ca noutate o procedură prin care se controlează admisia în liste. Soluţia propusă prezintă arhitectura aleasă, definirea acţiunilor utilizatorului pentru transmiterea de date vocale şi planul de acţiuni pentru controlul admisiei conexiunii (Connection Admission Control-CAC), în scopul admiterii unui număr limitat de utilizatori în lista de interogare şi invitare la emisie şi iniţializarea variabilelor pentru managementul bazei de informaţii (Management Information Base-MIB) .

3.5.2. Arhitectura reţelei

Arhitectura de reţea folosită pentru experimente este prezentată în fig.3.10

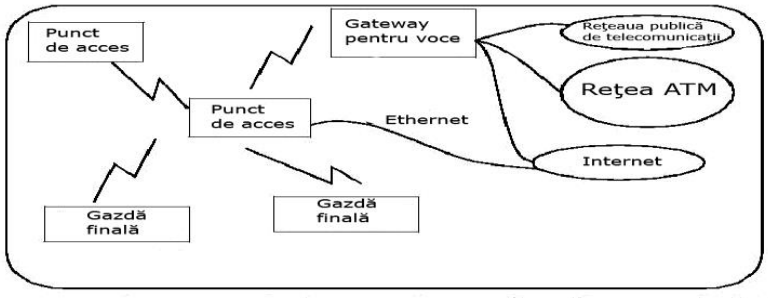


Fig.3.10. Arhitectura de reţea

Punctele de acces au în prezent, doar două interfeţe, o interfaţă IEEE 802.11 şi o interfaţă Ethernet. Interfaţa Ethernet suportă traficul de date trimise prin modul de funcţie distribuită de la staţiile mobile la punctele de acces (AP). Pe de altă parte, deoarece Ethernet nu furnizează servicii de calitate diferenţiale (Quality of Service-QoS), nu este potrivit pentru traficul în timp real. Modul de funcţionare cu coordonare prin puncte de acces (PCF) poate să fie folosit ca legătură între un punct de acces la o poartă (gateway) vocală (vezi fig.3.10.), care suportă interfeţe pentru reţele de telefonie clasică (PSTN), transmisii asincrone (Voice over ATM) şi Internet (Voice over IP). Gateway–ul vocal converteşte straturile protocolului standardului IEEE 802.11 în cadre PCM pentru a le putea transmite prin reţele de telefonie fixă, reţele cu transmisie asincronă (ATM Adaption Layer pentru ATM-uri) sau reţele de voce în timp real (Voice over Real-Time Transport Protocol-RTP/UDP/IP) pentru reţelele IP. Această arhitectură oferă garanţii pentru întârzierile între două puncte terminale (end-to-end) dat fiind faptul că atât reţelele clasice cât şi reţelele de transmisie asincronă (ATM-uri) sunt orientate pe conexiune.

În această arhitectură care utilizează modul de coordonare prin punct pentru traficul de voce între punctele de acces şi porţile vocale, un apel vocal către o reţea de telefonie fixă, asincronă sau IP utilizează aceleaşi resurse în cadrul unei reţele locale fără fir ca şi un apel între două puncte de acces. Astfel, atât pentru apelurile între două puncte cât şi cele între utilizatorii unei reţele fără fir şi reţeaua fixă/asincronă/IP, cele două capete sunt adăugate în lista de interogare a unui punct de acces. Pentru apeluri între utilizatori din reţele diferite, porţile destinate apelurilor vocale extrag semnalele vocale din cadrele IEEE 802.11 recepţionate şi le trimit prin protocoale dedicate către utilizatorii din celelalte tipuri de reţele. Pot fi prevăzute extensii care să permită mai multor puncte de acces sau a altor arhitecturi în care funcţionalitatea porţilor pentru apeluri vocale este localizată în punctele de acces, accesul în reţeaua fără fir.

În reţelele fără fir pachetele de voce sunt transportate în conformitate cu unul din cele două moduri de funcţionare ale standardului: rată constantă (Constant Bit Rate-CBR) în care apelurile au alocat tot intervalul de timp şi rată variabilă (Variabile Bit Rate VBR), în care este folosită multiplexarea, pauzele din cadrul apelurilor vocale sunt folosite de către alte apeluri de voce sau trafic de date.

În această lucrare am luat în considerare ambele posibilităţi de a trimite pachete de voce atât de dimensiune fixă cât şi de dimensiune variabilă. Având în vedere faptul că dispozitivele de codare-decodare a vocii (codec-uri) produc de obicei un anumit număr de octeţi la fiecare câteva msec (de exemplu, pentru voce un codec produce 32 de octeţi la fiecare 30ms), s-ar putea implementa un sistem cu pachete

mărime fixă. Acestea ar duce la supraîncărcarea straturilor protocolului (doar antetul substratului de acces la mediu-MAC este de 34 octeţi). În ambele moduri de operare, cu rată constantă sau variabilă, vor fi create pachete de lungime variabilă.

Se impune astfel necesitatea determinării intervalului de timp optim necesar transmiterii pachetelor de voce. Cele două alternative care pot fi utilizate sunt cu scheme de sincronizare cu informare completă de timp (CTI) sau cu scheme cu informare nulă de timp (NTI) [13] [15]. Schema cu informare completă de timp utilizează protocolul în timp real (RTP). Foloseşte o metodă relativă de amprentare a timpului, care funcţionează bine în reţelele în care pachetele utilizate sunt de lungime variabilă şi variaţia întârzierilor este mare pentru traficul în timp real. În reţelele de transport asincrone este utilizată schema cu informare nulă (NTI). În cadrul schemelor cu informare nulă de timp, fiecare pachet nu are un timp prestabilit. În schimb, dacă valoarea jitter-ului între terminale este cunoscută, primul pachet de voce este întârziat cu un timp egal cu durata jitter-ului, iar pachetele ulterioare sunt trimise la intervale de timp egale cu cel de asamblare a pachetelor (packetization interval). Deoarece celulele ATM sunt de dimensiune fixă, întârzierea de asamblare a pachetelor este fixă. Prin urmare, chiar dacă cadrele ulterioare au întârzieri diferite faţă de primul cadru, trimiterea lor la intervale T, egale cu întârzierea de asamblarea a pachetelor, permit reconstruirea lor. Deci, o combinaţie de reţele de ATM orientate pe conexiune şi mărime a celulelor ATM fixă, cu valoarea jitter-lui stabilită, permite utilizarea schemelor temporale de sincronizare cu informare nulă (NTI) [15]. În reţele fără fir, chiar dacă valoarea jitter-ului este cunoscută pentru funcţia de coordonare prin punct-PCF, dimensiunea pachetelor nu este fixă. Dat fiind faptul că exact de durata între interogări depinde dacă se va mări sau nu perioada de acces la mediu, ipoteza generării unor pachete la intervale constante nu poate fi făcută, prin urmare nu poate fi utilizată în acest caz schema de sincronizare cu informare nulă (NTI). Prin urmare, este indicat utilizarea unui sistem cu o schemă de sincronizare cu informare completă (CTI). Deoarece majoritatea apelurilor utilizatorilor din reţelele fără fir pleacă din reţea spre alte tipuri de reţele, am presupus că toate pachetele de voce sunt trimise prin puncte de acces, chiar dacă în unele cazuri, ambele capete se află în aria de acoperire a unei punct de acces şi ar fi putut fi trimise direct. În modul de coordonare prin punct, un punct de acces controlează datele trimise, dar datele ar putea ajunge direct de la staţie mobilă la staţie mobilă.

Stiva pentru protocol utilizată în scopul de a transporta cadre trebuie să fie de asemenea specificată. Având în vedere că cerinţele de întârziere limitează dimensiunea pachetelor de voce, am încercat să evit supraîncărcarea protocolului. Pentru acest scop, am utilizat protocolul de transport în timp real (RTP).

Punctul de acces ar putea parcurge lista sa de interogare şi invitare la emisie numai parţial, pe durata unui supercadru, o dată sau de mai multe ori. În modul cu rată de biţi constantă, sondajul este făcut o dată pe durata unui supercadru. Toate cele trei opţiuni amintite mai înainte vor fi luate în considerare pentru modul cu rată de biţi variabilă.

Pentru terminarea unui apel trebuie ţinut cont de cele două moduri de funcţionare ale reţelei fără fir, cea de neconcurenţialitate la mediu şi cea de concuren-ţialitate. În modul de transfer prin rată de biţi constantă, dat fiind faptul că fiecare apel vocal are alocat o durată fixă de timp, lungimea perioadei de acces la mediu va fi determinată de numărul de apeluri vocale admise. În modul de transfer prin rată de biţi variabilă, atunci când punctul de acces termină de interogat toate staţiile din listă, acesta trimite un sfârşit de interogare şi începe una nouă, chiar dacă durata maximă nu s-a terminat. Acest lucru impune ca încărcarea pachetelor să se facă la niveluri acceptabile.

Pentru ambele moduri, lungimea supercadrului este fixă. Numărul maxim de apeluri care pot fi admise este determinat de lungimea supercadrului. Variind lungimea supercadrului, aceasta determină variaţii ale întârzierilor apelurilor admise, lucru ce trebuie evitat. Analiza erorilor pentru voce arată că e necesară o formă de corecţie a erorilor. Există trei opţiuni pentru aceasta: trimiterea mai departe a erorii pentru corecţie (forward error corection FEC), retransmiterea şi livrarea pachetelor de eroare procesorului de semnal.

3.5.3. Calculul numărului maxim de apeluri vocale

Când un utilizator mobil iniţiază un apel vocal, un mesaj de semnalizare este trimis către un punct de acces (prin funcţia de coordonare distribuită) cerând să fie adăugat în lista de interogare. Punctul de acces ţine evidenţa numărului maxim apeluri admise care nu trebuie să depăşească valoarea maximă admisă. Punctul de acces trimite mai departe un mesaj de semnalizare către staţia mobilă apelată (pentru apeluri în aria de acoperire a punctului de acces) sau la o poartă vocală (voice gateway) pentru apeluri în reţeaua de telefonie PSTN/ATM/IP, specificând întârzierea pentru pachetele de voce recepţionate. Calculul reconstrucţiei acestei întârzieri este prezentat mai jos. La acceptarea apelului partea apelată sau poarta (gateway) trimite un răspuns punctului de acces. Acesta include cele două terminale în lista de interogare şi trimite un răspuns apelatului împreună cu reconstrucţia întârzierii care trebuie folosită la recepţionarea pachetelor care vin de la apelant. La terminarea convorbirii, punctul de acces primeşte un mesaj de eliberare (release) şi scoate din listă cele două terminale. Tabelul 3 prezintă lista de notaţii utilizată pentru demonstraţie.

Tabelul 3. Lista de notaţii utilizate pentru optimizarea numărului maxim de apeluri admise într-o lista de invitare la emisie (polling)

Parametru	**Simbol**	**Valoare**
Durata maximă a unui super cadru	T_{SF}	Variază
Intervalul de balizaj (beacon)	T_b	Variază
Rata de transmisie în kbits/s	R	2 (FHSS) şi 11 (DSSS)
Rata de codare voce în kbits/s	c	8,5
Supraîncărcare Antet (RTP, LLC, MAC cu WEP) în biţi	h	57*8
Mărime antet strat fizic în biţi	P	16*8 şi 24*8
Numărul maxim de apeluri vocale în modul de operare CBR	N_p	Se calculează
Numărul maxim de apeluri vocale în modul de operare VBR	N_s	Se calculează
Valoarea minimă a supercadrului	$T_{SF\text{-}min}$	Se calculează
Valoarea minimă a perioadei concurenţiale CP	$T_{cp\text{-}min}$	Se calculează
Valoarea minimă a perioadei neconcurenţiale CFP s	$T_{cfp\text{-}min}$	Se calculează
Valoarea maximă a pragului de fragmentare în biţi	f	1100*8 şi 2304*8
Mărimea cadrului de balizaj (beacon) în biţi	B	40*8
Dimensiune Terminare CF în biţi	CF_{end}	24*8
Intervalul SIFS	T_{sifs}	0.028m
Timp slot	T_{slot}	0.050ms
Întârzierea de asamblare pachete mi-	P_{min}	30ms

Parametru	Simbol	Valoare
nimă		
Timpul de trimitere pachete de voce pe durata unui supercadru T_{SF}	T_v	Se calculează
Timpul pentru trimiterea CTS (14 octeţi)	T_{cts}	Se calculează
Timpul pentru trimiterea RTS (20 octeţi)	T_{rts}	Se calculează
Timpul pentru trimiterea unui cadru de confirmare fără date (14 octeţi)	T_{ack}	Se calculează

Pentru a determina timpul necesar unui apel transmis cu o rată de biţi constantă (CBR), trebuie determinată dimensiunea maximă a pachetelor de voce. Timpul maxim între două interogări este T_{SF} în secunde. La acest timp trebuie adăugat P_{min} =30 ms, pentru a ţine cont de posibilitatea că un pachet de date vocale se termină după o interogare (poll). Astfel, dimensiunea cea mai mare a pachetului de voce creat va fi c*(P_{min} +T_{SF}) biţi. Ţinând cont de faptul că în modul cu rată de biţi constantă, CBR, acest interval de timp este alocat pentru fiecare apel vocal chiar dacă se generează sau nu un pachet, timpul pentru a menţine o convorbire este dată de relaţia:

$$T_V = \frac{\left(c \times \left(P_{min} + T_{SF}\right) + h + P\right) \times 4}{R} + 4T_{sisf} \tag{3.31}$$

Pentru a determina numărul maxim de apeluri, este necesar găsirea duratei minime de acces concurenţial şi apoi prin diferenţa între durata maximă a unui supercadru T_{SF} minus această durată minimă se obţine durata care se ia în calcul pentru perioada de timp neconcurenţială. Valoarea minimă a perioadei concurenţiale, $T_{cp\text{-}min}$, include timpul minim necesar transmiterii unui cadru. În afară de acest minim trebuie prevăzută şi posibilitatea măririi duratei cadrului (stretching). După un schimb de semnale de tip cerere de trimitere/ştergere (RTS-CTS) schimbate între intervalele de cadre de scurtă durată corespondente (SIFS), este trimisă o unitate de servire date (SDU) de dimensiune maximă, în perioada de prelungire, ca un flux continuu de fragmente fără erori fără necesitatea de a fi trimise înapoi.

Toate fragmentele şi confirmările ACK, sunt trimise doar cu intervale SIFS între ele. Fiecare fragment este confirmat. T_{max} este intervalul de trimitere a unui SDU (Service Data Unit) de dimensiune maximă. Pentru a calcula numărul maxim de apeluri avem:

$$T_{cp}=T_{cp\text{-}min} + T_{cp\text{-}stretch}, \text{ unde} \tag{3.32}$$

$$T_{cp\text{-}min}=2T_{sifs}+2T_{slot}+8T_{ack}+T_{max} \tag{3.33}$$

$$T_{cp\text{-}stretch}=T_{rts}+2T_{sisf}+T_{cts}+T_{max} \tag{3.34}$$

$$T_{max} = (m-1)\left(\left[\frac{f+h+P}{R}\right] + T_{ack} + 2T_{sisf}\right) + T_{last} \tag{3.35}$$

Unde

$$m = \left[\frac{S_{maxSDU}}{f}\right] \tag{3.36}$$

şi

$$T_{last} = \frac{S_{maxSDU} - f(m-1) + h + P}{R} + T_{ack} + 2T_{sisf} \tag{3.37}$$

Pentru a calcula numărul maxim de apeluri vocale care pot fi admise, am împărţit timpul scurs pentru o perioadă de neconcurenţialitate la mediu (CFP), după ce a fost acceptată mărirea duratei de acces la mediu (CP) şi supraîncărcarea cadrelor de balizaj şi a semnalelor de sfârşit acces la mediu, la timpul necesar pentru un apel VoIP. În cazul unei perioade de acces la mediu lungi, perioada de inactivitate (CFP) este scurtată pentru ca numărul de cadre de balizaj (beacon) să fie $(T_{SF} - T_{cp})/T_b$. Astfel numărul maxim de apeluri care pot fi admise utilizând modul de transmisie cu rată constantă (CBR) este:

$$Np = \frac{T_{SF} - Tcp - Tovhd}{Tv}, \text{ unde} \tag{3.38}$$

$$T_{ovhd} = \left(\frac{B+P}{R} + T_{sisf}\right) \cdot \left[\frac{T_{sf} - T_{cp}}{Tb}\right] + \frac{CF_{end} + P}{R} \tag{3.39}$$

Pentru modul de funcţionare cu transmitere cu rata de timp variabilă (VBR), am calculat numărul maxim de apeluri pentru două modele de voce: modelul Brady's şi Zebo's [39]. Ambele modele sunt ON-OFF Markov–Modulated-Fluid (MMF), unde în starea ON datele sunt generate cu rata codec–ului de voce. Cele două modele diferă prin timpul mediu de aşteptare al celor două stări, aşa cum se arată în tabelul 4.

Tabelul 4. Modele Vocale

Mod	Perioada Medie ON	Perioada Medie OFF	p
Model Brady's [39]	1 sec	1.35 sec	0.43
Model May and Zebo [39]	352ms	650ms	0.35

Prin admiterea mai multor apeluri vocale am demonstrat statistic că pierderile vor fi mai mici decât numărul ε. N_s este dat de (3.38)

$$\frac{1}{2pN_s} \sum_{k=2N_p-1}^{2N_s} \left(k - 2N_p\right)\binom{2N_s}{k} p^k (1-p) 2^{N_s - k} \le \varepsilon \tag{3.40}$$

unde p este probabilitatea ca un dispozitiv de trimitere să fie activ. Ecuaţia (3.38) se bazează pe presupunerea că, dacă un apel vocal nu este interogat într-un supercadru este mai bine să fie distrus, decât să fie transmis în supercadrul următor din considerente de întârziere.

3.5.4. Calculul întârzierii

Pentru calculul întârzierii acumulate pe parcursul transmiterii unui pachet am ales o schemă cu o informare completă pentru intervalul de timp (CTI), iar pentru transport protocolul de transport în timp real (RTP). Un receptor foloseşte întârzierea rezultată pe parcursul transmiterii mesajului la reconstruirea acestuia. Întârzierea acumulată trebuie să fie cât mai mică posibil. Mai întâi precizez că întârzierea trebuie să fie diferenţa maximă posibilă a întârzierii între două pachete, Fig.3.11.

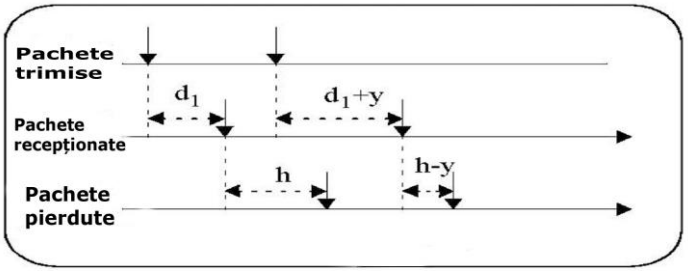


Fig.3.11. Calculul întârzierii

De exemplu, primul pachet presupunem că are nevoie de un timp d_1 secunde (necunoscut) până ajunge la destinaţie şi d, întârzierea totală acumulată de la împachetare şi până la receptor, care terbuie să fie în intervalul $d_{min} \le d \le d_{max}$. **În baza calculelor teoretice şi a experimentelor în această lucrare am oferit o soluţie de determinare a timpul de menţinere a acestui prim pachet la receptor înainte de a fi decodat**. Să presupunem că acesta ar fi h după cum se arată în Fig. 3.11. Astfel, întârzierea totală a primului pachet este d_1+h. Dacă al doilea pachet a avut nevoie de d_1+y secunde (unde y este cunoscut prin intermediul amprentei de timp relative), atunci acest pachet ar trebui să fie întârziat cu h-y secunde, astfel încât să aibă aceeaşi întârziere totală d_1+h ca primul pachet de date , h-y ≥ 0, ceea ce înseamnă cea mai mică valoare a lui h este egală cu valoarea maximă a lui y. Valoarea maximă a lui y este d_{max}-d_{min} şi prin urmare întârzierea acumulată este setată la valoarea jitter-ului. Chiar dacă y < 0, acest rezultat se menţine. În această secţiune, voi stabili valoarea jitter-ului pentru pachetele de voce ale acestei soluţii.

Pentru a determina jitter-ul, este necesar să se identifice modul în care cele două capete ale unui apel vocal sunt introduse pe lista de interogare. De exemplu, dacă un apel, să zicem A, are două capete A1 şi A2, A1 este introdus pe lista de interogare imediat urmat de A2. Pachetele de la A1 la A2 au întârzieri mici, deoarece în răspunsul primit de la A2 se indică faptul că datele pot fi livrate imediat. Cu toate acestea, pachetele de la A2 la A1 vor avea o întârziere mai mare. În modul CBR, toate apelurile vor avea aceeaşi întârziere. Întârzierea se calculează în două direcţii k1->k2 şi k2->k1, presupunând că sfârşitul lui k1 este pus pe lista de interogare înainte de sfârşitul k2.

$$P_{min} + \frac{T_v}{2} \le D_{k1 \to k2} \le P_{min} + T_{SF} + \frac{T_v}{2} \qquad (3.41)$$

Cel mai bun caz este cel în care un pachet scurt este creat în intervalul de timp P_{min}=30 ms şi întârzierea acumulată se termină înainte de o nouă interogare. Având în vedere că în modul de transmisie cu rată constantă CBR, chiar dacă pachetul este scurt, timpul alocat pentru emisie şi răspuns este $T_v/2$. Propagarea de întârziere este neglijată, dacă durata legăturii radio este scurtă.

Limita superioară am determinat-o plecând de la faptul că o interogare tocmai a pierdut crearea unui pachet de voce (P_{min}). Terminalul k1 aşteaptă un interval T_{SF} pentru o nouă interogare (acesta include şi perioada de prelungire). La următoarea interogare, atunci când terminalul k1 trimite pachetul de date, acesta este livrat

imediat terminalului k2. Timpul de transmisie este $T_v/2$. În direcţia opusă, k2->k1 întârzierea va fi mai mare. Această întârziere este delimitată de

$$P_{min} + T_{SF} - T_{cp\text{-}stretch} \le D_{k2 \to k1} \le P_{min} + 2T_{SF} \quad (3.42)$$

Limita inferioară este stabilită din nou, luând în calcul întârzieri mici ale pachetelor. În continuare, în cel mai bun caz, nu va fi nici o perioadă de prelungire, caz în care, intervalul de timp pentru terminalul k2 este T_{SF}-$T_{cp\text{-}stretch}$. Terminalul k1 va fi interogat mai repede cu intervalul Tv/2 faţă de terminalul k2, la cea de-a doua interogare. Aceasta înseamnă că intervalul de timp pentru interogarea celor doua terminale k1 şi k2 este de T_{SF}-$T_{cp\text{-}stretch}$-$T_v/2$. Timpul de transmisie adaugă $T_v/2$.

Limita superioară este atinsă atunci când o interogare a pierdut timpul alocat (P_{min}). Aceasta este urmată de un interval de aşteptare T_{SF} pentru următoarea interogare a terminalului k2. Aceste date aşteaptă apoi un alt interval de timp T_{SF}-$T_v/2$ pentru a fi livrate terminalului k1 în următorul supercadru. Timpul de transmisie este $T_v/2$.

Având în vedere valorile jitter-ului (întârziere maximă-întârziere minimă) pentru cele două direcţii ale apelului vocal, punctul de acces poate determina întârzierea pentru fiecare terminal implicat. Astfel valoarea maximă a întârzierii totale pentru ambele direcţii este dată de (3.43) şi (3.44):

$$TD^{max}_{k1 \to k2} = D^{max}_{k1 \to k2} + \left(D^{max}_{k1 \to k2} - D^{min}_{k1 \to k2}\right) \quad (3.43)$$

şi

$$TD^{max}_{k2 \to k1} = D^{max}_{k2 \to k1} + \left(D^{max}_{k2 \to k1} - D^{min}_{k2 \to k1}\right) \quad (3.44)$$

unde valorile max sunt limitele superioare, ale ecuaţiilor 3.39 şi 3.40, iar min sunt limitele inferioare ale aceloraşi ecuaţii.

Deoarece apelurile pleacă, un apel programat pe lista de interogare într-o anumită poziţie k, poate fi deplasat în sus în listă pentru a aduce toate apelurile vocale în faza de perioadă neconcurenţială. Acest lucru ar creşte timpul disponibil pentru perioada de acces la mediu.

Întârzierile acumulate la receptor şi datorate tranziţiei vor trebui să fie gestionate prin semnalizări corespunzătoare.

Pentru modul de funcţionare cu rată de timp variabilă (VBR), calculul întârzierilor este mult mai complex, deoarece în cazul unei pauze din cadrul apelului, un alt apel vocal sau alte pachete de date, pot profita de lipsa de semnal. Acest lucru face ca perioada să poată varia foarte mult şi să fie chiar mai mare decât T_{SF} (spre deosebire de cazul CBR, când durata unei interogări este maximum T_{SF}). Trei factori controlează întârzierea: valoarea T_{SF}, poziţia apelului în lista de interogare şi numărul de apariţii ale unui apel într-un supercadru. Pentru apelurile care au ca destinaţie terminale de tip ATM/IP, intervalul de timp al cererii unui utilizator dintr-o reţea fără fir pentru o poartă destinată apelurilor vocale, trebuie să fie păstrat cât mai mic.

3.6. Rezultate experimentale

Pentru a asigura funcţionarea optimă a punctelor de acces şi a staţiilor mobile este necesară iniţializarea unor variabile de management a bazei de informaţii (MIB). Câteva variabile relevante pentru managementul bazei de informaţii (MIB) sunt: dot11CFPPeriod, dot11CFPMAxDuration şi dot11BeaconPeriod.

dot11CFPPeriod este valoarea intervalului de repetiţie (supercadru). În lucrarea [39] am specificat minimul perioadei CFP ca având valoarea:

$$T_{cfp-min} = T_B + T_{CF-end} + 3T_{sifs} + (T_V / 2) \quad (3.45)$$

unde $T_V / 2$ este timpul necesar pentru a trimite un pachet de voce şi a primi răspuns. Dacă adun relaţia (3.45) cu $T_{cp\text{-}min}$ dată de relaţia (3.33) obţin

$$T_{SF\text{-}min}=T_{cfp\text{-}min}+T_{cp\text{-}min} \quad (3.46)$$

Durata supercadrului am ales-o astfel încât $T_{SF} \geq T_{SF\text{-}min}$. Perioada de repetiţie a intervalului dot11CFPPeriod este cunoscută a fi T_{SF}-$T_{cp\text{-}stretch}$, astfel că punctul de acces poate câştiga acces la mediu pentru perioada de neconcurenţă la sfârşitul intervalului de repetiţie a acestei perioade. Prin aceasta durata supercadrului include şi timpul de prelungire (stretching).

Numărul maxim de supercadre este de fapt un compromis între numărul de apeluri pentru care a fost proiectată reţeaua şi constrângerile legate de întârzierile pachetelor de voce.

Având setată perioada de neconcurenţialitate CFP, am stabilit valoarea variabilei dot11CFPPeriod la valoarea dot11CFPMaxDuration minus $T_{cp\text{-}min}$.

Dot11BeaconPeriod, intervalul de timp între 2 cadre de balizaj consecutive transmise de punctele de acces este egal cu variabila dot11CFPPeriod. Aceasta limitează numărul de cadre de balizaj generate în cadrul unei perioade de neconcurenţă la mediu la 1, reducând astfel depăşirea capacităţii acestora.

În continuare am determinat valorile numerice pentru diferiţi parametrii descrişi până în prezent, numărul maxim de apeluri utilizate în algoritmul CAC (Connection Admission Control) pentru punctele de acces şi întârzierea totală în modul de transmisie cu rată constantă. Tabelul 3 prezintă valorile anumitor parametri necesari pentru setările variabilei pentru managementul bazei de informaţii MIB. Acestea sunt determinate atât pentru viteze de 2 Mbps cât şi 11 Mbps.

Tabelul 5. Valori ale parametrilor pentru iniţializarea variabilei MIB (ms)

Viteza de transmisie (R) Mbps	$T_{cp\text{-}min}$	$T_{cp\text{-}stretch}$	$T_{SF\text{-}min}$
2	11,9	10.7	14.9
11	4,4	3,2	5,8

Fig. 3.12. arată numărul maxim de apeluri vocale, care pot fi efectuate în cazul transmisiei cu rată de biţi constantă pentru fluxuri de 2 Mbps şi 11 Mbps, pentru două valori ale pragului de fragmentare

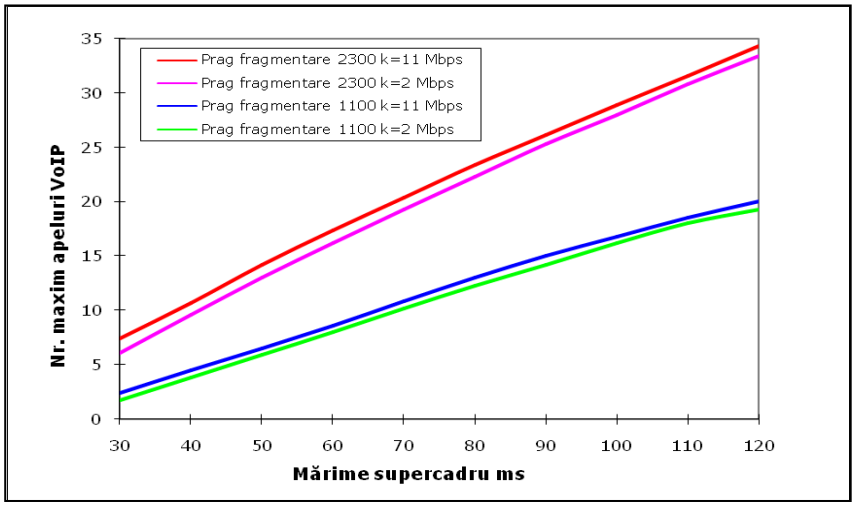


Fig.3.12. Numărul maxim de apeluri

De exemplu, pentru durata supercadrului de 90 ms, pot fi admise 14 respectiv 26 apeluri într-o reţea locală (LAN) de 2 Mbps respectiv 11 Mbps. Am observat că pragul de aplicare al fragmentării nu are un efect semnificativ asupra numărul maxim de apeluri vocale, care pot fi admise pentru fragmente care utilizează dimensiuni relativ mari, Fig.3.12. Tabelul 6 compară numărul maxim de apeluri admisibile în modul CBR (N_P) şi VBR mod (N_S) utilizând atât modelul Brady cât şi modelele de voce Zebo pentru supercadre de 75 ms şi 90 ms. Cu astfel de mărimi ale supercadrelor, presupunerea că un pachet ar trebui declarat pierdut dacă nu a servit într-un supercadru se menţine.

Tabelul 6. Numărul maxim de apeluri vocale B (model Brady), MZ (May and Zebo)

T_{SF} (ms)	FH (2Mbps)			DS (11Mbps)		
	N_p	N_s (B)	N_s(MZ)	N_p	N_s (B)	N_s(MZ)
75	12	22	27	22	41	51
90	14	26	32	27	52	65

Având în vedere că modul de transmisie cu rată variabilă (VBR) exploatează pauzele dintr-o convorbire, dimensiunea maximă a unui pachet de voce este mai mare decât valoarea $c*(T_{SF}+P_{min})$ pe care am presupus-o. De asemenea, în timp ce numărul maxim de apeluri care poate fi efectuat în modul VBR este aproximativ dublu faţă de cele ce pot fi efectuate în modul CBR, întârzierile sunt mai mari în modul VBR. Întârzierile pentru ambele direcţii k1→k2 şi k2→k1, pentru ambele fluxuri, 2 Mbps şi 11 Mbps, sunt prezentate în Fig. 3.13.

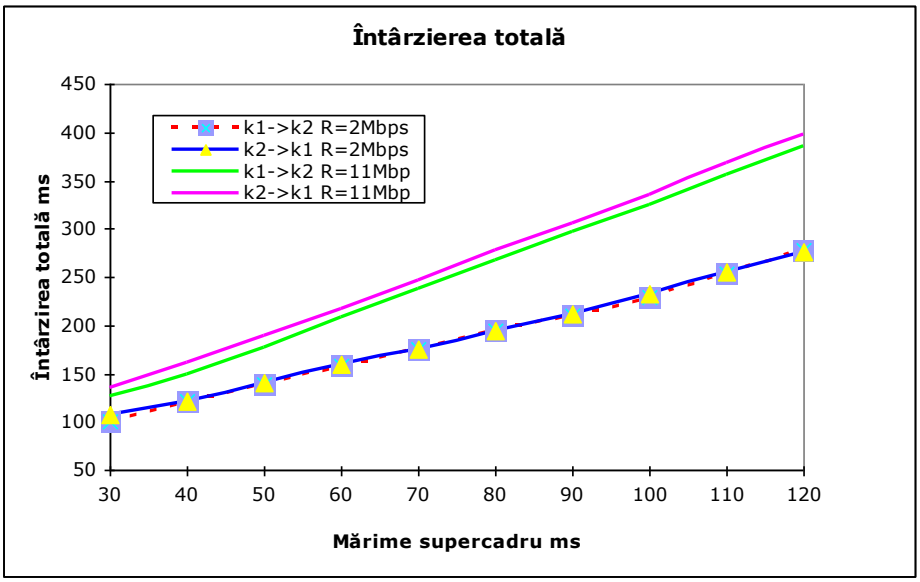


Fig.3.13. Întârzierea totală

De exemplu, în cazul în care este utilizată o dimensiune de supercadru de 90 ms, întârzierile totale de 121 şi 303 ms se vor reflecta în sensurile de la k1→k2 şi k2→k1, pentru această porţiunea de apel vocal a standardului IEEE 802.11 (într-un LAN de 11 Mbps).

3.7. Analiza erorilor în protocolul MAC 802.11

Protocolul MAC 802.11 retransmite datele pentru a gestiona erorile din ambele moduri PCF şi DCF. Cu toate acestea, retransmisia este de obicei evitată pentru traficul în timp real, datorită constrângerilor impuse de întârzieri. În această lucrare voi argumenta necesitatea unei forme de corecţie a erorilor pentru traficul de voce. Această analiză ia în considerare cele două modele de atenuare a erorilor. Ambele sunt de tipul unor lanţuri Markov cu două intervale de timp continuu, după cum se arată în Fig. 3.14 [39]. Parametrii pentru cele două modele sunt prezentate în tabelul 6.

Tabelul 7. Parametrii pentru simulare modele de eroare

Model	BER_G	BER_B	α	λ
1	10^{-10}	10^{-5}	10/sec	30/sec
2	10^{-4}	10^{-2}	20/sec	10/sec

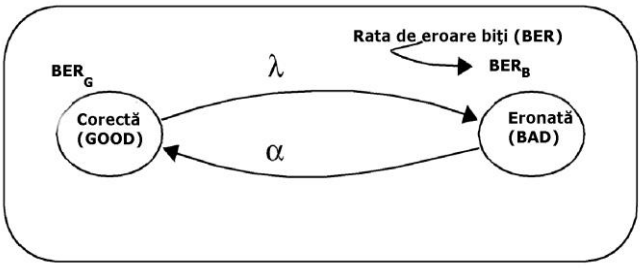


Fig.3.14. Model de canal pentru reţele fără fir

Primul model de eroare utilizat pentru a caracteriza atenuarea de semnal este prezentat în Fig.3.14, [39]. Al doilea model este mai realistic, cu o rată de eroare a biţilor mai mare. Timpul de menţinere este estimat grosier.

Timpul necesar pentru a transmite un pachet de voce cu informaţii utile de v biţi este dat de ecuaţia de mai jos

$$T_{v-pkt} = \frac{(v+h+P)}{R} \tag{3.47}$$

Sunt posibile trei cazuri:

Cazul 1: Când începe transmiterea unui pachet de voce canalul este în stare bună şi nu există nici o tranziţie înainte de a se termina transmisia;

Cazul 2: Când începe transmiterea unui pachet de voce canalul nu este în stare bună şi nu există nici o tranziţie înainte de a se termina transmisia;

Cazul 3: Toate celelalte posibilităţi; începe transmiterea unui pachet de voce canalul fiind în stare bună sau nu şi există una sau mai multe tranziţii înainte de a se termina transmisia.

Utilizând proprietatea distribuţiei exponenţială de a nu ţine cont de evenimete trecute şi neglijând întârzierea de propagare, probabilităţile din cele trei cazuri pot fi derivate astfel:

$$p_{caz1} = p_G P(G > T_{v-pkt}) = \frac{\alpha}{\alpha+\lambda} e^{-\lambda Tv-pkt} \tag{3.48}$$

$$p_{caz2} = p_B P(B > Tv-pkt) = \frac{\alpha}{\alpha+\lambda} e^{-\lambda Tv-pkt} \tag{3.49}$$

$$p_{caz3} = 1 - p_{caz1} - p_{caz2} \tag{3.50}$$

unde P_G şi P_B sunt probabilităţi de începere a unei transmisii de pachete în cazul în care canalul este în stare bună sau rea şi sunt date de:

$$p_G = \frac{\alpha}{\alpha+\lambda} \qquad p_B = \frac{\lambda}{\lambda+a} \tag{3.51}$$

Probabilitatea de eroare a pachetelor pentru cele cazuri este aproximată de:

$$\varepsilon_{caz1} = 1 - \left(1 - BER_G\right)^{(v+h+P)} \tag{3.52}$$

$$\varepsilon_{caz2} = 1 - \left(1 - BER_B\right)^{(v+h+P)} \tag{3.53}$$

$$\varepsilon_{caz2} \le \varepsilon_{caz3} \tag{3.54}$$

Combinând probabilităţile din cele trei cazuri, date de relaţiile (3.40) la (3.42), cu probabilitatea de eroare a pachetelor, în cele trei cazuri, rezultă probabilitatea totală de eroare a pachetelor conform inegalităţii de mai jos:

$$p_e \le \left(\begin{array}{l} p_{caz1}\varepsilon_{caz1} + p_{caz2}\varepsilon_{caz2} \\ + p_{caz3}\varepsilon_{caz3} \end{array} \right) \tag{3.55}$$

Cazul cel mai dezavantajos este cel în care rata de eroare este cea mai mare iar toţi biţii sunt supuşi BER_B .

În modul de transmisie CBR mărimea cea mai mare a pachetelor este dată de:

$$v = c\left(T_{SF} + P_{min}\right) \tag{3.56}$$

Fig.3.15. reprezintă limita superioară a probabilităţii p_e faţă de T_{SF} pentru modelele de eroare 1 şi 2.

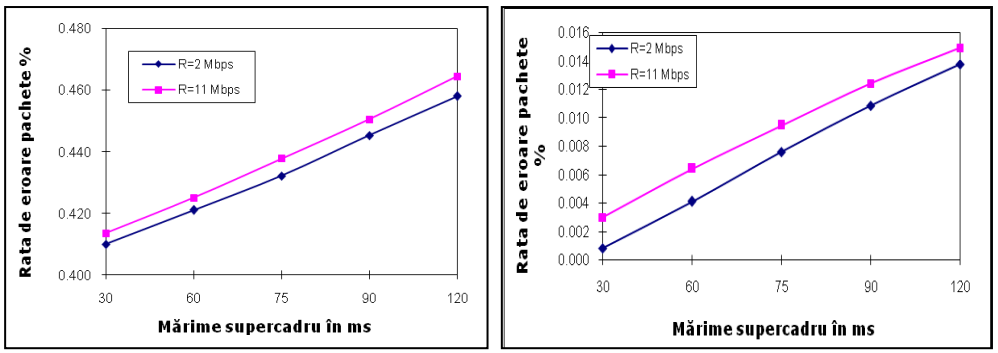


Fig.3.15. Rata de eroare a pachetelor

Reţeaua de 11 Mbps prezintă o rată de eroare mai mare a pachetelor, chiar dacă timpul de transmisie al pachetelor ar fi de aşteptat să fie mai scurt datorită ratei mai mari a datelor. Acest lucru se datorează faptului că pachetele care folosesc transmisia prin spectrul cu secvenţă directă DS (direct sequence) au un preambul mai mare decât cele prin FHSS (frequency hopping).

Pentru T_{SF} egal cu 90 ms, avem o rată de eroare a pachetelor de aproximativ 10^{-2} pentru modelul 1 şi 0.44 pentru modelul 2, fapt ce se poate observa chiar din grafice. Pentru voce, cu o toleranţă de pierdere de 10^{-3}, aceste rate de erori sunt mari. Acest lucru indică necesitatea corecţiei erorilor.

3.8. Concluzii

Deoarece capabilitatea funcţiei de coordonare prin punct (PCF) a protocolului MAC al standardului IEEE 802.11 de a transporta trafic telefonic a fost mai puţin analizată, în acest capitol am prezentat o cercetare referitoare la acest aspect. **Folosind o conexiune cu un algoritm pentru controlul admiterii care să gestioneze numărul de apeluri vocale admise pe lista de interogare, reţeaua poate asigura întârzieri garantate. Cel mai simplu mod de funcţionare al unui LAN în timpul funcţiei de coordonare distribuită(PCF) este cel cu o rată constantă de biţi (CBR).** În acest mod, dacă de la un utilizator vocal nu există semnal, timpul alocat nu este repartizat unei alte convorbiri sau pentru un transfer de date. Evident, acest lucru limitează numărul de apeluri care pot fi admise, dar în realitate limitează jitter-ul de întârziere şi prin aceasta întârzierea maximă admisă, modul CBR permiţând un număr rezonabil de apeluri care urmează să fie efectuate. De exemplu, cu o viteză de 11 Mbps într-un LAN IEEE 802.11 pot fi admise 26 apeluri vocale, în cazul în care dimensiunea supercadrului este de 90 ms, la o întârziere maximă de 303 ms. De asemenea, în acest mod, apelurile vocale cu timpi de întârziere diferiţi (de exemplu, apeluri intra-LAN sau apeluri către utilizatorii din reţelele fixe (PSTN) către telefoane VoIP) pot fi posibile prin modificarea numărului de prezenţă al apelului într-o lista de interogare. De asemenea am făcut o analiză a erorilor, care indică faptul că pachetele de voce pot avea o rată mare de eroare, fapt ce impune retransmisia datelor.

Tot în acest capitol am prezentat şi un studiu axat pe propunerea unui nou contor adaptiv pentru retransmisie, care este reglabil la dimensiunea pachetelor de semnalizare implicate în stabilirea unei sesiuni de apel vocal. Folosind un model analitic, am evaluat timpul mediu necesar sesiunii de configurare SIP în funcţie de rata de eroare (FER) a legăturii radio şi de puterea de procesare a serverelor şi sursa/destinaţia terminalelor (cozile de aşteptare). Alegerea protocolului datagramă (UDP) sau TCP pentru transportul mesajelor SIP influenţează sesiunea de iniţializare pentru o rată de eroare a cadrelor (FER) mai mare de 2 %. Folosirea UDP în loc de TCP poate reduce sesiunea de iniţializare cu 10 % pentru erori ale cadrelor mai mari de 4 %.

Mecanismele de retransmisie de la nivelul straturilor inferioare, cum ar fi protocolul pentru legături radio RLP, îmbunătăţesc considerabil întârzierile sesiunii de iniţializare. În medii cu rată de eroare mare, întârzierea sesiunii de iniţializare pentru protocolul pentru legături radio rămâne mică (4-7s).

RLP(1,2,3) surclasează RLP(1,1,1 ,1,1,1) numai pentru rate ale erorilor mai mari de 3-4 %. **Cu ajutorul contorului adaptiv pentru retransmisie, SIP prezintă întârzieri mai mici decât H.323 pentru rate de erori mai mari de 2%. Pentru rate de erori mai mici sau egale cu 2% protocolul H.323 este mai performant decât SIP datorită contorului adaptiv pentru retransmitere, ajustabil cu mărimea mesajului. Prin urmare, contorul adaptiv pentru retransmitere este eficient în general pentru optimizarea performanţelor protocoalelor de semnalizare.** Performanţa SIP folosind contorul adaptiv pentru retransmitere ar putea fi îmbunătăţită suplimentar şi prin utilizarea unor sisteme de compresie, pentru a reduce mărimea mesajelor SIP. De asemenea, mecanisme de corecţie a erorilor ar putea îmbunătăţi performanţa timpului de iniţializare al unei sesiuni VoIP prin corecţia mesajelor SIP şi evitarea retransmisiilor pe legătura fără fir.

4. SOLUŢII PENTRU ASIGURAREA SECURITĂŢII ÎN REŢELELE WIRELESS

O comunicaţie sigură între două părţi, printr-un mediu nesigur aşa cum este Internet-ul este una dintre cele mai importante probleme de securitate.

Pachetele de date conţinând informaţii legate de transmiterea vocii în timpul unui apel VoIP sunt rutate, în general, nesecurizat prin reţeaua publică de telecomunicaţii fixă sau mobilă. Există software care poate capta, reconstrui şi/sau modifica aceste apeluri.

Standardul IEEE 802.11 oferă suport limitat de confidenţialitate, prin utilizarea protocolului cu cheie partajată preluat din reţelele fixe (Wired Equivalent Privacy WEP), care conţine erori semnificative în proiectare [35].

Datorită faptului că reţelele fără fir pot oferi puncte de acces în reţea pentru orice intrus (dincolo de nivelul fizic şi dincolo de controalele de securitate ale organizaţiei), se impun măsuri de securitate sporite care să evite astfel de situaţii. Prin limitarea conexiunilor externe la câteva, bine securizate, se poate asigura o protecţie mai bună. Din păcate, desfăşurarea traficului printr-o reţea fără fir permite unui atacator accesul fizic în afara perimetrului de securitate al unei organizaţii. Ca rezultat, un atacator poate pune în aplicare un atac de tip "parking lot" ca în Fig.4.1, adică atacatorul stă în exteriorul clădiri, în aşa numita "parcare-parking lot" şi accesează gazdele (host) din intranet. Acest tip de atac este acela în care un intrus încearcă să înregistreze şi să observe traficul de reţea din afara perimetrului unui imobil, în scopul de a fura informaţii sensibile şi de valoare.

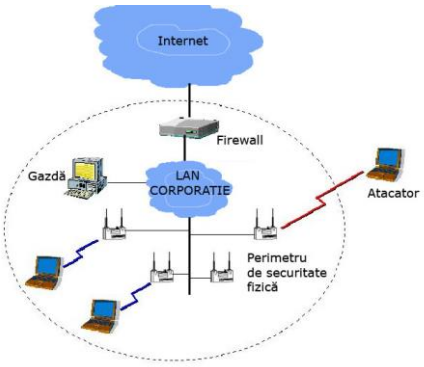


Fig.4.1. Atacul prin ascultare din exteriorul unei clădiri [26]

Pornind de la necesitatea de a asigura securitatea datelor în sistemele care utilizează reţelele fără fir ca suport pentru transmiterea VoIP, în acest capitol, sunt prezentate două contribuţii care conduc la îmbunătăţirea securităţii şi mobilităţii aplicaţiilor VoIP. Prima contribuţie vizează un software pentru securitatea şi mobilita

tea sistemelor VoIP, iar cea de-a doua contribuţie implementează un sistem criptografic pentru o comunicaţie sigură client-server.

Capitolul este structurat în cinci paragrafe. În primul paragraf sunt prezentate succint principalele probleme ale VoIP, protocoalele existente şi măsurile de securitate care ar trebui luate pentru o comunicaţie sigură. Paragraful 4.2 descrie standardul IEEE 802.11. Este prezentată o imagine de ansamblu a securităţii standardului IEEE 802.11 şi a extinderii mecanismelor de control al accesului.

Expunerea motivelor alegerii IAX ca şi protocol pentru o transmisie sigură VoIP este prezentată în paragraful 4.3. În paragraful 4.4 este dezvoltat un sistem care utilizează diverse moduri de criptare pentru a determina care este cel mai adecvat pentru a asigura atât calitatea apelului cât şi utilizarea cât mai redusă a resurselor procesorului. Paragrafele 4.5 prezintă o aplicaţie particulară a utilizării serviciilor VoIP, distribuţia multiplă a vocii cu mai multe salturi. În paragrafele 4.6-4.9 sunt investigate avantajele unei distribuţii multiple a vocii în cazul conferinţelor cu mai mulţi participanţi, aflaţi în locaţii diferite. Sunt analizate limitările datorate transmisiei prin mai multe puncte cu staţii ascunse. Concluziile capitolului sunt incluse în paragraful final.

4.1 Securitatea VoIP

Pachetele de date conţinând informaţii legate de transmiterea vocii în timpul unui apel VoIP sunt rutate, în general, nesecurizat prin reţeaua publică de telecomunicaţii fixă sau mobilă. Există software care poate capta, reconstrui şi/sau modifica aceste apeluri. Standardele VoIP oferă numeroase oportunităţi de implementare a unor softuri care să permită hackerilor interceptarea conversaţiilor cum ar fi:

- ascultarea şi înregistrarea apelurilor telefonice;
- urmărirea apelurilor;
- furtul de informaţii confidenţiale;
- modificarea apelurilor telefonice;
- efectuarea de apeluri telefonice gratuite;
- trimiterea de spam (voce sau e-mail).

În acest moment există pe piaţă mai multe standarde VoIP (SIP, IAX şi H.323) şi foarte puţine standarde de securitate disponibile pentru ele. Instalarea standard a VoIP, folosind protocoalele SIP, H.323 sau IAX nu oferă nici un fel de securitate pentru traficul de voce. Pentru a evita acest lucru, este necesar să se adauge o formă de protecţie, cum ar fi criptarea, la nivel de reţea sau de transport. Pentru transmisia sigură a VoIP prin reţelele fără fir ar trebui ca fiecare strat de reţea să aibă mecanisme care să asigure securitatea informaţiilor. Dispozitivele VoIP ar trebui de asemenea securizate, reţeaua ar trebui izolată, traficul criptat, precum şi introducerea unor sistemele de detecţie a intruşilor [21]. Încorporarea de sisteme de securitate la fiecare nivel de reţea, ar face mult mai dificil succesul hackerilor. Astfel, crearea unei breşe de securitate la un nivel al reţelei nu va expune întreaga reţea. Vor fi necesare mai multe breşe pentru a compromite sistemul de protecţie al reţelei.

Este esenţial ca astfel de soluţii să fie integrate în VoIP-ul standard. Deoarece protocoalele VoIP utilizează deja opţiuni de negociere pentru a stabili parametrii de apel (de exemplu codec-uri), este rezonabil ca parametrii de securitate să poată fi stabiliţi în mod asemănător.

Pentru a oferi servicii VoIP pe dispozitive mobile, este necesar să se ia în considerare restricţiile impuse de sistemele fără fir. Dispozitivele mobile au limitată

puterea de procesare, durata de funcţionare (depind de acumulator), de memorare, de stocare, de conectivitate la reţea şi performanţă.

4.2 Soluţii de securitate pentru reţelele fără fir

Reţele fără fir funcţionează în una din cele două moduri ad-hoc sau infrastructură. Standardul IEEE 802.11 defineşte modul ad-hoc, ca set de servicii de bază independente (Independent Basic Service Set-IBSS) şi modul infrastructură ca Set de Servicii de Bază (Basic Service Set BSS). În modul ad-hoc, fiecare client comunică direct cu alţi clienţi din cadrul reţelei, a se vedea Fig.4.2. Modul ad-hoc este conceput astfel că numai clienţii din aceeaşi celulă pot comunica între ei.

Fig.4.2 a) Exemplu de reţea ad–hoc b) Exemplu de infrastructură de reţea

În cazul în care un client dintr-o reţea ad-hoc, doreşte să comunice în afara celulei, un membru al celulei trebuie să funcţioneze ca o poartă şi să efectueze rutarea. În modul infrastructură, fiecare client trimite toate informaţiile de comunicaţii la o staţie centrală sau punct de acces (AP). Punctul de acces acţionează ca o punte de legătură Ethernet şi redirecţionează comunicaţiile la o reţea apropiată fixă sau mobilă, a se vedea Fig.4.2.

Înainte de a comunica date, clienţii reţelelor mobile şi punctele de acces trebuie să stabilească o relaţie sau o asociere. Numai după ce o asociere este stabilită cele două staţii de radio pot face schimbul de date. În modul infrastructură, clienţii sunt asociaţi punctelor de acces. Procesul de asociere este un proces care implică trei stări:

1. neautentificat şi neasociat;
2. autentificat şi neasociat;
3. autentificat şi asociat.

Pentru a tranzita între stări, părţile care comunică fac un schimb de mesaje numit management de cadre. Un client al reţelei fără fir va căuta şi va fi asociat unui punct de acces. Toate punctele de acces transmit un cadru de management pentru ascultare, la intervale fixe de timp. Pentru a se asocia cu un punct de acces şi a se alătura unei BSS, un client ascultă mesajele din reţea până identifică cadrul de date ce conţine informaţii legate de punctul de acces în a cărui rază de acoperire intră. Clientul selectează BSS pentru a se alătura într-o manieră independentă. De exemplu la reţele de tipul Apple-Macintosh, toate numele de reţea (sau set de servicii de identificare SSID), sunt, de obicei, conţinute în cadrul de balizaj şi sunt prezentate utilizatorilor, astfel încât aceştia să poată alege reţeaua la care să se alăture. Un client poate, de asemenea, trimite un cadru de balizaj pentru a găsi un punct de acces afiliat cu un SSID dorit. După identificarea unui punct de acces, clientul şi punctul de acces vor efectua o autentificare prin schimbul reciproc de mai multe cadre de management, ca parte a procesului. După succesul autentificării, clientul tre-

ce în cea de-a doua stare, autentificare şi neasociere Trecerea de la cea de-a doua stare la cea de-a treia şi finală, autentificare şi asociere, presupune ca, clientul să trimită un cadru de cerere de asociere, iar punctul de acces să răspundă cu un cadru de asociere. După ce se parcurg paşii descrişi mai sus, conform procesului descris anterior, clientul devine parte a reţelei fără fir, şi poate transmite cadre de date prin reţea.

Standardul IEEE 802.11 oferă mai multe mecanisme pentru un mediu de operare sigur cum ar fi cele descrise mai jos [65]:

4.3. Alegerea protocolului IAX ca şi soluţie pentru securitatea VoIP

Au fost mai multe încercări de securizare a serviciilor oferite de protocoalele VoIP, dar, din păcate, au exista următoarele probleme:

- sunt complicate pentru a fi implementate şi menţinute;
- se bazează pe soluţii oferite de una sau un grup restrâns de firme care îşi arogă drepturi de proprietate asupra lor, iar orice altă variantă nu este compatibilă cu cea furnizată;
- au nevoie de existenţa unei infrastructuri pentru cheile publice Public Key (PKI) şi/sau alte resurse;
- probleme de rutare la trecerea prin translatarea adreselor de reţea NAT.

Inter-Asterisk Exchange Protocol (IAX) este un nou protocol care a fost dezvoltat pentru softul open source al centralelor PABX (Centrale telefonice de abonat) cunoscut sub numele de Asterisk [66]. Acest protocol a fost creat ca o alternativă de semnalizare la protocolul SIP şi H.323. În prezent câştigă tot mai mult teren pe piaţa VoIP şi promite o spectaculoasă ascensiune în viitorul apropiat. Principalele caracteristici ale IAX sunt [66]:

- se poate optimiza foarte bine, funcţie de cerinţele existente ale VoIP;
- eficienţă superioară faţă de H.323 şi SIP pentru traficul VoIP;
- utilizează eficient lăţimea de bandă atât pentru semnalizare cât şi pentru transferuri mass-media;
- suport nativ pentru tehnologia de translaţie a adreselor de reţea (Network Address Translation-NAT). Are capacitatea de a partaja un singur număr de port şi de a transfera toate datele printr-un port UDP cunoscut;
- protocol unic de transfer mass-media. Toate apelurile de semnalizare pentru informaţii, secvenţiere şi temporizare sunt incluse în cadrele IAX transferate;
- scris într-o manieră uşoară;
- proiectat pentru a fi uşor de pus în aplicare;
- poate fi folosit cu orice tip de flux media de date (inclusiv video).

Inter-Asterisk eXchange (IAX) este un protocol IP care transportă fluxuri de date media. Pentru a iniţializa o conversaţie între doi utilizatori via IP, se foloseşte protocolul IAX ca metodă de transport semnal audio.

Pentru a crea un canal IAX a fost nevoie de iniţierea unei comunicaţii IAX în fişierul de configurare iax.conf. În primul caz am iniţializat pentru IAX parametrii globali, Fig.4.5.

```
[general]
port=4569 ; What port to bind to (4569 is the default for IAX2)
bindaddr=192.168.1.2; Which IP address on your server to bind to (if
; you have multiple NICs on your sever, you can
; restrict IAX2 to only one of them. 192.168.1.2 will
; allow it to work on all NICs in your system.
deny=all; You want to disallow the use of all audio
; codecs to ensure that
; your system won't tell the far end that it can
; support just any codec. Then, you specifically ALLOW
; the codecs that your system supports.
allow=alaw; The rest of the world's companding standard for G.711
```

Fig.4.5. Secvenţă stabilire canal comunicaţie

4.3.1. Definirea canalelor IAX

După ce am definit parametrii globali ai interfeţei protocolului IAX spre exterior, am putut crea canalele IAX care sunt foarte flexibile şi se pot conecta cu succes la orice tip de punct final. Deşi nu este un protocol standard, este extrem de mult utilizat Fig.4.6. Mulţi prevăd că IAX va înlocui SIP.

```
[general]
port=4569 ; What port to use
bindaddr=192.168.1.2; What IP address to bind to
allow=all; Allow the use of all audio codecs
register=> username:secret@kiax.com ;
replace username:secret with your credentials, kiax-out
type=peer; Allow connections out
username=username; TYour KiaxTel username
secret=password; Your secrepassword
deny=192.168.1.2/192.168.1.2; Not just anyone can be Kiax
permit=216.207.245.47/255.255.255.255 ; This is a server at Kiax
permit=69.73.19.178; This is a server at Kiax
[kiax-in]
type=user; Allow connections to come in
context=default ; Route calls to this context; in the dialplan
username=username; The IAX username
secret=password; The secret password
```

Fig.4.6. Secvenţa de cod de negociere conexiune Kiax şi utilizator

După cum se vede sunt necesare 2 intrări pentru a putea comunica cu serviciile oferite de Kiax. Kiax este un serviciu VoIP de apel gratuit şi este folosit ca su-

port de test pentru Asterisk şi ca un sistem comun de comunicare. Prima schimbare care se observă este în secţiunea generală. Este o linie care îi spune Kiax unde este apelantul, iar apelurile către utilizatorul IAX trebuie rutate prin server–ul asterisc.

Sunt 2 tipuri diferite de conexiuni ale Kiax, una de tip pereche (peer) şi alta de tip utilizator. Acest lucru permite să se poată decide dacă pentru apelurile de intrare se utilizează un server şi pentru cele de ieşire alt server. Acest lucru este extrem de util atunci când se manipulează o reţea mare de servere Asterisk şi este utilizat IAX pentru departajarea lor.

4.3.2. Securitatea IAX

S-a demonstrat că IAX este un protocol mult mai eficient faţă de SIP şi H.323 atunci când rulează nesecurizat [66]. Noutatea care o prezintă această teză este inserarea unui modul de securitate suplimentar în softphon-ul Kiax pentru asigurarea securităţii la translatarea adreselor (NAT).

4.3.3. VoIP–consideraţii de calitate

Parametrii care sunt asociaţi în mod normal cu noţiunea de calitate sunt cunoscuţi sub denumirea de caracteristicile de calitate ale serviciului. Datele care conţin informaţiile de voce traversează o reţea cu, comutare de pachete. Prin aceasta se va produce un trafic la diferite nivele, necesitând astfel asigurarea anumitor indicatori de performanţă operaţională. Întârzierile, bruiajul şi pierderea de pachete sunt folosite ca măsuri intrinseci ale QoS (Quality of Service) [65].

4.3.4. Codec–uri audio

Toate tehnologiile VoIP se bazează pe un codec care transformă semnalele analogice în semnale digitale sub formă de pachete de voce. Alegerea codec-ului este un compromis între calitatea vocii, puterea de procesare şi cerinţele de lăţime de bandă. O selecţie de codec-uri VoIP frecvent utilizate este dată în Tabelul 8 de mai jos [16]:

Tabelul 8. Comparaţie caracteristici codec-uri [16]

	Rata eşantionare (kHz)	Viteza de transmitere (kbps)	Multiplicare	VBR	PLC	Licenţa
Speex	8, 16, 32	2.15; 24.6;	Da	Da	Da	Sursa liberă/deschisă
iLBC	8	15.2; 13,3	Nu	Nu	Da	Sursa liberă/deschisă
AMR	8	4.75 or 12.2	Da	Nu	Da	Proprietar
G.729	8	8	Nu	Nu	Da	Proprietar
GSM	8	13	Nu	Nu	No	Patent
G. 723.1	8	5.3 or 6.3	Nu	Nu	Da	Proprietar

	Rata eşantio-nare (kHz)	Viteza de transmitere (kbps)	Multi-plicare	VBR	PLC	Licenţa
G.728	8	16	No	Nu	Nu	Proprietar

În scopul de a oferi siguranţă transmiterii de date este necesar a se asigura confidenţialitatea şi autentificarea lor. Cu alte cuvinte, datele trebuie să fie sigure şi să nu fie dezvăluite decât unei părţi autorizate. Pentru a putea utiliza diferite codecuri, algoritmii de criptare trebuie să fie capabili să suporte cadre de date cu informaţii utile transmise la o frecvenţă mare (aproximativ 30-100 octeţi de 50 de ori pe secundă). Deoarece informaţia utilă este de lungime relative mică ar fi avantajos să se folosească o metodă de criptare care să nu crească dimensiunea datelor ce urmează a fi trimise. Orice creştere nesemnificativă a informaţiei utile se va adăuga ca un plus la transmisie.

4.3.5. Clienţi mobili

În această lucrare am realizat un client VoIP sigur, care să poate fi rulat pe un dispozitiv mobil, cum ar fi un PDA sau telefon inteligent. Deoarece nu există în prezent un client mobil IAX Open Source, adecvat pentru testare, am folosit un laptop. În tabelul de mai jos se compară un laptop cu dotare minimă cu un PDA de nivel înalt [40].

Tabelul 9. Comparaţie CPU laptop şi PDA

Nume dispozitiv:	IBM X30 Laptop	DellAxim X51PDA
Producător CPU:	Intel	Intel
Viteza CPU:	800 MHz	624 MHz
RAM disponibil:	512MB	64MB
Rata MIPS:	2142	800
Comparaţie MIPS:	1.0	0.37

Deşi utilizarea MIPS (milioane de instrucţiuni pe secundă) nu ia în considerare diferitele seturi de instrucţiuni ale procesoarelor, este adesea folosită pentru a indica un rating de performanţă aproximativ. Pe baza unei simple comparaţii a MIPS, un PDA Dell Axim X51 este capabil să execute 37% din operaţiunile pe care le poate face un laptop IBM X30.

4.4. Proiectarea şi implementarea unor măsuri de securitate suplimentare protocolului IAX

Această teză aduce ca noutate implementarea unor măsuri de securitate la nivelul protocolul IAX, înainte de a fi implementat clientul VoIP. Pentru aceasta am selectat un client open source, am examinat codul şi identificat un punct de inserţie

pentru a adăuga codul de securitate. Instrumentele şi metodologia de realizare a acestui lucru sunt descrise mai jos.

4.4.1. Kiax Client-VoIP

Kiax este un softphone open source conceput pentru a utiliza exclusiv IAX. Ca la mulţi alţi clienţi IAX pentru open–source, Kiax se bazează pe biblioteca "libiax" pentru asigurarea funcţiilor aferente nivelurilor de jos ale unei reţele. Această bibliotecă a fost construită de către factorii de decizie ai Asterisk şi este frecvent folosită de către clienţii IAX open source. Modificările de cod necesare pentru a sprijini algoritmii de criptare sunt cerinţele cele mai des solicitate bibliotecilor libiax.

4.4.2. Cryptlib

Cryptlib este un pachet criptografic OpenSource, de uz general, fiind conceput să ofere servicii de securitate pentru aplicaţii.

Cryptlib oferă o interfaţă standardizată pentru o serie algoritmi de criptare populari. Permite ascunderea în cea mai mare parte a detaliilor de implementare şi foloseşte un sistem de codare independent de sistemul de operare, fapt ce facilitează transferul de date securizate de la un mediu de operare la altul.

La cel mai de jos nivel sunt componentele de bază, cum ar fi rutinele de criptare şi autentificare, care sunt, de obicei, folosite în aplicaţiile software, dar pot fi, de asemenea, incluse în partea de hardware (ca urmare a vitezei componentele software folosite în Cryptlib sunt de obicei mai rapide decât hardware–ul dedicat). La nivelul următor sunt componentele dedicate şi adesea, destul de complexe, care oferă funcţionalitate şi asigură portabilitatea datelor pentru orice tip de platformă utilizată. Aceste funcţii se referă de obicei la domenii care implică crearea unei semnături digitale sau a unei chei de criptare de schimb. La cel mai înalt nivel sunt foarte puternice şi uşor de utilizat, funcţii cum ar fi: criptează un mesaj, semnează un mesaj, deschide o legătură securizată şi creează un certificat digital. Nu necesită cunoştinţe de tehnici de criptare şi totodată gestionează procesele complexe cum ar fi cheia de management, codificarea datelor, criptarea şi decriptarea şi semnătura digitală.

Managementul interfeţei Cryptlib asigură posibilitatea de a adăuga capabilităţi de criptare şi de autentificare la o aplicaţie fără a fi nevoie să se ştie toate detaliile de nivel inferior ale criptării sau autentificării. Rutina de lansare automată a managementului se ocupă de problemele de codificare şi de portabilitatea pentru diverse platforme (cross-platform). Are funcţii care pe de o parte codează şi criptează datele la un capăt iar la celălalt le recreează aşa cum au fost ele iniţial. Acest lucru oferă un avantaj considerabil faţă de alte unelte (toolkit-uri) de criptare care necesită adesea sute de linii de cod şi de manipulări complexe de criptare a datelor pentru a obţine acelaşi lucru.

Principalul său scop este de a furniza funcţii criptografice care pot fi integrate în aplicaţii. Modelul Cryptlib se bazează pe o structură de straturi care să poată oferi diferite niveluri de control utilizatorului. Prin utilizarea Cryptlib, au fost posibile o varietate de experimente cu metode de criptare diferite pentru a evalua impactul acestora asupra performanţei. Arhitectura completă a unei astfel de diagrame este prezentat în Fig.4.7, de mai jos [40]:

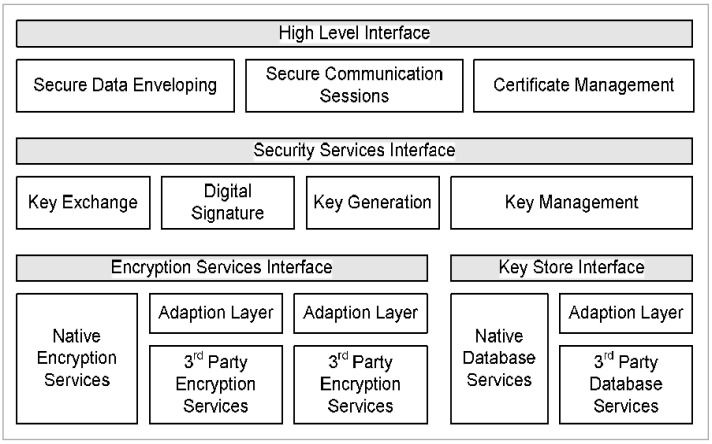


Fig.4.7. Arhitectura diagramei Cryptlib [40]

4.4.3. Descrierea soluţiei

Diagrama bloc de mai jos oferă o descriere pe straturi a soft–ului de bază, aferent unei structuri Kiax. Fig.4.8 de mai jos, arată arhitectura iniţială a Kiax.

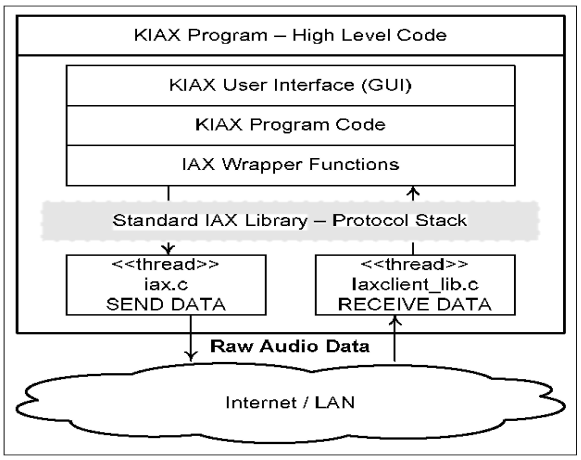


Fig.4.8. Kiax-Arhitectura standard [67]

Kiax oferă o interfaţă de tip grafic utilizatorului, care comunică setările şi preferinţele codului sursă al Kiax.

Programul protocolului de nivel inferior al IAX este furnizat sub forma unei biblioteci standard, cunoscută sub denumirea de bibliotecă libiax.c. Această bibliotecă este de asemenea responsabilă pentru codarea şi transportul datelor audio capturate de la utilizatori. Versiunea modificată a Kiax, care constituie noutatea adusă clientului Kiax, adaugă un strat suplimentar de prelucrare a fluxului audio. Datele

audio au fost codificate prin intermediul codec-ului audio, încapsulate şi criptate înainte de a fi transmise prin reţea. La receptor semnalul audio este decriptat şi apoi prelucrat de stiva de protocoale a Kiax, conform Fig.4.9.

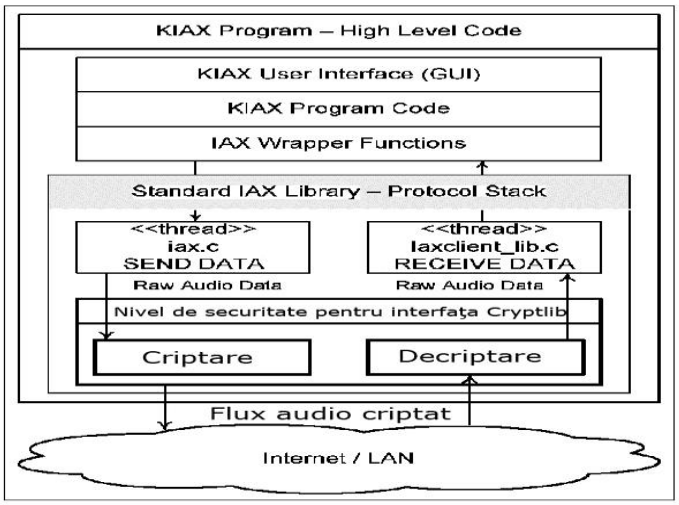


Fig.4.9. Kiax–Arhitectura modificată [40]

Cryptlib este construit în jurul unui nucleu de securitate. Acest nucleu asigură interfaţa între utilizator şi arhitectura obiectelor (securitate intra-obiect), precum şi între obiecte ele însele (securitate inter-obiect). Nucleul de securitate este baza întregii arhitecturi cryptlib. Toate obiectele sunt accesate şi controlate prin intermediul acesteia, precum şi toate atributele obiectelor sunt manipulate prin ea. Nucleul este implementat ca un strat de interfaţă situat în partea de sus a obiectului, monitorizând toate accesele şi manipulând toate funcţiile de protecţie. Fiecare obiect cryptlib este conţinut în întregime în cadrul perimetrului de securitate, astfel că datele şi informaţiile de control pot doar să intre şi să iasă într-o manieră foarte bine controlată, obiectele fiind izolate unele de altele în perimetrul de securitate de către nucleu. De exemplu, o dată ce informaţiile au fost trimise la un obiect, nu pot fi aduse de către utilizator înapoi decât în conformitate cu nişte condiţii de excepţie bine controlate. În general informaţia nu este vizibilă pentru utilizator, deoarece este generată în interiorul obiectului şi nu iese din perimetrul de securitate.

Asociat fiecărui obiect este un set de liste de control al accesului (ACL-uri) obligatorii care determină cine poate accesa un anumit obiect şi condiţiile în care accesul este permis. În cazul în care sistemul de operare permite aceasta, toate informaţiile sensibile vor fi de tipul page-locked pentru a se asigura că acestea nu vor fi copiate niciodată pe disc cu ajutorul unui editor de disc. Toată memoria alocată securităţii datelor este gestionată de cryptlib şi va fi în mod automat gestionată şi eliberată, atunci când acesta se închide, chiar şi în cazul în care un program care l-a apelat uită să elibereze memoria.

În cazul în care sistemul de operare suportă, cryptlib va aplica caracteristicile de securitate ale sistemului de operare la orice obiect pe care îl creează sau gestionează. De exemplu, sub Windows XP fişierul pentru cheile private ale cryptlib va fi creat cu o listă de control al accesului (ACL) care permite accesul la folder doar

cheii de acces a proprietarului. Sub UNIX fişierul cu permisiunile va fi stabilit astfel încât să se obţină acelaşi rezultat.

Pentru criptare am folosit secvenţa de mai jos cu o cheie publică de criptare Fig.4.10

```
/* Create an envelope for the message */
cryptCreateEnvelope( &cryptEnvelope,cryptUser, CRYPT_FORMAT_SMIME );
/* Push in the message recipient's name */
cryptSetAttribu-
teString(cryptEnvelope,CRYPT_ENVINFO_RECIPIENT,recipientName,  recipi-
entNameLength );
/* Push in the message data and pop out the signed and encrypted result */
cryptPushData(cryptEnvelope,message,messageSize,&bytesIn);
cryptFlushData(cryptEnvelope);
cryptPopData(cryptEnvelope, encryptedMessage, encryptedSize, &bytesOut );
/* Clean up */
cryptDestroyEnvelope(cryptEnvelope );
```

Fig.4.10. Secvenţă de cod pentru criptare mesaj utilizând o cheie publică

Prin secvenţa de cod de mai sus se execută următoarele acţiuni menite a mări securitatea datelor vehiculate:

- generează o cheie de sesiune aleatoare pentru algoritmul de criptare (de obicei, triple DES sau AES);
- caută cheia publică a destinatarului într-o bază de date de chei;
- criptează cheia de sesiune folosind cheia publică a destinatarului;
- criptează datele semnate cu cheia de sesiune;
- trimite rezultatul înapoi la utilizator.

Pentru a stabili o sesiune sigură am utilizat următoarea secvenţă de cod, Fig.4.11:

```
CRYPT_SESSION cryptSession;
/* Create the session */
cryptCreateSession( &cryptSession,
cryptUser, CRYPT_SESSION_SSL );
/* Add the server name and activate the session */
cryptSetAttributeString(cryptSession,
CRYPT_SESSINFO_SERVER_NAME, serverName, serverNameLength );
cryptSetAttribute( cryptSession, CRYPT_SESSINFO_ACTIVE, 1 );
```

Fig.4.11. Secvenţă cod pentru stabilirea unei sesiuni sigure

Dacă în loc de SSL (Secure Socket Layer) se doreşte utilizarea SSH (Secure Socket Shell) se va înlocui SSL cu SSH în CRYPT_SESSION_SSL şi se adaugă un utilizator şi o parolă la log on.

După cum se poate vedea mai sus, cryptlib prevede o singură interfaţă pentru mecanismul de securitate al sesiunii, astfel încât nu trebuie investit efort în special în adăugarea de mecanisme de securitate suplimentare pentru diferite protocoale.

Server–ul corespunzător SSL/TLS (sau SSH) este în cazul acesta Fig.4.12:

```
CRYPT_SESSION cryptSession;
/*Create the session */cryptCreateSession(&cryptSession,
cryptUser, CRYPT_SESSION_SSL_SERVER );
/* Add the server key / certificate and
activate the session */cryptSetAttribute( cryptSession,
CRYPT_SESSINFO_PRIVATEKEY, privateKey );
cryptSetAttribute( cryptSession,
CRYPT_SESSINFO_ACTIVE, 1 );
```

Fig.4.12. Secvenţă cod pentru o sesiune sigură prin server-ul SSL

Pentru interfaţa plug&play PKI (Public Key Infrastructure) am utilizat următorul cod cryptlib , Fig.4.13:

```
CRYPT_SESSION cryptSession;
/*Create the CMP session and add the server name/ address*/
cryptCreateSession( &cryptSession,
cryptUser, CRYPT_SESSION_CMP );
cryptSetAttributeString( cryptSession,
CRYPT_SESSINFO_SERVER, server, serverLength );
/* Add the username and password*/
cryptSetAttributeString( cryptSession,
CRYPT_SESSINFO_USERNAME, userName,
userNameLength );
cryptSetAttributeString( cryptSession,
CRYPT_SESSINFO_PASSWORD, password,
passwordLength ); cryptSetAttribute( cryptSession,
CRYPT_SESSINFO_CMP_PRIVKEYSET, cryptDevice );
/* Activate the session */cryptSetAttribute( cryptSession,
CRYPT_SESSINFO_ACTIVE, TRUE );
```

Fig.4.13. Secvenţă de cod pentru interfaţa PKI

Secvenţa de cod din Fig.4.13, generează separat cheile de criptare şi autentificare şi utilizează acestea pentru a obţine cheia de criptare.

Prin comparaţie cu alte servicii de securitate cryptlib face acest lucru într-un mod facil, fără a mai fi nevoie scrierea a sute sau chiar mii de linii de cod care să facă acelaşi lucru.

Cele mai multe biblioteci de criptare sunt furnizate sub forma de totul în una (all-in-one) unde sunt cuprinse toate capabilităţile lor într-o singură aplicaţie şi care trebuie să se comporte ca o singură unitate. Actualmente sunt trei versiuni de cryptlib, se poate folosi oricând una din ele:

Versiune	Caracteristică
cryptlib lite	Criptare convenţională, semnătură, hashing, algoritmi MAC şi funcţii aferente pentru a prelucra chei şi parole.
cryptlib cert	Ca şi cryptlib lite dar cu certificat de management X.509, operaţii CA şi certificate de memorare.
cryptlib pro	CA şi cryptlib cert dar cu structură digitală şi suport S/MIME, SSL, TLS şi sesiune sigură ssh.

Fig.4.14. Versiuni Cryptlib

4.4.4. Evaluare şi rezultate

Testarea a fost realizată pentru a evalua impactul pe care îl au modificările de securitate asupra programului pentru Kiax. După configurarea reţelei locale şi a clientului, au fost efectuate apeluri şi au fost analizate datele colectate. Toate testele au fost repetate şi au furnizat un pachet consistent de date. Un rezumat al rezultatelor este prezentat în tabelele de mai jos:

Tabelul 10. Rezultate test 1 LAN

Client VoIP	Kiax	Kiax	Kiax	Kiax
Criptare	Nu	IDEA/CBC	IDEA/CFB	RC4
Utilizare min. CPU	5.812 %	17.818 %	16.132 %	17.635 %
Utilizare max. CPU	10.020 %	28.629 %	26.226 %	27.756 %
Utilizare medie CPU	7.935 %	24.158 %	22.756 %	23.090 %
Lăţime de bandă maximă	1.75 kByte / s	2.08 kByte / s	1.75 kByte / s	1.75 kByte/s
Întârziere	16-58 ms	16-58 ms	16-58 ms	16-58 ms
Jitter	26-28 ms	26-28 ms	26-28 ms	26-28 ms

Tabelul 11. Rezultate test 2 LAN

Client VoIP	Kiax	Kiax	Firefly
Criptare	AES/CBC	AES/CFB	None
Utilizare min. CPU	17.818 %	14.629 %	8.719 %
Utilizare max. CPU	27.427 %	27.227 %	13.123 %
Utilizare medie CPU	23.447 %	22.592 %	11.364 %
Lăţime de bandă maximă	2.48 kByte /s	1.75 kByte / s	1.69 kByte / s
Întârziere:	16-58 ms	16-58 ms	2-3 ms
Jitter:	26-28 ms	26-28 ms	2-4 ms

Utilizând Kiax fără criptare, media de utilizare a procesorului este de 7,9 %, iar lăţimea de bandă de este aproximativ 1,75 Kbytes pe secundă. Aceasta asigură o bază pentru performanţa Kiax. Făcând o analiză a diverselor metode de criptare utilizate avem următoarele situaţii:

1. dacă se utilizează algoritmul IDEA (International Data Encryption Algoritm)- în modul înlănţuirii blocurilor de cifru (CBC-Cipher Block Chaining), calitatea apelului a rămas similară cu cea în care nu s-a folosit criptarea, însă lăţimea de bandă utilizată a crescut. Acest lucru era de aşteptat, deoarece dimensiunea datelor a crescut de la 33 la 40 octeţi. Când se foloseşte algoritmul IDEA în modul cifru cu feedback (CFB-Cipher Feedback), deşi lăţimea de banda a fost identică cu cea iniţială, calitatea apelului a fost mai frecvent întreruptă de pierderi ale semnalului audio.
2. dacă se utilizează algoritmul AES (Advanced Encryption Standard) în modul înlănţuirii blocurilor de cifru (CBC) procentul de utilizare al procesorului este uşor mai mic, comparativ cu IDEA/CBC, aceasta datorită algoritmului AES care este mult mai eficient. Aceasta metodă a utilizat cea mai mare valoare a lăţimii de bandă, adăugând aproximativ 0.7 Kbyte/s. Creşterea lăţimii de bandă este mai mare pentru AES decât pentru IDEA. În timp ce algoritmul AES are dimensiunea blocului de 128 biţi, IDEA foloseşte doar 64 biţi. AES, folosind CFB, are cea mai mică medie de utilizare a procesorului pentru metoda de criptare testată şi nu are nevoie de lăţime de bandă suplimentară.
3. agoritmul RC4 (Rivest Cipher 4) are cele mai slabe rezultate, faţă de AES/CFB. Acest lucru este surprinzător, având în vedere că este cifru nativ pentru flux.

În ansamblu, rezultatele atât pentru calitatea apelului cât şi a utilizării procesorului sunt similare pentru diferiţi algoritmi de criptare. Cu toate acestea, AES în modul CFB ar trebui să fie considerată ca metodă preferată, deoarece oferă cea mai mică medie de încărcare a procesorului, nu adăuga cerinţe de lăţime de bandă suplimentare şi introduce un minim de probleme în fluxul audio.

4.5 Distribuţia multiplă a vocii în substratul de control al accesului la mediu în reţelele fără fir bazate pe standardul IEEE 802.11

În acest capitol este realizat un studiu experimental al performanţei şi fiabilităţii transmisiei cu destinaţii multiple în subnivelul de acces la mediu al reţelelor fără fir bazate pe standardul IEEE 802.11. În multe cazuri, distribuţia multiplă permite o utilizare mult mai eficientă a reţelelor, deoarece elimină nevoia de a trimite mai multe pachete identice, la destinaţii diferite. Acest studiu experimental are ca scop determinarea gradului de utilizare a distribuţiei multiple a vocii la nivelul substratului de control al accesului la mediu (MAC) pentru două situaţii. Prima situaţie este utilizarea distribuţiei multiple pentru fluxurile de voce din link-ul de coborâre (downlink) şi este destinată mai mult celor aflaţi în aceeaşi celulă a unei reţele fără fir, cum ar fi teleconferinţele, emisiuni audio în întreprinderi sau situaţii de urgenţă. A doua situaţie este utilizarea în regim de walkie-talkie unde numai unul din participanţi are permisiunea de a accesa reţeaua la un moment dat. Spre deosebire de reţelele fixe unde transmisia cadrelor la nivelul substratului de acces la mediu se face identic indiferent dacă e distribuţie multiplă sau nu, în reţelele locale fără fir, bazate pe standardul IEEE 802.11 există diferenţe semnificative între cele două tipuri de transmisie. Pentru a face faţă pierderii de cadre şi a coliziunilor în reţeaua fără fir în comparaţie cu cea fixă, protocolul de acces la mediu aşteaptă confirmări de recepţie a cadrelor şi le retransmite pe cele neconfirmate. Valorile contorului pentru retransmitere sunt alese astfel încât protocoale de transport din straturile superioare, în particular TCP, nu sunt afectate de pierderea cadrelor. În cazul transmisiei cu distribuţie multiplă cadrele nu se mai retransmit cu excepţia celor către punctele de acces. Prin urmare, rata de pierdere este mult mai mare faţă de transmisia unicast. În plus, funcţia de coordonare distribuită a standardului IEEE 802.11 are implementat un schimb de cadre pentru cerere de trimitere/anulare (RTS/CTS) pentru a proteja traficul unicast de interferenţele datorate încercărilor simultane de transmisie a două staţii care nu se sesizează reciproc (staţii ascunse). Funcţia de coordonare distribuită nu permite utilizarea de cereri de trimitere/anulare RTS/CTS pentru traficul distribuţiei multiple cu excepţia celui pentru punctele de acces. În consecinţă, în astfel de scenarii, ne putem confrunta cu o pierdere mare de cadre.

După cum s-a subliniat mai sus, avantajele utilizării trimiterii de mesaje cu distribuţie multiplă la nivelul substratului de acces la mediu ar fi convingătoare în cazul în care calitatea fluxurilor de voce ar fi acceptabilă, la majoritatea sau toţi abonaţii. În plus, spre deosebire de majoritatea traficului de date în care fiecare cadru pierdut este de obicei obiectul retransmisiei la nivelul straturilor superioare, traficul de voce poate tolera pierderea unui cadru "din când în când ". Astfel, lipsa de recunoaşteri şi retransmisia pentru traficul cu distribuţie multiplă ar putea fi tolerabilă. Cu toate acestea, dacă pierderea depăşeşte un anumit prag, calitatea vocii poate degenerează până la un punct în cazul în care conexiunea este inutila. În afară de pierderi, calitatea unei conexiune este caracterizată de asemenea de o întârziere de conectare dus-întors şi de jitter. **Cele mai multe studii de simulare a transmisiei cu distribuţie multiplă în reţelele fără fir au studiat mecanismele de distribuţie din straturile superioare. Această teză se concentrează pe studierea comportamentului canalului fără fir al standardului IEEE 802.11 în distribuţia multiplă. Proprietăţile distribuţiei multiple ale substratului de acces la mediu al standardului IEEE 802.11 nu au fost studiate încă suficient.** Deoarece, aşa cum s-a subliniat mai sus, transmisia cu distribuţie multiplă este

foarte diferită de cea unicast pentru standardul IEEE 802.11. Un studiu experimental este necesar pentru a determina proprietăţile reale ale distribuţiei multiple în substratul de acces la mediu, în special atunci când este utilizat pentru transmiterea vocii. În timp ce în reţelele cu o topologie variată, simulările sunt mai uşor de configurat, controlat şi modificat, datele prezentate în această lucrare nu pot fi obţinute prin simulări. În concluzie acest studiu experimental al proprietăţilor transmisiei distribuţiei multiple în reţelele fără fir este bine motivat.

Pentru experimente, am utilizat PC-uri (laptop-uri, Desktop-uri) pe care au rulat Linux 7.4. Toate experimentele descrise au fost realizate în modul Ad-hoc. Cardurile radio utilizate pentru toţi clienţii au fost de la acelaşi furnizor. Standardul IEEE 802.11 precizează că în toate transmisiile cu distribuţie multiplă cadrele sunt transmise la o rată care este suportată de toate seturile de servicii de bază ale staţiilor. Cu alte cuvinte, rata de transfer utilizată trebuie să fie cea anunţată prin cadrul de balizaj (beacon). Toate experimentele au fost făcute pentru o rată de transfer de 2 Mbps.

4.6 Pierderile şi rata de transfer în distribuţia multiplă la nivelul substratului de acces la mediu

Primul experiment măsoară rata de transfer disponibilă la nivelul stratului transport pentru trimiterea multiplă, prin intermediul protocolului Internet sau datagramă IP/UDP, printr-un singur punct intermediar. Am folosit Skype ca şi program care trimite în mod constant, către mai multe destinaţii ale unei reţele fără fir cadre UDP, asemănător unui experiment cu trimitere spre o singură destinaţie. Fluxul a fost recepţionat de un punct final al unei reţele fără fir care, în urma ascultării a identificat adresa de destinaţie ca fiind a lui. Pentru măsurarea capacităţii, transmiţătorul şi receptorul au fost amplasate unul lângă celălalt, în scopul de a minimiza pierderile.

Rezultatele indică faptul că rata maximă de transfer a cadrelor cu informaţie utilă, care poate fi transmisă cu destinaţie multiplă este de aproximativ 1.76 Mbps şi este atinsă atunci când fiecare pachet UDP are 1472 octeţi (pentru pachete mai mari de 1472 octeţi datele ajung fragmentate). Când cei 62 de octeţi ai standardului IEEE 802.11 şi antetul protocoalelor IP/UDP (34+20+8) din fiecare cadru trimis sunt contabilizate, rata de transfer prin reţea este de aproximativ 1.83 Mbps. Între 0,1% şi 0,35% din pachete nefragmentate au fost pierdute cu o medie de 0,15%. Pierderea a fost independentă de dimensiunea informaţiei utile conţinute de cadre.

Fig. 4.15 arată măsurătorile pentru o rată de transfer funcţie de mărimea sarcinii utile pentru o singură transmisie cu distribuţie multiplă. Căderea bruscă se datorează unor pachete mai mari de 1472 octeţi deoarece informaţia este fragmentată.

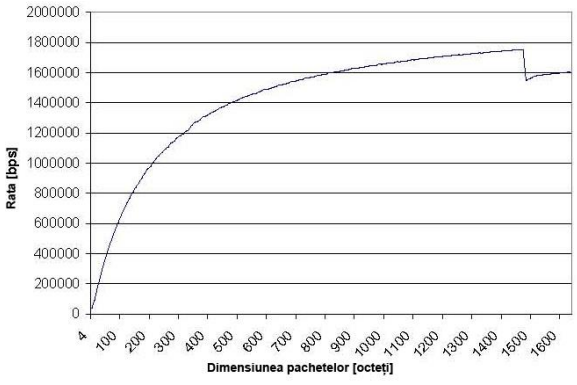


Fig.4.15 Rata de transfer în funcţie de mărimea pachetului pentru traficul cu distribuţie multiplă a standardului IEEE 802.11 la 2 Mbps.

Ţinând cont de numărul de cadre pe secundă şi de faptul că pentru acest caz fiecare cadru este transmis cu o rată de 2 Mbps, se poate calcula capacitatea maximă pentru transmiterea fiecărui cadru. Pentru măsurători, capacitatea maximă a fost evaluată pentru o medie de aproximativ 815 μs per cadru, echivalent cu transmiterea de aproximativ 200 octeţi la 2 Mbps.

Sistemul de acces la mediu, pentru Funcţia de Coordonare Distribuită (DCF), în conformitate cu standardul IEEE 802.11 este protocolul de acces multiplu cu sesizarea purtătoarei cu evitarea coliziunii (Carier Sense Multiple Access/Collision Avoidance-CSMA/CA). O prezentare a imaginii acestui mecanism şi structura cadrului de transmisie sunt prezentate în fig.4.16.

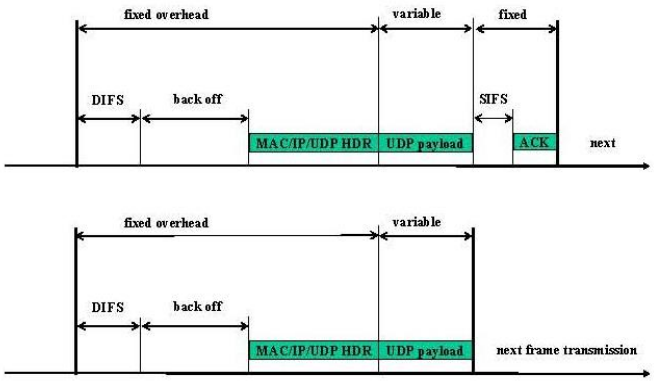


Fig.4.16 Sistemul de acces la mediu pentru cadre cu destinaţie multiplă (jos) sau unică (sus) al standardului IEEE 802.11 bazat pe protocolul CSMA/CA [35]

După cum a fost precizat, transmisia cu destinaţie multiplă pentru funcţia de coordonare distribuită nu este confirmată. Dacă R este rata de transfer în bps şi b dimensiunea cadrului de date în octeţi, timpul necesar pentru transmisia cadrelor componente poate fi calculat după cum se arată în tabelul următor.

Tabelul 12. Calculul timpului pentru transmisia cadrelor

Reper	Timp
Cadre de date	192ns+8b/R
SIFS	10ns
ACK	192ns+112/R
DIFS	50ns

În plus, pentru cazul transmiterii, în mod constant pentru un singur client, timpul mediu aleator de revenire (back-off) este 310μs

Pentru cadrul actual de date avem 34 octeţi pentru antetul accesului la mediu al standardului IEEE 802.11, 20 octeţi pentru antetul protocolului IP şi 8 octeţi

antetul protocolului UDP, în total 62 octeţi plus informaţia utilă a datagramei UDP. Adunând aceste valori, putem stabili valoarea maxima admisă pentru traficul multi-punct, cu o rată de 2 Mbps, la 800 μs.

Această valoare se potriveşte cu cea determinată prin experiment. Valorile experimentale sunt ceva mari datorită faptului că periodic sunt trimise cadre de balizaj de către staţiile din reţeaua ad-hoc a căror valoare nu este inclusă în calcule. Deoarece în transmisia cu destinaţie multiplă cadrele nu includ şi transmiterea unui semnal de confirmare, durata acestora este mai mică cu 258 μs faţă de transmiterea obişnuită la aceeaşi rată de 2Mbps. Acest lucru a fost, de asemenea verificat experimental. În condiţii de rată de trafic identică cu transmisia simplă, cu 1472 octeţi de informaţie utilă ai datagramei UDP, se atinge o rată maximă de 1.68 Mbps, spre deosebire de transmisia cu destinaţie multiplă unde rata de trafic este de 1,76 Mbps.

4.7 Redirecţionarea distribuţiei multiple a vocii cu salturi multiple

Un alt experiment studiat în această teză este şi cel al traficului VoiP, cu distribuţie multiplă, redirecţionat prin mai multe puncte. Rezultatele obţinute sunt de reţinut de asemenea şi pentru cazul în care traficul este transmis între puncte de acces care formează un sistem de distribuţie fără fir (wireless distribution system-WDS) cu distribuţie multiplă prin intermediul substratului de control al accesului la mediu. Am utilizat cinci laptop-uri aşa cum se arată în fig. 4.17.

Fig.4.17 Configurare schematică a laptop-urilor pentru multisalt

Laptop-urile au fost instalate într-un birou cu distanţa între ele de 25 m şi 30 m. Staţiile neadiacente nu s-au putut vedea reciproc fiind despărţite de pereţi. Astfel, fiecare staţie a putut comunica doar cu vecinul alăturat ca în Fig.4.17. Puterea semnalului între staţiile vecine a fost excelentă.

Expeditorul a sintetizat un flux de trafic echivalent unui flux VoIP generat de un codec ITU G.729 cu o durată a datelor audio de 30 ms/pachet trimis (42 octeţi UDP sarcină utilă/pachet). Am folosit acest codec deoarece este folosit frecvent în reţelele fără fir. Experimentele cu alte tipuri de codec-uri conduc la rezultate similare. Pentru a ajunge la receptorul din dreapta (a 4 a staţie), cadrul este necesar a fi transmis de către toate staţiile. Pentru direcţionarea cadrului şi sintetizarea vocii, am utilizat un cadru în care inundarea este utilizată pentru distribuirea pachetelor cu distribuţie multiplă din reţea. Cu alte cuvinte, fiecare staţie care recepţionează un cadru cu distribuţie multiplă îl direcţionează mai departe dacă l-a primit pentru prima dată. O aglomerare este evitată prin memorarea pachetelor care au fost deja transmise. Pachetele transmise sunt stocate pentru o secundă într-o memorie de 245 KB la o rată de 2 Mbps.

Am ales inundarea întrucât aceasta constituie cea mai simplă modalitate de a facilita experimentarea cadrelor. Această alegere nu are nici o influenţă asupra rezultatelor experimentale. Orice altă dirijare multipunct a cadrelor la nivelul substratului MAC trebuie să direcţioneze astfel cadrele încât să nu modifice nici un alt mecanism de dirijare.

În scopul de a calcula timpul dus-întors, staţiile receptoare răspund la întâmplare la fiecare al 50-lea pachet vocal primit. Fiecare experiment a durat 105 secunde şi a constat din 3500 de pachete de voce. La fiecare receptor, am calculat pierderile şi jitter-ul. Timpul dus-întors de la toate receptoarele a fost calculat la expeditor pe baza răspunsurilor de la receptori. Am realizat acest experiment de 12 ori. În afară de fluxul de voce şi răspunsurile sporadice de la receptori, nici un alt trafic nu a fost prezent. Valorile obţinute pentru pierderi, bruiaj şi transmisie dus-întors sunt date de tabelul 13

Tabelul 13. Valori rată pierderi, jitter şi timp dus-întors

Caracteristică	Primul salt	Al doilea salt	Al treilea salt	Al patrulea salt
Media ratei de pierderi. Rata de pierderi pt. dev.std.	0.007 0.003	0.012 0.004	0.015 0.006	0.017 0.007
Media valorii jitter-ului Valoarea jitter pt. dev.std	0.18 0.06	0.21 0.09	0.47 0.22	0.80 0.16
Media RTT [ms] Valoare pt. dev.std. RTT.	2.96 1.55	6.46 0.95	9.79 0.44	13.04 1.58

Fig. 4.18 arată rata pierderilor din toate experimentele pentru toate receptoarele. Valorile pentru întârzieri, pierderi şi jitter au crescut o dată cu numărul de staţii parcurse. În acest scenariu cu patru staţii, timpul dus-întors şi jitter-ul sunt mai mult decât acceptabile pentru traficul VoIP. Rata de pierdere de 1,7% de la a patra staţie poate fi considerată acceptabilă pentru VoIP. În configuraţia studiată, este clar că fiecare cadru pierdut la o staţie nu poate fi transmis mai departe şi prin urmare figurează ca pierdut ulterior. Raportul pierdere per staţie este între 0,2% şi 0,7%. Acesta este semnificativ mai mare decât în experimentul anterior în care emiţătorul şi receptorul au fost situate imediat unul lângă altul. Am obţinut valori identice de pierdere pentru fiecare staţie atunci când am verificat legătura individuală a pierderilor.

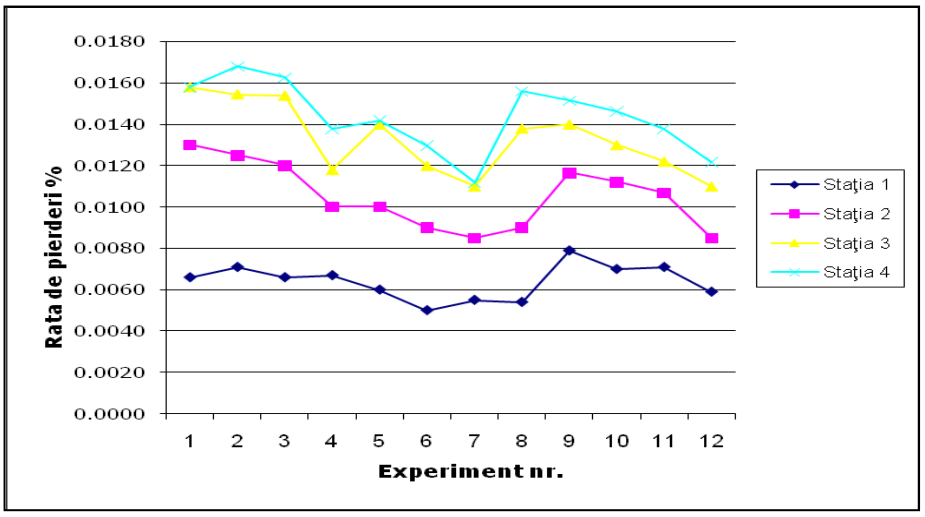


Fig.4.18 Rata de pierderi pentru multisalt

Rata pierderilor în cazul acestui experiment a variat semnificativ. Creşterea timpului dus-întors de la 3 ms la 4 ms pe staţie era de aşteptat. Timpul de transmisie pentru un cadru este de aproximativ 1 ms care se ridică la un timp minim dus-întors de 2 ms pe staţie. Timpul suplimentar se datorează procesului suplimentar de prelucrare pentru expediere. Valorile de bruiaj observate cresc odată cu numărul de staţii; acestea sunt foarte mici la toate patru receptoarele. În concluzie, calitatea fluxului de date pentru distribuţia multiplă a vocii (VoIP) a fost acceptabilă pentru cele patru receptoare. Presupunând o creştere similară per staţie în raport cu pierderile (între 0,2% şi 0,7%), calitatea traficului VoIP nu va mai fi suficientă sau cel puţin critică la a 5 a staţie. Această ipoteză nu poate fi confirmată experimental, deoarece locul în care experimentele au fost efectuate nu au permis instalarea unui alt laptop care ar putea primi transmisiile numai printr-un vecin imediat.

4.8 Redirecţionarea multisalt cu distribuţie multiplă a vocii în cazul staţiilor ascunse

O altă posibilitate de transmitere a vocii este cea multisalt (multihop) cu staţii ascunse. Pentru acest experiment au fost utilizate patru laptop-uri.

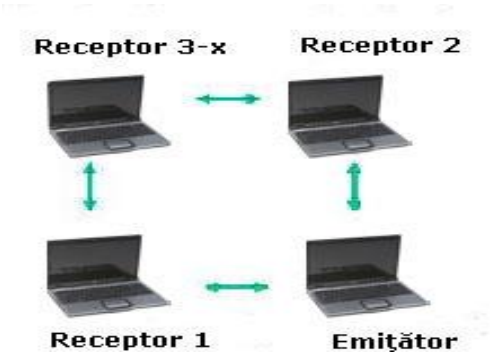


Fig.4.19 Configurarea laptop-urilor pentru direcţionarea multisalt cu staţii ascunse

Emiţătorul poate trimite direct la staţiile 1 şi 2. Receptoarele 1 şi 2 nu pot să îşi trimită reciproc mesaje. Până la trei laptop-uri, receptoarele 3-1, 3-2 şi 3-3 au fost situate într-o astfel de poziţie încât ele puteau asculta receptoarele 1 şi 2, dar nu puteau asculta emiţătorul. Receptoarele 3-1, 3-2 şi 3-3 pot primi mesaje unul de

la altul. Toate staţiile direcţionează fiecare pachet o singură dată exact aşa cum este descris în experimentul anterior.

Eu am realizat trei variante ale acestui experiment. În experimentul 1, doar receptorul 3-1 a fost activ. În experimentul 2, receptoarele 3-1 şi 3-2 au fost active şi în experimentul 3, toate receptoarele (3-1, 3-2 şi 3-3) au fost active. Fiecare experiment a constat din 3500 cadre trimise şi a fost repetat de 50 de ori. Fig.4.19. Pentru întârziere şi jitter, am observat o valoare medie a jitter-ului de 0,3 s pentru toate staţiile din toate experimentele, iar timpul de răspuns dus-întors a variat între 3 şi 8 ms, în funcţie de numărul de salturi. Deoarece aceste valori sunt excelente pentru transmiterea vocii, cum era de altfel şi de aşteptat, mă voi concentra asupra pierderilor observate. Tabelul 14 de mai jos indică rata pierderilor pentru toate staţiile. Fig. 4.20 arată rata pierderilor pentru trei instanţe ale fiecărui experiment 1, 2 şi 3.

Tabelul 14. Rata pierderi [%]

Exp. nr.	Caracteristica	Recep-tor 1	Recep-tor 2	Recep-tor 3-1	Recep-tor 3-2	Recep-tor 3-3
1	Media ratei de pierderi% Media ratei de pierderi pt. dev.std %.	0.0187 0.043	0.0154 0.041	0.137 0.125		
2	Media ratei de pierderi% Media ratei de pierderi pt. dev.std.%	0.006 0.0023	0.005 0.029	0.021 0.615	0.021 0.614	
3	Media ratei de pierderi % Media ratei de pierderi pt. dev. std.%	0.002 0.002	0.001 0.002	0.009 0.009	0.012 0.009	0.008 0.009

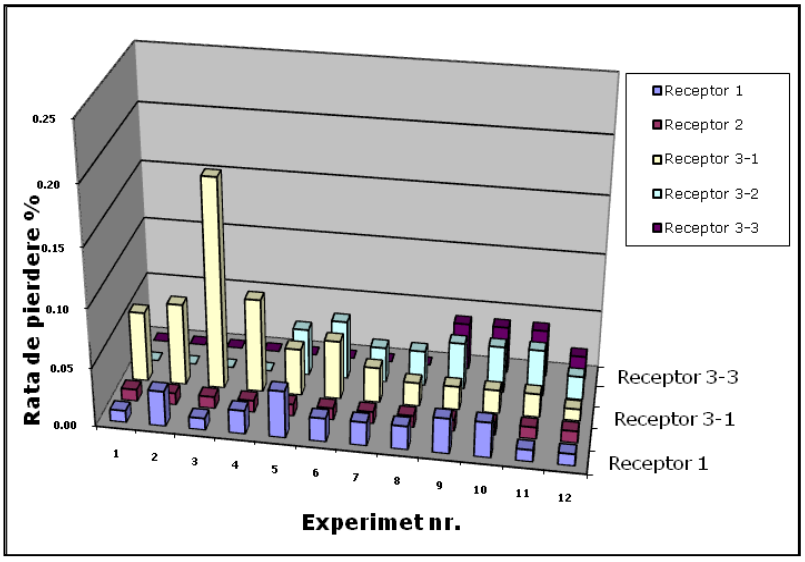


Fig.4.20 Rata de pierdere în distribuţia multisalt cu staţii ascunse

În experimentul 1, rata de pierdere pentru receptoarele 1 şi 2 este 1,9%, respectiv 1,5%, iar pentru receptorul 3-1 aproximativ 14%. Ratele de pierdere la receptoarele 1 şi 2 sunt mai mari decât în experimentul precedent. Acest lucru se datorează a cinci experimente în serie căror rată de pierdere este foarte mare la receptoarele 1 şi 2 (până la 26%). Dacă aceste efecte sunt reduse, rata de pierdere de la receptoarele 1 şi 2 este comparabilă cu pierderea de la primul salt din experimentul anterior. Motivul unei rate a pierderilor foarte mare la receptorul 3-1 (în experimentul anterior, rata de pierdere la saltul al doilea a fost doar de 1,2%) este legată de detectarea unei staţii ascunse. Receptoarele 1 şi 2 au primit acelaşi pachet de la emiţător pe care trebuie să îl transmită mai departe. Deoarece receptoarele 1 şi 2 nu pot detecta când transmit fiecare din ele, încep să transmită simultan.

Mecanismul de decrementare pentru protocolul de detecţie a purtătoarei cu acces multiplu şi evitarea coliziunii al standardului IEEE 802.11 nu ajută, pentru că poate preveni numai coliziunile între transmisiile staţiilor care se pot identifica reciproc. Dacă staţiile nu se pot vedea una pe alta, în funcţie de valoarea aleasă pentru contorul de decrementare, fiecare staţie amână transmisia între 0 şi 0,62 ms, dar transmiterea unui cadru ia în jur de 1 ms. Astfel, receptoarele 1 şi 2 transmit practic întotdeauna simultan, ceea ce duce la interferenţe la receptorul 3-1. Această staţie este capabilă să recupereze aproximativ 74% din cadrele transmise (nu orice interferenţă duce la pierderea de cadre) dar 26% din trafic nu în poate recupera.

Experimental s-au confirmat aceste presupuneri. Într-o variantă a experimentului cu receptorul 1 respectiv 2, oprite, rata de pierdere la receptorul 3-1 a fost în acelaşi interval ca rata de pierdere pentru saltul al doilea din experimentul precedent. În alte variante, am testat cât de sensibilă este rata de pierdere la mişcări minore ale receptoarelor/emiţătoarelor, prin înclinarea antenelor. Acest fapt a dovedit că efectul produs de direcţionările multiple a rămas sau chiar a crescut, pierderile la receptorul 3-1 variind semnificativ (de la 10% la 39%, fiecare variaţie a fost testată doar o dată). În toate cazurile testate, pierderile au fost inacceptabile pentru fluxuri VoIP.

Având în vedere natura nedeterministă a interferenţelor, am studiat efectele de amplasare a staţiilor pentru receptorul 3-1 în experimentele 2 şi 3. Am dorit să văd dacă staţiile care au acelaşi amplasament vor pierde aceleaşi cadre datorită interferenţelor. Pentru staţiile amplasate într-o locaţie comună cadrele recepţionate au fost trimise mai departe. Prin urmare, un receptor care a pierdut un cadru transmis de la receptorul 1 şi 2 ar putea totuşi să îl primească atunci când e retransmis de către unul din ele. În cazul în care cadre diferite, provenind de la receptoare diferite s-au pierdut, raportul general de pierdere ar trebui să scadă. Într-adevăr, experimentele 2 şi 3 au confirmat această ipoteză. Când o staţie are acelaşi amplasament cu receptorul 3-1, rata de pierdere la staţiile 3-1 şi 3-2 ajunge la aproximativ 2%. Când două staţii au acelaşi amplasament ca şi receptorul 3-1, rata de pierdere scade în continuare pentru a atinge 1% pentru toate staţiile.

Tabelul de mai sus arată sursele imediate ale cadrelor nou primite de către receptoarele 3-1, 3-2 şi 3-3 din experimentul 3. Receptoarele 3-1 şi 3-3 primesc cele mai multe pachete de la receptorul 1, receptorul 3-2 primeşte atât de la receptorul 1 cât şi 2 în mod egal. Fiecare dintre staţii primeşte cel puţin 5% din cadre de la una din perechea ei, iar rata de recepţie a ambelor perechi este comparabilă pentru toate receptoarele. După cum se poate observa, rata de pierdere pentru receptoarele 3-1, 3-2 şi 3-3 variază între 5% şi 13% atunci când pachetele recepţionate de perechi se reduc.

Calitatea fluxului de voce VoIP nu poate fi luată în considerare în acest experiment, pentru nici unul din receptoarele 3-x, fără retransmisia de la perechile

vecine. Cu toate acestea calitatea VoIP în experimentul 3 este suficientă pentru toate receptoarele.

În mod evident, acest experiment arată că redirecţionarea aleatoare a traficului cu distribuţie multiplă la nivelul substratului MAC nu este întotdeauna recomandabilă. O abordare gen structură arborescentă (urmărită de majoritatea protocoalelor de rutare cu distribuţie multiplă) ar putea evita cu uşurinţă pierderea la receptorul 3 din scenariul de mai sus datorită interferenţelor. Cu toate acestea, considerăm un scenariu extins cu două staţii suplimentare 4 (respectiv 5), care pot recepţiona doar de la receptorul 1 (2). În acest caz, atât receptorul 1 cât şi 2 trebuie să fie în structură arborescentă. După cum se poate dovedi, în afară de receptoarele 1 şi 2, ambele direcţionând imediat datele ce au fost recepţionate de la emiţător, doar două variante suplimentare sunt posibile şi anume secvenţele de expediere S-1-3-2 şi S-2-3-1. Aceste secvenţe de transport ar duce în mod semnificativ la creşterea timpului dus-întors şi a jitter-ului, precum şi la o rată de pierdere mai mare la receptorul 5 (4), deoarece traficul de la emiţătorul 5 (4) este transmis prin trei salturi, spre deosebire de situaţia de dinainte. Nu este dificil de construit şi alte configuraţii cu staţii ascunse, care duc însă la probleme similare, mai puţin evidente, care trebuiesc rezolvate. Putem concluziona că prevenirea fenomenului de staţie ascunsă prin structuri arborescente, pentru transmiterea multiple este dificilă.

4.9 Efectul întârzierilor redirecţionate aleator

În distribuţia multiplă cu unul sau mai multe salturi un rol important îl au întârzierile. Am studiat efectul întârzierilor redirecţionate aleator din rata de pierdere, timpul dus-întors şi jitter-ul. În general, ideea este să se evite coliziunile datorate transmiterii pe mai multe căi printr-un mecanism de revenire aleatoriu, similar celui folosit pentru controlul accesului la mediu la standardului IEEE 802.11. Mă voi referi la acest abordare ca "revenire suplimentară" (AL-backoff).

Cu excepţia traficului sursei, fiecare staţie ajunge la o valoare aleatoare între 0 şi valoarea de AL-backoff (care este similară cu valoarea ferestrei de conflict Contention Window-CW a standardului IEEE 802.11). Această valoare, în milisecunde, este timpul de aşteptare al staţiei înainte de a transmite mai departe pachetele. Valorile de sincronizare sunt alese astfel că două cadre cu timpi de revenire (backoff) diferiţi sunt transmise la intervale de timp diferite Fig. 4.21.

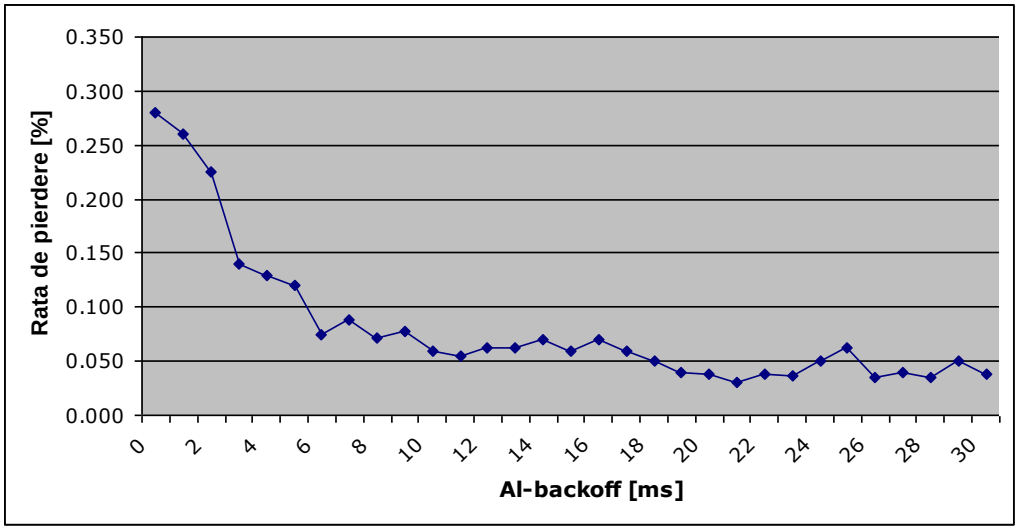


Fig.4.21 Rata de pierdere în distribuţia multisalt cu staţii ascunse cu revenire suplimentară

Fig.4.21 arată rata de pierdere în funcţie de valoarea de revenire suplimentară (AL-backoff) utilizată într-un experiment de iniţializare, similar cu distribuţia multiplă multisalt cu staţii ascunse experimentale. Trebuie reţinut că plasarea de staţii în acest experiment nu a fost identică cu cea descrisă în secţiunea anterioară şi că rata de pierderi fără reveniri suplimentare din acest experiment este ceva mai mare. Următorul tabel arată de asemenea jitter-ul şi timpul dus-întors.

Tabelul 15. Valori jitter şi timp dus-întors pentru distribuţia multisalt cu staţii ascunse cu revenire suplimentară

AL-Backoff [ms]	Rata de pierderi %	Jitter [ms]	RTT [ms]
0	0.292	0.12	6.47
5	0.123	0.93	7.64
10	0.059	2.57	9.04
15	0.054	3.83	11.00
20	0.039	5.33	13.37
25	0.031	6.50	15.85

Rata de pierdere din experiment scade de la 29% la sub 5% prin creşterea valorii AL-backoff. Cele mai semnificative scăderi ale ratei de pierdere sunt pentru valori mici ale AL-backoff. Aşa cum ar fi de aşteptat, jitter-ul şi timpul dus-întors cresc odată cu creşterea valorii AL-backoff. Deci, în acest scenariu, folosind valorile AL-backoff am putea ajuta la scăderea ratei de pierdere împiedecând în acelaşi timp creşterea la valori inacceptabile a timpului dus-întors sau a jitter-ul.

Am studiat, de asemenea, efectul valorilor AL-backoff în scenarii de redirecţionare pentru distribuţii multiple cu salturi multiple. Rezultatele acestui experimentului sunt prezentate în Fig. 4.22, Fig.4.23 şi Fig.4.24.

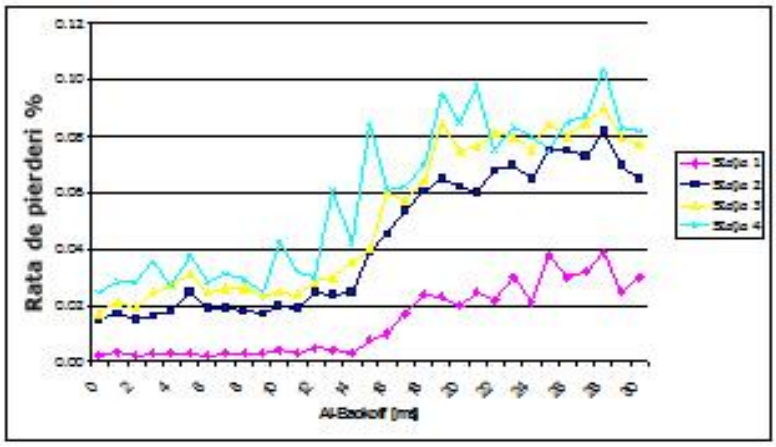


Fig.4.22 Rata de pierdere cu revenire suplimentară în redirecţionarea distribuţiei multiple multisalt

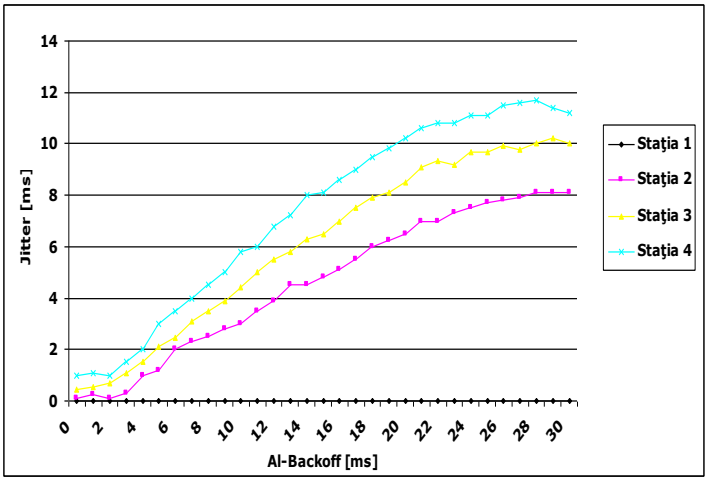


Fig.4.23 Jitter cu revenire suplimentară în redirecţionarea distribuţiei multiple multisalt

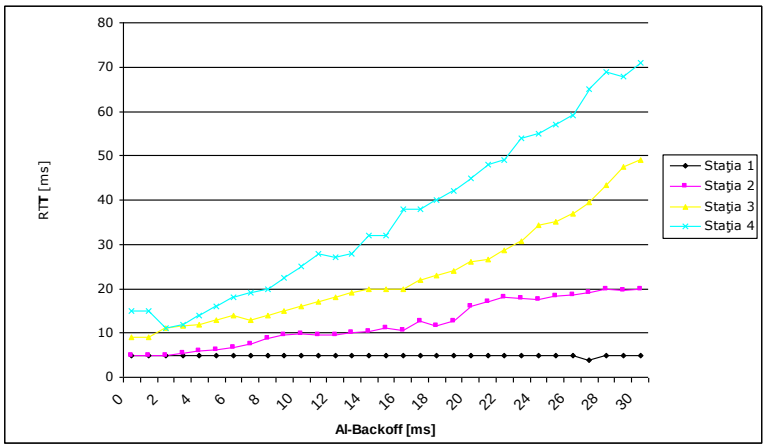


Fig.4.24 Timp dus-întors cu revenire suplimentară în redirecţionarea distribuţiei multiple multisalt

Utilizarea valorilor AL-backoff duc la creşterea jitter-ului şi a timpului dus-întors, crescând rata de pierdere. Un salt particular în rata de pierdere poate fi sesizat ca şi cum s-ar comasa timpii de aşteptare reali şi ar rezulta o coliziune între două pachete consecutive VoIP.

După cum arăta cele două scenarii, un mecanism care să reducă efectele valorii Al-backoff poate fi de ajutor, în special pentru valori mici ale acestuia. Rata de pierdere se poate îmbunătăţi în mod semnificativ atunci când este folosit un astfel de mecanism pentru transmiteri multiple.

4.10 Concluzii

Acest capitol se adresează problemelor de securitate şi mobilitate prin integrarea, sub formă de noutate, a unor caracteristici de securitate robuste protocolului IAX. **Au fost analizate din punct de vedere teoretic proprietăţile de securitate şi mobilitate ale standardului IEEE 802.11 şi pe baza acestor rezultate a fost dezvoltat un modul software. Modulul software creat pentru a evalua această abordare a avut următoarele proprietăţi:**

- **a permis alegerea a 5 metode diferite de criptare;**
- **a traversat cu succes translatorul de adrese de reţea (NAT-Network Address Translator);**
- **a simulat schimbul de chei prin utilizarea cheilor de sesiune pre–partajate;**
- **securitate puternică;**
- **nici o modificare pentru cerinţele de lăţime de bandă;**
- **cerinţe relativ mici în utilizarea procesorului.**

Am selectat Softphon-ul Kiax ca bază pentru sistemul propus, deoarece a fost la dispoziţie ca şi licenţă open-source. Rezultatele de performanţă testate demonstrează în mod clar fezabilitatea acestei abordări.

Am folosit ca şi algoritm de securitate Cryptlib, un modul open source care este conceput să ofere servicii de securitate pentru aplicaţii.

Cryptlib oferă o interfaţă standardizată pentru o serie algoritmi de criptare populari. Permite ascunderea în cea mai mare parte a detaliilor de implementare şi

foloseşte un sistem de codare independent de sistemul de operare, fapt ce facilitează transferul de date securizate de la un mediu de operare la altul.

Folosind acest algoritm am creat un modul de program pe care l-am înglobat apoi în softphon-ul Kiax pentru a asigura o comunicaţie sigură client/server.

Asigurarea confidenţialităţii şi autentificării în cadrul comunicaţiei dintre client şi server se realizează folosind un sistem criptografic ce utilizează chei publice şi private pentru distribuţia cheilor de sesiune şi chei simetrice pentru criptarea datelor ce se transmit pe canal.

O parte importantă a sistemului o constituie protocolul de conectare prin care se realizează autentificarea părţilor, distribuţia cheilor de sesiune şi iniţializarea conexiunii. De asemenea am urmărit şi performanţele legate de utilizarea procesorului şi a lăţimii de bandă.

În ansamblu, rezultatele atât pentru calitatea apelului cât şi a utilizării procesorului sunt similare pentru diferiţi algoritmi de criptare. Cu toate acestea, algoritmul de criptare avansată standard (AES) în modul de feedback al cifrului (CFB) ar trebui să fie considerată ca metodă preferată, deoarece oferă cea mai mică medie de încărcare a procesorului, nu adăuga cerinţe de lăţime de bandă suplimentare şi introduce un minim de probleme în fluxul audio.

Toate reţelele fără fir sunt expuse riscului de compromitere oferind un punct de acces la reţelele fizice interne, dincolo de controalele de securitate ale nivelului fizic. Din păcate, problema nu este uşor de rezolvat nici în viitor. O soluţie intermediară de reducere a riscurilor de securitate, pe termen scurt, (nu este o soluţie completă) este un sistem de management robust al cheilor pentru WEP şi utilizarea unor mecanisme de nivel mai ridicat de securitate, de exemplu, IPsec. Cu toate acestea, aceste mecanisme, atenuează doar problema, dar nu o rezolvă. Stabilirea unui algoritm care să fie încapsulat în standardul IEEE 802.11 este misiunea comisiei de standarde. Până atunci pachetele falsificate vor fi în continuare o problemă. Singura soluţie bună pe termen lung este o revizuire majoră a standardelor actuale, care pot solicita înlocuirea punctului de acces curent (cu toate că în unele cazuri, o actualizare a firmware-ului nu ar putea fi posibil). Din fericire, se lucrează în prezent la îmbunătăţiri semnificativă a standardului IEEE 802.11 [34]. Cu toate acestea, este prea târziu pentru reţelele existente şi pentru cele pe cale de a fi extinse. O serie de furnizori, care oferă puncte de acces, susţin că investesc enorm pentru creşterea securităţii. Din păcate, puţine din produse furnizează suficiente informaţii pentru a putea trage concluzia că se asigură o securitate a reţelei sută la sută. Mai rău, multe din produsele care nu furnizează suficiente informaţii utilizează un algoritm de autentificare Diffie-Hellman care suferă de cunoscutul 'man in the middle of attack'. Utilizarea de autentificări bazate pe algoritmul Diffie-Hellman introduce o mai mare vulnerabilitate în organizarea reţelei. Creşterea riscurilor se produce când un atacator se poate insera personal în mijlocul schimbului de chei între client şi punctul de acces şi poate obţine cheia de sesiune K. Acest fapt este semnificativ mai rău decât în situaţia curentă unde atacatorul trebuie să stabilească mai întâi un flux pseudo aleator produs pentru o anumită cheie, K şi vector public IV, şi apoi să utilizeze fluxul pentru a falsifica pachetele.

Un alt studiu prezentat în acest capitol este pentru traficul la nivelul substratului de acces la mediu cu distribuţie multiplă din reţelele fără fir bazate pe standardul IEEE 802.11. Rezultatele arată că într-o topologie liniară simplă, rata de pierdere a cadrelor/salt este între 0,2% şi 0,7%. Prin urmare, chiar şi atunci când se utilizează astfel de reţele, exclusiv pentru trafic VoIP cu distribuţie multiplă, pierderea de cadre devine critică dacă traficul trece prin mai mult de patru staţii. **Problema staţiilor ascunse poate duce la pierderea semnificativă de**

cadre, făcând traficul VoIP inutilizabil. Experimentele sugerează că,deşi traficul VoIP tolerează unele pierderi, distribuţia multiplă poate, în general, să fie utilizată numai dacă mecanisme suplimentare vor fi implementate în straturile superioare ale reţelei pentru a atenua pierderile de cadre de la ni velul substratului de acces la mediu.

În pofida rezultatelor obţinute în acest studiu experimental, transmisia cu distribuţie multiplă poate încă să fie "suficient de bună" în multe scenarii, în special dacă densitatea staţiilor este mare. În activitatea viitoare, îmi propunem să efectuez simulări care utilizează rezultatele experimentelor descrise în acest document ca intrare şi să investighez astfel de situaţii. În plus, am în plan analiza calităţii traficului de voce atunci când se utilizează tehnici de securitate pentru distribuţia multiplă şi tehnici de rutare sofisticate. De asemenea, doresc să experimentez utilizarea distribuţiei spre un singur punct şi puncte multiple pentru distribuţia traficului VoIP prin reţele fără fir bazate pe standardul IEEE 802.11.

5. CONTRIBUŢII ŞI CONCLUZII

Asigurarea calităţii în sistemul de telefonie VoIP bazat pe standardul IEEE 802.11 implică interacţiunea mai multor factori cum ar fi: sistemul de operare, interoperarea între reţele, protocoalele VoIP, criptografia şi securitatea întregului sistem.

Din punct de vedere al securităţii, sunt aceleaşi probleme de rezolvat ca şi în reţelele fixe. Singura diferenţă este cea legată de securizarea legăturii fără fir.

Deoarece mediul de transmitere este aerul, comunicaţiile pot fi mai uşor interceptate. Atacatorii pot să se conecteze ilegal la aceste reţele şi să lanseze atacuri. În plus, atacatorii pot să se mascheze în puncte de acces legale, păcălind astfel utilizatorii.

Pentru securizarea unei conexiuni VoIP fără fir se impun măsuri de securitate suplimentare faţă de o conexiune dintr-o reţea fixă. Standardul IEEE 802.11 reglementează această problemă. Deşi măsurile de securitate nu pot elimina în totalitate posibilitatea producerii unor incidente, probabilitatea de reuşită a atacurilor poate fi diminuată substanţial. Prin implementarea şi supravegherea politicilor de securitate se doreşte evitarea unor incidente.

În lucrarea de doctorat s-au evidenţiat breşele din mecanismele de securitate utilizate de majoritatea punctelor de acces ale reţelelor fără fir bazate pe standardul IEEE 802.11. Barierele de securitate (securitatea de bază) care au fost prevăzute în protocoalele reţelelor fără fir asigură un nivel relativ scăzut al securităţii acestor reţele, ceea ce le-a frânat întrucâtva dezvoltarea.

Securitatea de bază a reţelelor fără fir este asigurată prin implementarea următoarelor funcţii: set de servicii de identificare (SSID-Service Set Identifiers), chei secrete partajate şi verificarea adresei mediului de acces (MAC-Media Acces Control).

În practică, mecanismele de securitate bazate pe un secret partajat nu sunt foarte robuste şi nu asigură protecţie atât la utilizare cât şi la distribuţie. Din păcate, mai multe mesaje de management conţin numele reţelei sau funcţia SSID. Aceste mesaje sunt difuzate în clar de către punctele de acces şi de clienţi. Mesajul real, care conţine funcţia SSID, depinde de furnizorul punctului de acces. Rezultatul final este că un atacator poate depista numele reţelei, stabilind astfel cheia partajată şi putând astfel pătrunde în reţeaua utilizatorului. Acest aspect există chiar şi cu funcţia WEP, pentru că mesajele de management sunt difuzate în clar.

O aplicaţie VoIP este alcătuită din două părţi componente: aplicaţia *Client*, aplicaţia *Server*. Cele două funcţionează ca nişte automate cu stări finite ce comunică prin semnale.

Rezultatele experimentale au confirmat că asigurarea confidenţialităţii şi autentificării în cadrul comunicaţiei dintre client şi server se poate realiza folosind un sistem criptografic hibrid ce utilizează chei publice şi private pentru distribuţia cheilor de sesiune şi cheilor simetrice pentru criptarea datelor ce se transmit pe canal.

O parte importantă a sistemului o constituie protocolul de conectare prin care se realizează autentificarea părţilor, distribuţia cheilor de sesiune şi iniţializarea conexiunii.

În lucrarea de doctorat se pot evidenţia un număr de 10 contribuţii teoretice şi experimentale, cu caracter de noutate în domeniul iniţializării şi securităţii protocolului SIP în reţelele fără fir, prezentate sintetic în continuare, fiind însoţite de referinţe bibliografice, cu referire la articolele publicate.

5.1 Contribuţii teoretice

(1) Efectuarea de cercetări privind numărul maxim de apeluri admise în listele de interogare ale punctelor de acces bazate pe standardul IEEE 802.11.

Am cercetat fundamentele teoretice ale funcţiei de coordonare prin punct ce permite accesul centralizat în reţeaua fără fir. Am descris un model analitic şi am experimentat un algoritm de control al numărului de apeluri vocale admise în lista de interogare şi invitare la emisie a punctelor de acces din reţele fără fir, pentru a reduce întârzierile în momentul transmiterii şi recepţionării pachetelor de date, (capitolul 3, paragraful 3.5.3), [39].

(2) Efectuarea de cercetări privind întârzierile din sesiunea de iniţializare a protocolului de semnalizare SIP, folosit pentru a stabili, modifica şi iniţia apelurile telefonice VoIP.

Am determinat principalii parametrii care produc întârzieri semnificative ale sesiunii de iniţializare a protocolului SIP în reţelele fără fir şi care afectează calitatea acesteia. Aceştia sunt: întârzierea la transmiterea prin reţea, fapt ce poate produce pierderi şi cozile de aşteptare, (capitolul 3, paragraful 3.2), [38].

(3) Analiza comparativă a performanţelor sesiunii de iniţializare a protocolului SIP funcţie de protocolul de transport utilizat.

Această analiză comparativă mi-a permis evaluarea ratei de eroare a cadrelor (FER-Frame Error Rate) funcţie de protocoalele de transport utilizate: TCP, UDP şi RLP. Întârzierile produse de fiecare dintre ele depind de mărimea pachetelor de semnalizare implicate în stabilirea sesiunii şi de numărul de servere pe care acestea le traversează până la destinaţie, (capitolul 3, paragrafele 3.3.2-3.3.5), [38].

(4) Realizarea unui studiu comparativ al mecanismelor de control al accesului în punctele de acces, AP, ale reţelelor fără fir.

Acest studiu comparativ, evidenţiază breşele din mecanismele de securitate utilizate de marea majoritate a punctelor de acces care au la bază standardul IEEE 802.11.

Concluzia finală este ca toate reţelele fără fir bazate pe standardul IEEE 802.11 sunt expuse riscului deoarece accesul la reţelele fizice, ale utilizatorilor se face după implementările de securitate ale acestora. Din păcate, problema nu este uşor de rezolvat. Singura soluţie bună pe termen lung este o revizuire majoră a standardelor actuale şi introducerea unui sistem robust de management al cheii partajate şi utilizarea unor mecanisme de nivel mai ridicat de securitate, de exemplu, IPsec, (capitolul 4, paragraful 4.2), [41].

(5) Justificarea necesităţii corecţiei erorilor pachetelor în reţelele fără fir bazate pe standardul IEEE 802.11

Necesitatea corecţiei erorolor este motivată de faptul că subnivelul accesului la mediu (MAC-Medium Access Control) al standardului IEEE 802.11 suportă retransmiteri ale pachetelor, impuse de erorile de transmisie ale celor două funcţii ale standardului IEEE 802.11 de coordonare prin punct (PFC) şi coordonare distribuită (DCF). În mod normal retransmiterile sunt evitate pentru traficul în timp real datorită întârzierilor pe care le implică, (capitolul 3, paragraful 3.7), [41] .

(6) Efectuarea de cercetări privind performanţa şi fiabilitatea transmisiei vocii către destinaţii multiple în subnivelul de acces la mediu al reţelelor fără fir bazate pe standardul IEEE 802.11.

Experimentele arată că pentru o transmisie către destinaţii multiple pachetele ajung la destinaţie şi pot fi reasamblate dacă nu trec prin mai mult de 4 staţii, eroarea fiind între 0,2-0,7 %. Staţiile ascunse pot conduce la rate de eroare mult mai mari. Chiar dacă traficul VoIP acceptă erori mai mari, controlul de acces la mediu pentru astfel de situaţii necesită corecţii de pachete la nivelul straturilor superioare, (capitolul 4, paragraful 4.6), [37].

(7) Analiza comparativă privind performanţele celor două protocoale de semnalizare SIP şi H.323.

Această comparaţie mi-a permis să definesc o direcţie prin care să se poată reduce întârzierile în iniţializarea unei sesiuni de iniţializare SIP, (capitolul 3, paragraful 3.4), [38].

5.2 Contribuţii aplicative

(8) Implementare unui contor adaptiv pentru retransmitere în scopul reduceri timpului de iniţializare SIP.

Bazându-mă pe analiza comparativă privind performanţele celor 2 protocoale de semnalizare SIP şi H.323 am realizat un contor adaptiv pentru retransmitere care să se poată adapta la mărimea pachetelor de semnalizare implicate în stabilirea conexiunii , (capitolul 3, paragraful 3.3.1.), [38].

(9) Implementarea unui modul de program software care să asigure securitatea şi mobilitatea aplicaţiilor VoIP.

Această implementare mi-a permis crearea unui modul de program software care să răspundă următoarelor cerinţe, (capitolul 4, paragraful 4.3), [40].

- permite alegerea a 5 metode diferite de criptare;
- translatarea cu succes a adreselor dintr-o reţea privată în publice (NAT-network Address Translation);
- simularea de cheie de schimb prin utilizarea cheilor de sesiune partajate;
- securitate foarte bună;
- nici o modificare la cerinţele de lăţime de bandă;
- cerinţe reduse pentru procesorul calculatorului utilizat.

(10) Implementat unui sistem criptografic pentru o comunicaţie sigură client-server

Criptografia şi securitatea datelor sunt baza fără de care nu se poate discuta despre securitatea transmiterii prin Internet a informaţiilor. Contribuţia originală constă în realizarea unui sistem criptografic pentru o comunicaţie sigură client / server, (capitolul 4, paragraful 4.3), [40].

5.3 Consideraţii finale

Toate reţelele fără fir dezvoltate pe baza standardul IEEE 802.11 sunt expuse riscului de compromitere, oferind un punct de acces la reţelele fizice interne, dincolo de controalele de securitate ale nivelului fizic. Din păcate, problema nu este uşor de rezolvat nici în viitor. O soluţie intermediară de reducere a riscurilor de securitate pe termen scurt (nu este o soluţie completă) este un sistem de management robust al cheilor partajate şi utilizarea unor mecanisme de nivel mai ridicat de securitate, de exemplu IPsec. Cu toate acestea, aceste mecanisme, doar atenuează problema, dar nu o rezolvă. Stabilirea unui algoritm care să fie încapsulat în standardul IEEE 802.11 este misiunea comisiei de standarde. Până atunci pachetele falsificate vor fi în continuare o problemă. Singura soluţie bună pe termen lung este o revizuire majoră a standardelor actuale, care pot solicita înlocuirea punctului de acces (AP acces point) curent (cu toate că în unele cazuri, o actualizare a firmware–ului nu ar putea fi posibil). Din fericire, se lucrează în prezent la îmbunătăţiri semnificative a standardului IEEE 802.11. Cu toate acestea, este prea târziu pentru reţelele existente şi pentru cele pe cale de a fi extinse. O serie de furnizori, care oferă puncte de acces, susţin că investesc enorm pentru creşterea securităţii. Din păcate, puţine din produse furnizează suficiente informaţii pentru a putea trage concluzia că se asigură o securitate sută la sută a reţelei. Mai rău, multe din produsele care nu furnizează suficiente informaţii utilizează un algoritm de autentificare Diffie-Hellman care suferă de cunoscutul *"man in the middle of attack"*. Utilizarea de autentificări bazate pe algoritmul Diffie-Hellman introduce o mai mare vulnerabilitate în organizarea reţelei. Creşterea riscurilor se produce şi când un atacator se poate insera personal, în mijlocul schimbului de chei între client şi punctul de acces şi poate obţine cheia de sesiune.

Lucrarea de doctorat aduce soluţii originale ce permit creşterea securităţii schimbului de mesaje într-o aplicaţie VoIP, bazată pe o conexiune client/server. Soluţiile de securitate propuse în cadrul lucrării de doctorat completează soluţiile de securitate cunoscute, putând fi aplicate concomitent cu acestea.

Lucrarea de doctorat vine de asemenea cu o soluţie originală de reducere a întârzierilor în sesiunea de iniţializare a unei conexiuni VoIP, printr-un contor adaptiv pentru retransmitere a pachetelor. Tot în scopul reducerii timpului de iniţializare a unei sesiuni VoIP am făcut şi un studiu comparativ al protocoalelor utilizate. Pentru o rată de eroare mai mare de 2% este de preferat protocolul SIP în locul lui H.323.

Îmbunătăţiri ale transmiterii vocii prin reţelele fără fir pot fi aduse în toate straturile acesteia. Această teză stabileşte un număr de convorbiri care pot fi admise în lista de interogare şi invitare la emisie a funcţiei de coordonare prin punct la nivelul substratului de acces la mediu al unei reţele fără fir. Astfel, pentru o rată de 11 Mbps, sunt admise în lista de interogare 26 de convorbiri pentru o mărime a supercadrului nu mai mare de 90 ms şi o întârziere maximă de 303 ms. Tot din motive

de limitare a întârzierilor se preferă modul de transmitere cu rată de biţi constantă (CBR).

O altă propunere cu caracter de noutate este utilizarea în transmisiile VoIP a protocolului IAX şi a unei interfeţe prevăzută cu un modul de securitate pentru transmiterea şi recepţionarea pachetelor de date.

Această teză aduce ca noutate şi un studiu al distribuţiei multiple a traficului de voce în reţelele bazate pe standardul IEEE 802.11. Rezultatele arată că pentru o reţea cu o rată de 2 Mbps, rata maximă de transfer este de 1,76 Mbps. De asemenea numărul maxim de staţii prin care se poate face redirecţionarea este limitat la patru, altfel se depăşeşte raportul de pierdere a cadrelor/obstacol ce trebuie să fie între 0,2% şi 0,7%. Prin urmare, chiar şi atunci când se utilizează astfel de reţele exclusiv pentru trimiterea multiplă a traficului de voce, pierderea de cadre devine critică dacă traficul este transmis prin mai mult de patru staţii. Problema staţiilor ascunse poate duce de asemenea la pierderea semnificativă de cadre, făcând imposibilă refacerea semnalului. Experimentele au arătat, că deşi traficul VoIP tolerează unele pierderi, trimiterea multiplă (MAC distribuţia multiplă) poate, în general, să fie utilizată numai dacă mecanisme suplimentare sunt prevăzute la nivelurile superioare. Rolul acestora este de a atenua pierderea de cadre din substratul de acces la mediu (MAC). În pofida rezultatelor obţinute în acest studiu experimental, transmisiile multiple pot fi suficient de bune în multe scenarii, în special dacă densitatea staţiilor este mare.

BIBLIOGRAFIE

[1] Agarwal A.K., Wang W. , *On the impact of quality of protection in wireless local area networks with IP mobility,* Mobile Networks and Applications Journal, Volume 12, Issue 1, pp.93-110, ISSN 1383-469X, Kluwer Academic Publishers, Hingham, MA, USA, January 2007.

[2] Albers J., Hahn B., McGann S., Park S., Zhu R., *An Analysis of Security Threats and Tools in SIP-Based VoIP Systems,* http://www.colorado.edu /cs/policylab/, University of Colorado, Boulder, April 2005.

[3] An Chan, Liew S. C., *Performance of VoIP over Multiple Co-Located IEEE 802.11 Wireless LANs*, Mobile Computing, IEEE Transactions 2009, Volume 8, Issue 8, pp. 1063-1076, ISSN 1536-1233, IEEE Computer Society, August 2009.

[4] Balachandran A., Voelker G.M., Bahl P., *Wireless Hotspots: Current Challenges and Future Directions,* Mobile Networks and Applications, Volume 10, Number 3, pp.265-274, ISSN 1383-469X, Springer Netherlands, June 2005.

[5] Bandyopadhyay S., Coyle E.J., Falck T., *Stochastic Properties of Mobility Models in Mobile Ad Hoc Networks,* Mobile Computing, IEEE Transactions on, Volume 6, Issue 11, pp.1218-1229, ISSN 1536-1233, November 2007.

[6] Barker E., Roginsky A., *DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes,* National Institute of Standards and Technology, Special Publication SP 800-131, Gaithersburg, MD, USA, January 2010.

[7] Benini M., Sicari S., *Assessing the risk of intercepting VoIP calls Source,* The International Journal of Computer and Telecommunications Networking, Volume 52, Issue 12, pp.2432-2446, ISSN 1389-1286, Elsevier North-Holland, Inc. New York, NY, USA, August 2008.

[8] Berger A., Hefeeda M., *Exploiting SIP for botnet communication*, Secure Network Protocols 2009. NPSec 2009. 5th IEEE Workshop on, pp.31-36, ISBN 978-1-4244-4866-1, Princeton, New Jersey, USA, October 2009.

[9] Bianchi G., *Performance analysis of the IEEE 802.11 distributed coordination function*, *IEEE Journal of Selected Areas in Communications*, Vol. 18, pp.535–547, 2000.

[10] Binet D., Martin A.,Gaabab B., *A Proactive Authentication Integration for the Network Mobility*, Third International Conference on Wireless and Mobile Communications (ICWMC'07), pp. 53-59, ISBN 0-7695-2796-5, Guadeloupe, French Caribbean, March 2007.

[11] Boyle D., Newe T., *Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures*, Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference, pp.54-60, ISBN 0-7695-2796-5, Guadeloupe, French Caribbean, March 2007.

[12] Camilo T., Pinto P., Rodrigues A., Sa Silva J., Boavida F., *Mobility management in IP-based Wire-less Sensor Networks*, Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 1-8, ISBN 978-1-4244-2099-5, Newport Beach, California, USA, June 2008.

[13] Canberk B., Oktug S., *Self Similarity Analysis and Modeling of VoIP Traffic under Wireless Heterogeneous Network Environment,* Telecommunications, 2009. AICT'09. Fifth Advanced International Conference on, pp.76-82, ISBN 978-1-4244-3840-2, Venice, Italy, May 2009.

[14] Casola V., Mazzeo A., Mazzoccca N., Rak M., *Security design and evaluation in a VoIP secure infrastructure*, Proceedings of ITCC'05, volume 1, pp.727–732, ISBN 0-7695-2315-3, Las Vegas, Nevada, USA, April 2006.

[15] Celik Guner D., Zussman G., Khan Wajahat F., Modiano E., *MAC for Networks with Multipacket Reception Capability and Spatially Distributed Nodes*, IEEE Transactions on Mobile Computing Volume 9, Issue 2, pp. 226-240, ISSN:1536-1233, Piscataway, New Jersey, USA , February 2010.

[16] Chan Yeob Yeun, Salman Mohammed Al-Marzouqi, *Practical Implementations for Securing VoIP Enabled Mobile Devices*, 2009 Third International Conference on Network and System Security 2009, pp.409-414, ISBN 978-0-7695-3838-9, Gold Coast, Queensland, Australia, October 2009.

[17] Chang Chin-Chen, Chiu Yen-Chang, Tsai Hao-Chuan, *A Simple and Robust Authenticated Multiple Key Agreement Scheme*, International Conference on Security Technology, SECTECH '08, pp. 214-218, ISBN 978-0-7695-3486-2, Hainan Island, China, December 2008.

[18] Chen Lin, Leneutre J.A, Puig J.-J., *Secure and Efficient Link State Routing Protocol for Ad Hoc Networks*, Wireless and Mobile Communications, 2006. ICWMC'06. International Conference on, pp.36-42, ISBN 0-7695-2629-2, Bucharest, Romania, July 2006.

[19] Chen Ling, Lu Jian-de, *IMEWAS--A Integrated Multi-platform EAPoW-Based WLAN AAA Solution*, Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, pp.17–21, ISBN 0-7695-2796-5, Guadeloupe, French Caribbean, March 2007.

[20] Chen Z., Wang L., Wang X., Chen Hsiao-Hwa, *Voice over Internet Protocol over IEEE 802.11 Wireless Local Area Networks and effective admission control with transmission interval adaptation,* International Journal of Autonomous and Adaptive Communications Systems, Volume 1, Issue 1, pp.82-105, ISSN 1754-8632, Inderscience Publishers, Geneva, Switzerland, July 2008.

[21] Cheriton D.R., Faria D.B., *Detecting Identity-Based Attacks in Wireless Networks Using Signal Prints,* Proceedings of the 5th ACM workshop on Wireless security, SESSION: Radio-layer security, pp.43-52, ISBN 1-59593-557-6, Los Angeles, California, September 2006 .

[22] Choi S., Prado J., Mangold S., Shankar S., *IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation*, Proceedings of the IEEE International Conference on Communications (ICC), pp.1151–1156, 2003.

[23] Cole R.G., Rosenbluth J.H., *Voice over IP performance monitoring*, ACM SIGCOMM Computer Communication Review, Volume 31, Isssue 2, pp.9–24, ISSN 0146-4833, ACM, New York, NY, USA, 2001.

[24] Cuppens F., Cuppens-Boulahia N., Nuon S., Ramar T., *Property Based Intrusion Detection to Secure OLSR*, Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, pp.52–60, ISBN 0-7695-2796-5, Guadeloupe, French Caribbean, March 2007.

[25] D.Binet, A.Martin, B.Gaabab, *A Proactive Authentication Integration for the Network Mobility,* Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, ISBN: 0-7695-2796-5, pp:53-53, Guadeloupe, French Caribbean, March 2007.

[26] Degabriele J.P., Paterson K.G., *Attacking the IPsec Standards in Encryption-only Configurations, Security and Privacy*, 2007. SP '07. IEEE Symposium on, pp.335-349, ISSN 1081-6011, Berkeley, California, USA, May 2007.
[27] Garg S., Kappes M. *'Can I add a VoIP call?'*, Paper presented in the Proceedings of the *IEEE International Conference on Communications (ICC)*, Anchorage, Alaska, May, 2003.
[28] Guillen E. P., Chacon D. A., *VoIP Networks Performance Analysis with Encryption Systems*, World Academy of Science, Engineering and Technology, Volume 58, art.119, pp.688-696, ISSN 2070-3724, Venice, Italy, October 2009.
[29] Gupta G.R., Shroff N.B, *Delay analysis of scheduling policies in wireless networks*, Signals, Systems and Computers, 2008 42nd Asilomar Conference on, pp.2137-2141, ISSN 1058-6393, Pacific Grove, CA ,USA, October 2009.
[30] Gupta P., Shmatikov V., *Security Analysis of Voice-over-IP Protocols*, Computer Security Foundations Symposium, 2007. CSF '07. 20th IEEE, pp.49-63, ISSN 1063-6900, Venice, Italy, July 2007.
[31] Hayajneh T., Krishnamurthy P., Tipper D., *De Worm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad Hoc Network,* Network and System Security 2009, NSS'09. Third International Conference on, pp.74-80, ISBN 978-0-7695-3838-9, Gold Coast, Queensland, Australia, October 2009.
[32] Hong Hou, Borkar V., Kumar P.R., *A Theory of QoS for Wireless*, Proceedings of Infocom 2009, pp.486-494, ISSN 0743-166X, Rio de Janeiro, Brazil, April, 2009.
[33] Hu X., Morely Mao Z.*, Accurate Real-time Identification of IP Prefix Hijacking,* Security and Privacy, 2007. SP '07. IEEE Symposium on, pp.3-17, ISSN 1081-6011, Berkeley, California, USA, May 2007.
[34] IEEE 802 Standards and the Committee (1999) *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ISO/IEC 8802-11: 1999(E).
[35] IEEE 802 Standards and the Committee (2004) *Draft Supplement to Part 11: Medium Access Control (MAC) Enhancements for Quality of Service (QoS*), IEEE STD 802.11e/D8.0, February.
[36] Intel Co., Ltd. (2007) *Enhance Collaboration and Communication through VoIP*. Available at: http://www.intel.com/netcomms/.
[37] **Ioaneşiu M**., *An Experimental Analysis of Performance of MAC Multicast Distribution in 802.11 Networks for VoIP Traffic*, Lucrările sesiunii de comunicări ştiinţifice „Doctor Etc 2009", Timişoara, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, pp.49-54, ISSN 2066-883X, Timişoara, September 2009.
[38] **Ioaneşiu M**., Toma C.I., *Optimization of SIP session setup delay for VOIP in 3G wireless networks*, Proceedings of the 4th International Conference on Engineering Technologies–ICET 2009, pp. 367-375, ISBN 978-86-7892-227-5, Novi Sad, Serbia, April 2009.
[39] **Ioaneşiu M**., Toma C.I., *Support of Voice services in IEEE 802.11 wireless LANs*, Proceedings of the 4th International Conference on Engineering Technologies–ICET 2009, pp. 379-385, ISBN 978-86-7892-227-5, Novi Sad, Serbia, April, 2009.
[40] **Ioaneşiu M**., *Security of Mobile VoIP*, International Symposium on Electronics and Telecommunications, ETC 2008, Eight Editions, Buletinul Ştiinţific al Universităţii „Politehnica" din Timişoara, Tom 53 (67), Fascicola 2, 2008, pp.

36-41, ISSN 1583-3380, Seria Electronică şi Telecomunicaţii, Timişoara, September 2008.
[41] **Ioaneşiu M**., *The security in wireless networks based on 802.11 standards. Problems and solutions. Developments of 802.11 standards in connection with security problems*, Lucrările sesiunii de comunicări ştiinţifice „Doctor Etc 2007", Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, pp. 88–93, ISBN 978–973–625–494-9, Timişoara, September, 2007.
[42] **Ioaneşiu M**., *Securitatea datelor prin criptare,* Referatul 3 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2006.
[43] **Ioaneşiu M.,** *Stadiul actual şi de perspectivă al securităţii reţelelor de calculatoare,* Referatul 2 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2005.
[44] **Ioaneşiu M.**, *VPN şi securitatea datelor***,** Referatul 1 pentru doctorat, Universitatea „Politehnica" din Timişoara, Facultatea de Electronică şi Telecomunicaţii, Departamentul Comunicaţii, 2004.
[45] Izquierdo A., Sierra J.M., Torres J., *An analysis of conformance issues in implementations of standardized security protocols*, Computer Standards & Interfaces, Volume 31 , Issue 1, pp.246-251, ISSN 0920-5489, Elsevier Science Publishers B.V. Amsterdam, Netherlands, January 2009.
[46] Johnston A., Sparks R., Cunningham C, Donovan S., Summers K., *Session Initiation Protocol Service Examples*, Network Working Group Request for Comments:5359, http://tools.ietf.org/html/rfc5359, October 2008.
[47] Juniper Networks, *Enterprise VoIP security*, White papers, Part Number 200179-001, Juniper Networks, Inc., USA, 408 745 2000 or 888 JUNIPER, www.juniper.net, April 2006.
[48] Khan K.M., Han J., Specifying *Security Goals of Component Based Systems: An End-User Perspective*, Composition-Based Software Systems, 2008. ICCBSS 2008. Seventh International Conference on, pp. 101-109, ISBN 978-0-7695-3091-8, Madrid, Spain, February 2008.
[49] Kolahi S.S., Mani P., Narayan S., Nguyen D.D.T., Sunarto Y., *The impact of wireless LAN security on performance of different Windows operating systems,* IEEE Symposium on Computers and Communications, ISCC 2008, pp.260–264, ISSN 1530-1346, Marrakech, Maroc, July 2008.
[50] Kuhn D.R., Walsh T.J., Fries S., *Security Considerations for Voice Over IP Systems*, National Institute of Standards and Technology, Special Publication SP 800-58, Gaithersburg, MD, USA, January 2005.
[51] Le Boudec J.-Y., Vojnovic M., *The Random Trip Model: Stability, Stationary Regime, and Perfect Simulation*, Networking, IEEE/ACM *Transactions on,* pp.1153-1166, Volume 14, Issue 6, ISSN 1063-6692, San Francisco, California, USA, December 2006.
[52] Lewis N., Foukia N., *An Efficient Reputation-Based Routing Mechanism for Wireless Sensor Networks: Testing the Impact of Mobility and Hostile Nodes,* Proceedings of the 2008 Sixth Annual Conference on Privacy, Security and Trust, pp.151-155, ISBN 978-0-7695-3390-2, Fredericton, New Brunswick, Canada, October 2008.
[53] Liang W., Wang W., *A quantitative study of authentication and QoS in wireless IP networks*, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Com-

puter and Communications Societies. Proceedings IEEE, Volume 2, pp. 1478-1489, ISSN 0743-166X, Miami, Florida, USA, March 2005.
[54] Manivannan N., Neelameham P., *Alternative Pair-wise Key Exchange Protocols (IEEE 802.11i) in Wireless LANs,* Wireless and Mobile Communications, 2006. ICWMC'06. International Conference on, pp.52-60, ISBN 0-7695-2629-2, Bucharest, Romania, July 2006
[55] Marius HERCULEA, Tudor Mihai BLAGA, Virgil DOBROTA, *Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture*, 7th RoEduNet International Confrence 2008, Cluj Napoca, Romania, August 2008.
[56] Marshall P.F., *Recent progress in moving cognitive radio and services to deployment*, World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on, pp. 1-8, ISBN 978-1-4244-2099-5, Newport Beach, California, USA, June 2008.
[57] Melnyk M., Jukan A., *On Signaling Efficiency for Call Setup in all-IP Wireless Networks,* ICC apos;06. IEEE International Conference, Volume 5, pp.1939-1945, Istambul, Turkey, June 2006.
[58] Moon Jong-Sik**,** Lee Sun-Ho, Park Jong-Hyuk, Lee Deok-Gyu, Lee Im-Yeong**,** *Admissible Bilinear Map Based Key Management Technology in Heterogeneous Mobile Networks***,** International Conference on Security Technology, 2008, SECTECH apos;08, pp.242–247, ISBN 978-0-7695-3486-2, Hainan Island, China, December 2008.
[59] Morvan M., Sené S., *A Distributed Trust Diffusion Protocol for Ad Hoc Networks,* Wireless and Mobile Communications, 2006. ICWMC'06. International Conference on, pp. 87-83, ISBN 0-7695-2629-2, Bucharest, Romania, July 2006.
[60] Myakotnykh E.S., Thompson R.A., *Adaptive Speech Quality Management in Voice-over-IP Communications*, Fifth Advanced International Conference on Telecommunications 2009, pp.64–71, ISBN 978-1-4244-3840-2, Venice/Mestre, Italy, May 2009.
[61] Ng Ching Yu, *Contributions to Security in Wireless Ad-Hoc Networks*, Computing Science Department, University of Wollongong, Australia, 2005. http://ro.uow.edu.au/theses/38.
[62] Niculescu G.,Bărbălău S., *Analiza și modularea sistemelor de comunicații*, Editura MatrixRom, București, 1997;
[63] Papadimitriou A,.Le Fessant F, Viana A.C., Sengul C., *Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks*, Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on, pp. 43-48, ISBN 978-1-4244-4866-1, Princeton, New Jersey, USA, October 2009.
[64] Paterson K.G., Yau A.K.L., *Lost in Translation: Theory and Practice in Cryptography,* IEEE Security and Privacy, Vol.4, No.3, pp.69-72, ISSN 1540-7993, May-June 2006.
[65] POTORAC, A. D., *Considerations on VoIP Throughput in 802.11 Networks*, Advances in Electrical and Computer Engineering Volume 9, Issue 3, pp. 45-50, Year: 2009, ISSN 1582-7445, Suceava, Romania, October 2009.
[66] Rehart R., *Securing Voice Traffic Over Wireless Packet Networks,* http://www.docstoc.com/docs/12874303/Voice-security-of-Wireless-Networks/, February 20, 2006
[67] Rughinis R. Iconaru C., *A Practical Analysis of Asterisk SIP Server Performance*, 7th RoEduNet International Confrence 2008, Cluj Napoca Romania, August 2008.

[68] Saltuk Aksahin, *Security Implications of Converged Networks and Protecting them, without Comprising Efficiency*, Volume abs/cs/0702110, Journals CoRR, http://arxiv.org/abs/cs/0702110, February 2007

[69] Sangho S., Schulzrinne H., *Call Admission Control in IEEE 802.11 WLANs Using QP-CAT*, INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp.726-734, ISSN 0743-166X, Phoenix, Arizona, USA, April 2008.

[70] Shankesi R., AlTurki M., Sasse R., Gunter Carl A., Meseguer J., *Model-Checking DoS Amplification for VoIP Session Initiation*, Symposium on Research in Computer Security (ESORICS '09), Volume 5789, pp.390-405, ISSN 0302-9743, Saint Malo, France, September 2009.

[71] Sharma G., Mazumdar R., Shroff Ness B., *Delay and Capacity Trade-Offs in Mobile Ad Hoc Networks: A Global Perspective,* IEEE/ACM Transactions on Networking (TON), Volume 15, Issue 5, pp.981-992, ISSN 1063-6692, San Francisco, California, USA October 2007.

[72] Shi E., Bethencourt J., Chan T.-H.H., Dawn Song Perrig A., *Multi-Dimensional Range Query over Encrypted Data*, Security and Privacy, 2007. SP '07. IEEE Symposium on, pp.350-364, ISSN 1081-6011, Berkeley, California, USA, May 2007.

[73] Shin Won-Yong, Chung Sae-Young, Lee Yong H., *Improved Power-Delay Trade-off in Wireless Ad Hoc Networks Using Opportunistic Routing*, Information Theory, 2007. ISIT 2007. IEEE International Symposium on, PP. 841-845, ISBN 978-1-4244-1397-3, Nice, France, June 2007.

[74] Silva R.M.S., Pereira N.S.A., *Applicability Drawbacks of Probabilistic Key Management Schemes for Real World Applications of Wireless Sensor Networks*, Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, pp.51–58, ISBN 0-7695-2796-5, Guadeloupe, French Caribbean, March 2007.

[75] Srivatsa M., Liu Ling , Iyengar A., *Preserving Caller Anonymity in Voice-over-IP Networks*, IEEE Symposium on Security and Privacy, 2008. SP 2008**,** pp. 50-63, ISSN 1081-6011, Oakland, California, USA, May 2008.

[76] Tao S., Xu K., Estepa A., Gao T.F.L., Guerin R., Kurose J., Towsley D., Zhang Z.-L., *Improving VoIP quality through path switching*, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, Volume 4, pp. 2268-2278, ISSN 0743-166X, Miami, Florida, USA; March 2005.

[77] Vaidya B., Choi D-Y., Park J., Han S., *Investigation of Secure Framework for Multipath MANET*, International Conference on Multimedia and Ubiquitous Engineering (mue 2008), pp.182-185, ISBN: 978-0-7695-3134-2, Busan, Korea, April, 2008.

[78] Wang K., Lin C., Liu F., *Quality of protection analysis and performance modeling in IP multimedia subsystem*, Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on, pp.234-239, ISBN 978-0-7695-3641-5, Shanghai, China, June 2009.

[79] Wei Liu, Wenjing Lou, Yuguang Fang, *An efficient quality of service routing algorithm for delay-sensitive applications,* The International Journal of Computer and Telecommunications Networking, Volume 47, Issue 1, pp. 87-104, ISSN 1389-1286, Elsevier North-Holland, Inc. New York, NY, USA, January 2005.

[80] Wilhelm M., Martinovic I., Schmitt J.B., *On key agreement in wireless sensor networks based on radio transmission properties*, Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on, pp. 37-42, ISBN 978-1-4244-4866-1, Princeton, New Jersey, USA, October 2009.
[81] Wright C.V., Ballard L., Coull S.E., Monrose F., Masson G.M., *Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations*, IEEE Symposium on Security and Privacy 2008, SP 2008, pp. 35-49, ISSN 1081-6011, Oakland, California, USA, May 2008.
[82] Wu W., Nilanjan B., Kalyan B., Sajal K. D., *Network Assisted IP Mobility Support in Wireless LANs,* Second IEEE International Symposium on Network Computing and Applications, NCA 2003, pp.257-264, ISBN: 0-7695-1938-5, Cambridge, Massachusetts, USA, May 2003
[83] Yaghmaee M.H., Adjeroh D., *New priority based congestion control protocol for Wireless Multimedia Sensor Networks*, World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008, International Symposium on, pp. 1-8, ISBN: 978-1-4244-2099-5, Newport Beach, California, USA, June 2008.
[84] Zahran A.H., Liang B, Saleh A., *Mobility Modeling and Performance Evaluation of Heterogeneous Wireless Networks*, IEEE Transactions on Mobile Computing, Volume 7, Issue 8, pp.1041-1056, ISSN 1536-1233, August 2008.

ANEXA-ARTICOLE PERSONALE PUBLICATE ŞI CITATE ÎN TEZĂ

PSU-UNS
4th INTERNATIONAL CONFERENCE ON ENGINEERING TECHNOLOGIES - ICET 2009
Novi Sad, April 28-30, 2009

OPTIMIZATION OF SIP SESSION SETUP DELAY FOR VOIP IN 3G WIRELESS NETWORKS

Mirela Ioanesiu [1*], Corneliu Toma [2*]
Politehnica" University of Timisoara, Faculty of Electronics and Telecommunications, Timisoara, Romania
[2]"Politehnica" University of Timisoara, Faculty of Electronics and Telecommunications, Timisoara, Romania
*Contact person: ioanesium@yahoo.com
*Contact person: corneliu.toma@etc.upt.ro

Abstract: *Wireless networks beyond 2G aim at supporting real- time applications such as VoIP. This paper focuses on SIP session setup delay and proposes optimizing it using an adaptive retransmission timer. It also evaluates SIP session setup performances with various underlying protocols such as TCP, UDP, and RLP. For 19.2 Kbps channel, the SIP session setup time can be up to 6.12 s with UDP and 7 s with TCP when the FER is up to 10 percent .It also compares SIP and H.323 performances using an adaptive retransmission timer: SIP outperforms H.323, especially for a FER higher than 2 percent.*

Key Words: IP-based wireless networks / SIP / Session setup delay / TCP / UDP / RLP / H.323.

1. Introduction

Internet Protocol (IP) based networks have become ubiquitous in recent years. The IP multimedia subsystem (IMS) has been adopted by 3GPP for Universal Mobile Telecommunication System (UMTS). Unlike the fix lines, the wireless access network is highly erroneous due to fading, shadowing, and even intermittent disconnections. This may result in a frame error rate (FER) as high as 10 percent [3]. To cope with such a high FER in CDMA 2000, the data link control (DLC) layer of wireless access networks includes, along with the medium access control (MAC) and logical link control (LLC), a radio link protocol (RLP) sub layer. RLP can work in two modes: transparent and nontransparent. In nontransparent mode, the purpose of RLP [4] is to provide extra reliability to the Layer 2 on top of LLC. LLC was primarily designed for wire line access networks, experiencing much less data losses. In transparent mode, RLP does not provide extra reliability. In the GSM system, the voice traffic is circuit-switched with the help of the signaling system 7 (SS7). On the other hand, two different signaling schemes were evolved for VoIP services. The first one is H.323, specified by International Telecommunication Union standardization group (ITU-T), for the implementation of multimedia services over packet-based networks. The other one, adopted in the IMS domain is the Session Initiation Protocol (SIP), developed by the Internet Engineering Task Force (IETF), "SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls" [5]. Unlike H.323, SIP is specifically defined for the Internet.

While VoIP quality has been extensively studied in [6] and [7], session setup time for VoIP has received relatively less attention. The session setup time has a direct impact on the users' satisfaction. The user is used to waiting a maximum of 11 s as specified in [8] and expects to experience the same even if the technology is different. In [9], the session setup delay over public Internet is evaluated for H.323 and SIP using simulations. Kist and Harris in [10] investigate, through simulations, the SIP session initiation delay in the 3GPP context. In an important study [3], the performance of H.323 is evaluated in terms of average call setup delay, considering the RLP (1, 2, 3) scheme. This is the motivation behind this paper. Here, it was considered SIP as the signaling protocol enabling VoIP and is investigated its performance in a wireless model similar to that suggested in [3], [11] and [12]. In this paper, only one type of media (speech)

is considered, therefore, there is no need to use RTCP with SIP.

2. Overview of SIP Protocol in IMS

The basic architecture of SIP is based on a client - server model. In IMS, the SIP functions are located in the IMS domain. These main functions of SIP in IMS are various SIP servers which are called call session control functions (CSCF) and gateways. A user agent, or SIP endpoint, is usually identified using an e - mail like address: user@domain.

1.1. SIP Protocol Stack

SIP works together with the session description protocol (SDP) which is in charge of describing the session to be opened. SIP messages can be carried by UDP or TCP. When SIP is carried by TCP, the transport layer provides reliability. When SIP is carried by UDP, the reliable delivery procedures are ensured by SIP. UDP is the widespread SIP transport protocol [5].

1.2. SIP Session Establishment in IMS

SIP is a transactional protocol in the sense that a SIP transaction consists of a single request and any responses to that request. The establishment of a session using SIP consists of various transactions. Fig. 1. illustrates the session setup between two user agents.

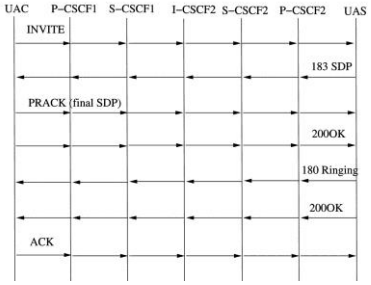


Fig.1. SIP Session Setup

To ensure the reliable delivery of the SIP requests and responses involved in the various transactions, retransmission mechanisms are needed at the user agent client and the user agent server. The client-side transaction consists of sending an INVITE request and receiving the 183 response. The UAC is aware of the successful transmission of the INVITE request as soon as it receives the 183 response. If SIP messages are carried over UDP, the UAC retransmits the INVITE request after an interval that lasts *Tr (1)* seconds and doubles after each retransmission. The SIP timer *Tr (1)* is an estimate of the round-trip time and its default value is 500 ms, but it is recommended to be larger in case of high latency access links [5]. The retransmissions cease upon the re-ception of a 183 response at the user agent client or after seven transmissions of the INVITE request. For reliable transport protocols such as TCP, there is no retransmission me-chanism at the application layer; this is han-dled by the transport layer. Each end has to acknowledge the data it receives from the other end. But, data segments and acknow-ledgments can get lost. TCP handles this by setting a timer when it sends data and, if the data is not acknowledged when the timer ex-pires, it retransmits the data [6]. The default value for the first TCP retransmission timer is usually 1-1,5 seconds [16]. But any type of transport protocol, the retransmission of re-quests cease when the timer reaches $2^6*Tr(1)$ seconds. The server-side transaction consists of the UAS sending, for instance, the 200 OK response and receiving an ACK. The UAS is aware of the successful transmission of the 200 OK at the beginning of the call when it receives the ACK. The retransmission mecha-nism is identical to the one on the client side for reliable and unreliable transport protocols.

3. Session Setup Delay

Several delays are considered to assess the quality of service of signaling protocols. This paper investigates the session setup delay defined as the period between the instant the user agent client triggers the session initiation with an INVITE request and the instant the user agent server has been alerted that the client received the server's agreement upon the session (reception of ACK request at the user agent server). The session setup delay depends on a number of factors. The most obvious factors are: the transmission delay over the network, which may experience losses, and the queuing delays. This transmission delay can be affected by the transport protocols used and their error recovery strategies.

3.1 Transport Protocols

If SIP is used over UDP, only the simple exchange illustrated in Fig. 1. is needed to set up the VoIP session. Retransmissions are ensured by SIP using an exponential back off timer. Therefore, the total session setup delay for SIP over UDP is the time needed for all messages involved in the various transactions to be successfully received by the UAC and the UAS.

If SIP is used over TCP, the TCP connection should first be established by the exchange of SYN/SYN–ACK/ACK messages. Then, the SIP messages are exchanged as illustrated in Fig. 2.

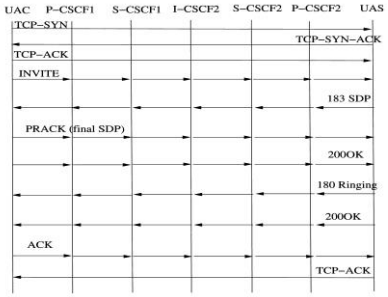


Fig.2. Session setup of SIP over TCP

The total session setup delay for SIP over TCP is the addition of the setup time of the TCP session and the successful transmission time of all the SIP messages necessary to establish a VoIP session.

3.2 Radio Link Protocols

The use of SIP over RLP can reduce the effect of FER on the session setup time and can increase the reliability over the wireless link RLP. When the RLP receiver finds a frame in error or missing, it sends back a NAK requesting the retransmission of the erroneous frame. NAKs are sent in the next radio frame (time slot) after reception of the erroneous frame. At the sender, each NAK received correctly triggers the retransmission of the frame requested in the NAK. This retransmission is done in the next radio frame after the reception of the NAK. This is illustrated in Fig. 3.

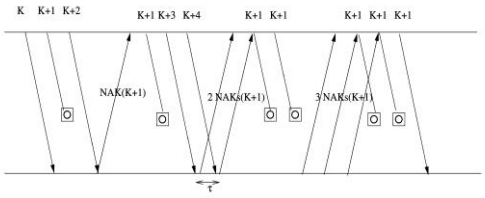


Fig.3. The RLP scheme (1,2,3)

RLP classifies RLP frames into three priority classes. These are: RLP control frames (such as NAK), retransmitted data frames and new data frames
In RLP, the number of NAK rounds and the number of NAKs sent in a round can be chosen to optimize the delay performance. In this paper, it is investigated RLP (1, 2, 3) and RLP (1, 1, 1, 1, 1, 1). The total number of retransmissions for the two schemes is the same (i.e., six) with the difference that (1, 2, 3) performs six retransmissions in three rounds while (1, 1, 1, 1, 1, 1) achieves this in six rounds of NAKs. For detailed information on RLP, refer to [4].

4. Performance Analysis of SIP Signaling over Wireless Links

For the analysis, it is considered a simple session setup messages flow of SIP as depicted in Fig.1. for UDP and Fig.2. for TCP. The following assumptions are made about the end-to-end SIP session:

- TCP is assumed to operate in an interactive mode;
- The delayed acknowledgment mode of TCP is turned off;
- TCP always times out when a packet is lost: A user agent client after transmitting an SIP message (e.g., INVITE) waits for its acknowledgment (e.g., 200 OK) before transmitting the next SIP message (e.g., ACK).

4.1 Transmission Delay for SIP over UDP

The SIP back off timer after the i_{th} transmission Tr(i) doubles after each retrans-mission. Hence:

$$Tr(i) = 2^{i-1} \cdot Tr(1) \qquad (1)$$

The initial retransmission timer *Tr(1)* is a crucial parameter which should be optimized since it has a direct impact on the session setup delay. It should not be too short, otherwise the packet is transmitted while a response is on the way to be received, and it should not be too long to avoid increasing the session setup unnecessarily if a loss occurs. Therefore, it has to be proportional to the transmission time of the messages involved in the transaction. It is function of the number of frames *k* contained in the UDP datagram, of the end-to-end frame propagation delay *D* and of the inter frame time *r*, the time interval between the transmissions of two consecutive frames. Let us consider the client-side transaction: transmission of the INVITE request (containing k_1 frames), acknowledged by the 183 response (containing k_2 frames). Hence, the adaptive retransmission timer of the client-side tran-saction proposed in this paper is:

$$Tr(1) = D + (k_1 - 1)\cdot\tau + D + (k_2 - 1)\cdot\tau + D_{elay_{queuing/Processing}} \qquad (2)$$

4.1.1 Transmission Delay without RLP

Let *p* be the probability of a frame being erroneous in the air link. There for, *(l-p)* is the probability of a frame not being in error in the air link. With *k* frames contained in one UDP packet, $((1-p)^k)$ is the probability that the UDP packet is not erroneous. Hence, the packet loss rate is $(1-(1-p)^k)$. The probability of retransmission *q* is the probability of a transaction having failed: This means that the first pac-

ket sent (INVITE request containing k_1 frames) is lost or that the first packet is received but the response (183 containing k_2 frames) is lost. Therefore, the probability of having a retransmission of invite during a client-side transaction is:

$$q = 1 - \left((1-p)^{k_1 + k_2} \right) \quad (3)$$

For the server-side transaction, the value of q is changing; reflecting the number of frames contained in 200 OK (k_2) and ACK (k_1). (for SIP, it is the i_{th} UDP). Let N_m be the maximum number of transmissions (for SIP, it is fixed to $N_m = 7$). The average delay for a successful transaction is the average delay for successfully transmitting a UDP datagram containing an SIP message and successfully receiving the corresponding acknowledgment. This is because the sender (e.g., UAC) knows that the sending packet (e.g., INVITE) has successfully been received when it receives an "acknowledgment"

Therefore, the total transmission delay for setting up the session is the addition of the delays for transmitting all the N messages necessary to set up a VoIP session using SIP over UDP. The average session setup delay Tt_{UDP} is given as:

$$Tt_{UDP} = \sum_{i=1}^{N} Tt(i)_{UDP} \quad (4)$$

4.1.2 Transmission with RLP(1, 2, 3)

RLP protocol is performing retransmissions at the frame level. In the first retransmission trial, one NAK is sent to the endpoint which triggers a retransmission of the missing frame. In the second trial, two NAKs are sent and each NAK triggers the retransmission of the missing frame. Finally, in the third trial, three NAKs are sent triggering three consecutive retransmissions of the same missing frame. For this analysis, similar to [3], the following terms need to be defined:

X_{ij} = i_{th} retransmission frame at the j_{th} retransmission trial, received correctly at the destination.

Y_{ij} = i_{th} NAK frame at the j_{th} retransmission trial,received correctly at the source.

C_{ij} = the first frame received correctly at the destina-tion, which is the i_{th} retransmission frame at the j_{th} retransmission trial. These frames are independent one from each other.

$$P(X_{ij}) = P(Y_{ij}) = 1 - p, \quad (5)$$

where p is the FER. Therefore, if a frame is not received correctly at the j_{th} retransmission comprising, the j_{th} trial are lost, and then:

$$P(A^j) = ((2-p)p)^j \quad (6)$$

If the frame is aborted after the n_{th} retransmission trial, it means that the frame is not received correctly up to the end of the n_{th} retransmission trial; this is expressed in the following terms:

$$P(B_n) = p((2-p)p)^{\frac{n(n+1)}{2}} \quad (7)$$

And, if the first frame received corresponds to the i_{th} retransmitted frame of the $(j-1)_{th}$ trial, it means that the missing frame has been lost up to the j_{th} retransmission trial and up to the $(i-1)_{th}$ retransmissions in the j_{th} trial.

$$P(C_{ij}) = p \cdot (1-p)^2 ((2-p)p)^{\frac{j(j-1)}{2}+i+1} \quad (8)$$

Therefore, the probability of transmitting a frame successfully over the RLC layer is given by:

$$Pf = 1 - P(B_n) = 1 - p((2-p)p)^{\frac{n(n+1)}{2}} \quad (9)$$

4.1.3 Transmission Delay with RLP (1, 1, 1, 1, 1, 1)

RLP (1, 1, 1, 1, 1, 1) performs six retransmission trials and each trial involves one NAK triggering, one retransmission. It was assumed that:

$$P(X_{ij}) = P(Y_{ij}) = 1 - p \quad (10)$$

where p is the FER. The probability that a frame is not received correctly at the j_{th} retransmission trial is:

$$P(A_j) = ((2-p)p)^j \quad (11)$$

The probability that a frame is aborted after the n_{th} retransmission trial is expressed in the following terms:

$$P(B_n) = p((2-p)p)^{\frac{n(n+1)}{2}} \quad (12)$$

And if the first frame received corresponds to the retransmitted frame of the j_{th} trail:

$$P(C_{ij}) = p(1-p)^2 \cdot ((2-p) \cdot p)^{\frac{j(j+1)}{2}+i-1} \quad (13)$$

Therefore the probability of transmitting a frame successfully over the RLC layer is given by

$$Pf = 1 - P(B_n) = 1 - p \cdot ((2-p) \cdot p)^{\frac{n(n+1)}{2}} \quad (14)$$

4.1.3 Transmission Delay SIP over TCP

In this paper, is used an adaptive timer similar to the one used by SIP over UDP:

$$Tr(1) = 2D + (K_1 - 1) \cdot \tau + (K_2 - 1) \cdot \tau + Delay_{Queuing/Processing} \quad (15)$$

K_1 is the number of frames contained in the data packet and K_2 is the number of frames contained in the TCP acknowledgment piggyback with the data to be sent by the receiver (e.g., 183). For TCP, the SIP user agent follows TCP specifications to retransmit messa-

ges until an acknowledgment is received. The total session setup delay is

$$Tt_{TCP} = \sum_{i=1}^{N} Tt(i)_{TCP} \qquad (16)$$

In the transmission of SIP messages appears also the Internet delay, which is part of the total session setup delay. The delay introduced by the Internet depends on the number of routers and the type of links in the path of datagram transmission.

5. Numerical Results

This section presents the results of the average session setup delay for SIP over transport and radio link protocols. The number and the size of the messages exchanged affect the average session setup delay. The reduction of these factors leads to a shorter session setup delay. For the evaluation, the approximate size for each SIP message is obtained from packets captured by the protocol analyzer Ethereal [17] in the experimental test bed. The number of frames is needed in each case and it was taken into consideration two types of channel: 9.6 Kbps and 19.2 Kbps. The duration of each radio frame is assumed to 20 ms, which corresponds to 24 bytes in a 9.6 Kbps channel and 48 bytes in a 19.2 Kbps channel. The values of the delay D and the inter frame time τ are set as in [3], respectively, 100 ms and 20 ms. For SIP over TCP and UDP, the maximum number of transmissions N_m is set to seven.
The total average session setup delay using the adaptive retransmission timer is computed for both channels and is shown in Fig. 4.

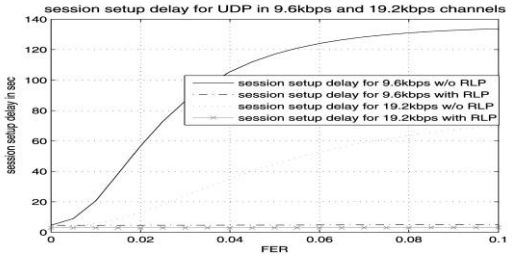


Fig. 4. Average session setup delay in 9.6 Kbps and 19.2 Kbps channels for SIP over UDP with / without RLP (1,2,3).

The average session setup delay is evaluated at various FER between 0-10 percent. However, the session is established for VoIP. Voice services are supported if the FER is between 1 percent and 3 percent. Results for 1 percent FER are presented in Table 1.
The results show that the SIP session delay is compliant with ITU-T recommendation [8] if RLP is used or the bandwidth is as high as 19.2 Kbps. Fig.4 shows that, if the bandwidth of the channel doubles, the session setup delay is reduced by 20 percent to 58 percent (39 percent in average). The proportion of the session setup delay that is due to the queuing is relatively small: 0.6136 s for SIP over UDP for both channels.

Table 1. Comparison UDP versus TCP, for FER = 1 percet

Protocols	Session setup delay (s) for 9.6 Kbps	Session setup delay (s) for 19.2 Kbps
UDP w/o RLP	20.65	5.6
UDP with RLP(1,2,3)	4.61	2.9
UDP with RLP (1,1,1,1,1,1)	4.61	2.9
TCP w/o RLP	23.8	6.9
TCP with RLP(1,2,3)	5.9	3.9
TCP with RLP(1,1,1,1,1,1)	5.9	3.9

5.1 Relevance of Adaptive Timer

The retransmission mechanisms specified for SIP over UDP and for TCP follow an exponential function of the initial timer. The retransmission timer doubles after each retransmission. It is therefore very important to consider a relevant initial value of the timer.

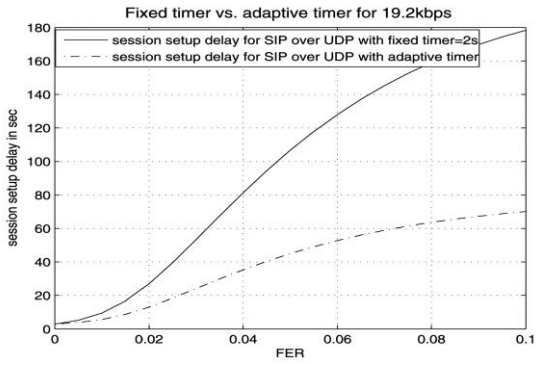


Fig. 5. Comparison of the average session setup delay in 19.2 Kbps channels for SIP over UDP with fixed timer 2 s.

Fig. 5. shows the result from comparing the session setup delay with a fixed timer of 2 s and the adaptive timer. The adaptive timer makes the session setup delay 70 to 40 percent shorter (46 percent on average). The use of the adaptive timer is very relevant to minimize the delay cost of any transmission in general and of the session setup in particular as the latter directly affects user satisfaction.
Fig. 6. illustrates the average session setup delay for the two channels. The doubling of the bandwidth of the channel reduces the session setup delay from 20 percent to 70 percent (37

percent in average). The proportion of the session setup delay that is due to the queuing is higher than for UDP: 1.0227 s for both channels. This is due to the higher number of messages involved in the session setup with TCP and their bigger size.

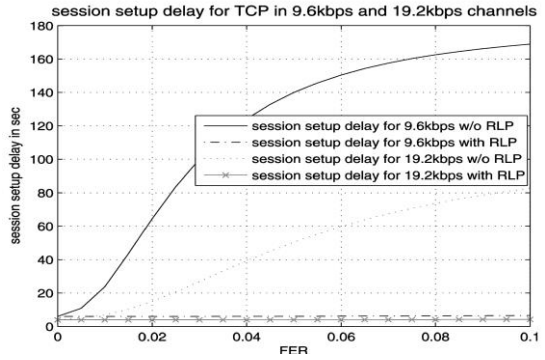


Fig. 6. Average session setup delay in 9.6 Kbps and 19.2 Kbps channels for SIP over TCP with / without RLP.

Fig. 7. shows that if the FER is less than 2 percent the session setup delay of SIP over TCP is slightly equal to the one over UDP. This is due to the use of the adaptive timer because the adaptive timer adjusts to the size of the messages involved in the setup, and TCP sends relatively small messages for the TCP connection setup.

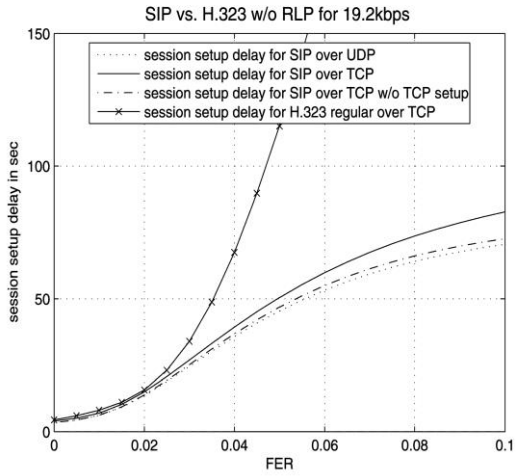


Fig.7. SIP versus H.323 for SIP session setup delay in 19.2 kbps channel with adaptive timer

5. Conclusion

H.323 is the concurrent of SIP for establishing VoIP sessions. In this paper were compared both protocols using the adaptive retransmission timer and the FER model described previously. H.323 messages are carried over TCP and IP. The size of the H.323 messages needed to compute the session setup delay is taken from [3]. The calculations are made for the regular H.323 session setup. The maximum number of retransmissions is 10. The H.323 session setup delay is as long as the SIP one for an FER less than 2 percent. But, for FER higher than 2 percent, SIP outperforms H.323. Such results are due to the adaptive timer used for H.323 session establishment that consists of 19 messages smaller than SIP ones. Moreover, the H.323 session setup time grows exponentially because 10 retransmissions are allowed while seven retransmissions for SIP. This comparison shows the considerable influence of the timer and of the maximum number of retrans-missions allowed on the delay performances of the signaling protocol.
Therefore, to optimize further the SIP session setup delay, some compression schemes could be employed such as Signaling Compression (Sig Comp) [18] or the Text-Based Compression using Cache and Blank approach (TCCB) [19]. TCCB can compress up to 30-50 percent of the size of most of the SIP messages by removing redundant header and payload information, but the initial INVITE request can only be compressed to about 9 percent [19]. The number of users can affect the session setup delay in many different ways: user admission in a cell and availability of the SIP servers. In this paper, the avai-lability of the servers was related to their load and the SIP message arrival rate.
The work was focused on a proposal of a novel adaptive transmission timer that is adjustable to the size of signaling packets involved in the session establishment. Using an analytical model, it was evaluated the average SIP session setup depending on the FER of the wireless link and the processing power of the servers and source / destination terminals (queuing delays). The choice of UDP or TCP to transport SIP messages influences the session setup time for FER higher than 2 percent. To use UDP instead of TCP can make the session setup 10 percent shorter for FERs higher than 4 percent. Low-layer retransmission mecha-nisms, such as RLP, considerably improve the session setup delay. Therefore, the adaptive timer is efficient for optimizing the perfor-mance of signaling protocols in general. The performance of SIP using the adaptive timer could be improved by using some compression schemes to reduce the size of the SIP mes-sages.
Also, error correction mechanisms or hybrid ARQ schemes could improve the performance of VoIP session setup time by correcting the SIP messages and avoiding retransmissions on the wireless link.

6. References

[1] Black, Voice over IP. Prentice Hall, 2000.

[2] 3GPP, "Technical Specification Group Services and System Aspects; Network Architecture (Release 5)," Technical Report TS23.002, GPP, Mar. 2002.
[3] S. Das, E. Lee, K. Basu, and S. Sen, "Performance Optimization of VoIP Calls over Wireless Links Using H.323 Protocol," IEEE Trans. Computers, vol. 52, no. 6, pp. 742-752, June 2003.
[4] 3GPP2, "Data Service Options For Spread Spectrum Systems: Radio Link Protocol Type 3," Technical Report C.S0017–010-A, June 2004.
[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Proto col,"RFC 3261 IETF, June 2002.
[6] B. Goode, "Voice over Internet Protocol (VoIP)," Proc. IEEE, vol. 90, no. 9, 2002.
[7] Valko , A. Racz , and G. Fodor, "VoIP QoS in Third - Generation Mobile Systems," IEEE J. Selected Areas in Comm , vol. 17 , no. 1, Jan. 1999.
[8] T.S.S. of ITU, "ITU-T Recommendation E. 721-Network Grade of Service Parameters and Target Values for Circuit-Switched Services in the Evolving ISDN," 1991.
[9] T. Eyers and H. Schulzrinne, "Predic-ting Internet Telephony Call Setup Delay," Proc. First IP Telephony Workshop, Apr. 2000.
[10] Kist and R.J. Harris, "SIP Signaling Delay in GPP," Proc. Sixth Int'l Symp. Comm. Interworking, pp. 211-222, 2002.
[11] J. Harris and M. Airy, "Analytical Model for Radio Link Protocol for IS - 95 CDMA Systems," Proc. IEEE Vehicular Technology Conf., vol. 3, pp. 2434 - 2438, 2000.
[12] G. Bao, "Performance Evaluation of TCP/RLP Protocol Stack over CDMA Wireless Link," IEEE Wireless Net-works, vol. 3, no. 2, pp. 229 - 237, 1996.
[13] Hersent, D. Gurle, and J. Petit, IP Teleph ony, Packet-Based Multimedia Communications Systems. Addison-Wesley, 2000.
[14] F. Khan, S. Kumar, K. Medepalli and S.Nanda, "TCP Performance over CDMA 2000 RLP," Proc. IEEE Vehicular Technology Conf., pp. 41-45, 2000.
[15] L. Kleinrock, Queuing Systems, Vol. 1: The Theory. Wiley, 1975.
[16] R. Stevens, TCP / IP Illustrated vol. 1. Addison-Wesley, 1994.
[17] Ethereal,http://www.ethereal.com/,2006.
[18] R. Price et al. "Signaling Compression," RFC 3320, Jan. 2003.
[19] IETF, "Text-Based Compression Using Cache and Blank Approach," Internet Draft, July 2001.
[20] G.Foster, M.I.Pous, D.Pesch, A.Sesmun and V.Kenneally, "Performance Estimation of Efficient UMTS Packet Voice Call Control, Proc. IEEE Vehicular Technology Conf., vol. 3, pp. 1447-1451, Sept. 2002.

Support of voice services in IEEE 802.11 wireless LANs

[1]"Politehnica" University of Timisoara, Faculty of Electronics and Telecommunications, Timisoara, Romania
[2]"Politehnica" University of Timisoara, Faculty of Electronics and Telecommunications, Timisoara, Romania
*Contact person: ioanesium@yahoo.com
*Contact person: corneliu.toma@etc.upt.ro

Mirela Ioanesiu 1*, Corneliu Toma

Abstract: *The IEEE 802.11 MAC protocol supports two modes of operation, a random access mode and a polling mode. The problem investigated in is paper is the use of the polling mode for interactive voice traffic. For larger inter - poll periods and more voice calls, the delay will increase. The analysis shows that with an inter - poll period of 90 ms, 26 voice calls the delay is 303 ms. With an inter - poll period of 60 ms and 17 voice calls the delay is 213 ms .This paper present also an error analysis that demonstrates the need for error correction of voice packets.*
Key Words: VoIP /Real Time Application /DCF /PCF /AP / CP

1.Introduction

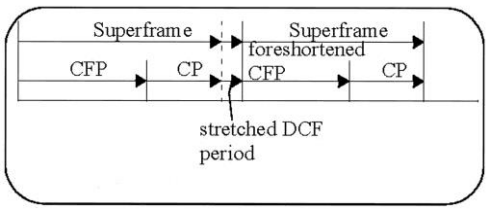
The IEEE 802.11 wireless LAN [1] is gaining popularity for data applications in campus networks, such as in university campuses and airports. Data rates of these indoor wireless LANs are in the order of 11 Mbps, which is considerably higher than outdoor wireless data services offered through cellular base stations. Most commercial available offers implement only the 802.11 mode of operation that supports data services called the Distributed Coordination Function (DCF) mode and not the second 802.11 mode of operation, designed for real - time services, called the Point Coordination Function (PCF) mode.
The problem statement of this work is to determine whether the 802.11 PCF mode is suitable for supporting interactive voice services. For this mode of operation it was used a polling scheme to provide resource guarantees for real - time sessions. Therefore, more generally, the results of this are appli-cable to any polling-based scheme.
The motivation for this paper comes from an observation that the PCF mode offers a "packet-switched connection-oriented" service, which is well suited for telephony traffic. Telephony traffic has been shown to have alternating periods of talk spurts and silences [2], [3]. Packet-switched solutions that take advantage of silences in a given voice call by multiplexing voice data from other calls are more bandwidth-efficient than circuit-switched solutions.

1.1 Description

An 802.11 LAN can be operated in an ad hoc configuration, without an Access Point (AP), or in an infrastructure configuration, with an AP. The AP serves as a MAC layer bridge between wireless stations as well as between wireless and wired stations. The 802.11 standard specifies a MAC protocol (with the DCF and PCF modes) and three physical layer options: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infra Red (IR). The main focus of this work is on the MAC sub layer and particularly the PCF.
The DCF mode is the fundamental access method of the 802.11 MAC sub layer and is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA). The time period during which the LAN operates in the DCF mode is known as the Contention Period

(CP). Access priority to the medium is controlled through the use of Inter Frame Spaces (IFS), the time interval between frames. There are three types of inter frame spaces: the Short IFS (SIFS), the Point Coordination Function IFS (PIFS) and the Distributed Coordination Function (DIFS). The SIFS is the shortest interval and is used for transmission of acknowledgements, stations responding to polls from the point coordinator (usually the AP) during the PCF mode, and between fragments if an MAC Service Data Unit (MSDU) is fragmented. Transmissions required waiting only SIFS intervals have the highest priority over the medium. The AP uses the PIFS for example, to initiate the CFP. The DIFS is used by stations during the CP. Transmissions required to wait a DIFS interval, have the lowest access priority to the medium. The PCF mode provides contention free frame transfer. The time period in which the LAN operates in the PCF mode is known as the Contention - Free Period (CFP). The AP performs the function of the point coordinator by gaining control of the medium at the beginning of the CFP after sensing the medium to be idle for a PIFS period. During the CFP, stations that are CF - Poll able (can respond to polls), are polled by the AP. On receiving a poll the station transmits its data after a SIFS interval. In order to poll the stations, an AP must maintain a polling list, which is implementation dependent. The CFP must alternate with the CP. The sum of the two periods is called the "super frame" and is shown in Fig. 1. It may happen that a station begins to transmit a frame just before the end of the CP, hence elongating the current super frame and shortening the next CFP as shown in Fig. 1:

Fig.1. Timing diagram



The elongation of current super frame and shortening the next CFP is known as stretching. To understand the effect of stretching on the CFP, one should allow for an MSDU of maximum size (which is 2304 bytes) to be sent right before the end of the super frame. If the Fragmentation Threshold (a management - settable parameter) is not equal to this maximum size, then additional overhead will be incurred due to the fragmentation of the MSDU. All fragments of an MSDU are sent SIFS intervals, which mean, that, the AP, in waiting for a PIFS interval to initiate the CFP, cannot acquire the medium between fragment transmissions. Thus, in the worst case, the stretching period could be as large as is needed to send a 2304 byte payload with fragmentation.

The AP initiates the CFP by transmitting a Beacon frame. If the traffic during the CFP is light and / or the AP has completed polling all the stations on the polling list, it can end the CFP by transmitting a CF-End frame. The contention - free repetition interval (CFP Period) is the reciprocal of the rate at which the AP initiates the CFP. The AP then takes control of the medium and starts polling the stations on its polling list. Retransmissions are used in 802.11 for error correction both in the DCF and PCF modes. To support error correction, positive acknowledgments (ACKs) are used. An ACK for a frame is piggybacked on the next frame even if the latter is not destined to the same station as the sender of the previous frame. There is no mechanism to turn off retransmissions in the PCF mode, or to use different retry counts in the PCF and DCF modes. Beacons are generated periodically according to the beacon interval. Mobile stations awaken at listen intervals (which are multiples of beacon intervals) to hear beacons. A beacon is sent at the start of a CFP, but if the CFP duration is larger than the beacon interval, then multiple beacons will be sent during a CFP. The CFP MaxDuration is also settable and indicated in beacons. For beacons that arrive in the middle of a CFP, the CFP Remaining Duration indicates how long is left in the CFP. Thus, if a mobile station sleeps and awakens on its listen intervals that may not coincide with the start of a CFP, it can still determine the time left in the CFP.

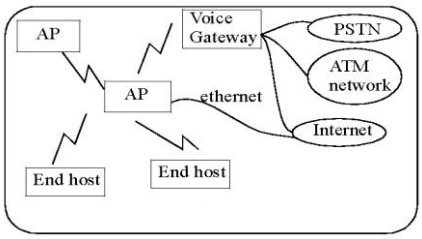
2. Proposed Solution

This section describes design choices made to carry interactive voice traffic in the PCF mode. The solution consists of describing the architectural design, defining the user actions to send voice data and control plane actions, such as Connection Admission Control (CAC) in order to admit only a limited number of users into the polling list, and setting Management Information Base (MIB) variables.

2.1. Architectural assumption

Given the motivation to enable voice calls to be made from 802.11 users to wired, cellular, or Internet telephones, the network architecture proposed is shown in Fig. 2.

Fig.2. Network architecture



Access points currently have only two interfaces, an 802.11 interface and an Ethernet interface. The Ethernet interface supports data traffic sent via the DCF mode from mobile stations to the APs. On the other hand, because Ethernet does not provide differential Quality of Service (Q o S) support, it is not suitable for real - time traffic. As a matter of fact, the PCF mode of 802.11 could itself be used from the AP to a voice gateway (see Fig.2.), with the voice gateway supporting interfaces to the PSTN, ATM network (for voice over ATM) and to the Internet (for voice over IP). The voice gateway converts the 802.11 voice protocol stacks to PCM voice for use on the PSTN voice over an ATM Adaptation Layer (AAL) for ATM networks or voice over Real - time Transport Protocol (RTP) / UDP / IP for IP networks. This architecture allows for end – to - end delay guarantees given that both PSTN and ATM networks are connection oriented. Voice packets are carried on 802.11 in two modes of operation: Constant Bit Rate (CBR) mode in which calls are allocated their peak rate and Variable Bit Rate (VBR) mode, in which statistical multiplexing is used and silences in voice calls are used by other voice calls or data traffic. For both modes, the super frame length is fixed. The maximum number of calls that can be admitted is determined by the super frame length. Varying the super frame length would impact delay variations of admitted calls and hence this is avoided. Interestingly, it is possible to change the super frame length because beacons carry a parameter indicating the super frame length. The error analysis for voice shows that some form of error correction is needed. There are three options: forward error correction (FEC), retransmission and delivering error packets to the signal processor.

2.2. Computation of the maximum number of voice calls

This section focuses on computing the maximum number of voice calls for the two modes of operation, CBR and VBR. In the CBR mode, to determine how much time to allocate per call, is necessary to determine the maximum size of voice packets. The maximum time in this mode is T_{SF} seconds. Add to this $P_{min} = 30\ ms$, to capture the possibility that a voice packet completes just after a poll. Thus, the largest voice packet size created will be c (P_{min} + T_{SF}) bits long. Given that in CBR mode, this time is allocated to each voice call whether or not it generates a packet. To determine the maximum number of calls, it is necessary to find the minimum duration of the CP and then use T_{SF} minus this minimum duration for the CFP. $T_{cp\text{-}min}$ includes the time to minimally send one frame as specified by Section 9.3.3.3 of [1]. All fragments and ACKs are sent with only SIFS intervals between them. Each fragment is acknowledged. T_{max} is the time to send a maximum - sized SDU. To accommodate the maximum number of calls,

$T_{cp} = T_{cp\text{-}min} + T_{cp\text{-}stretch}$, where (1)

$T_{cp\text{-}min} = 2T_{sifs}+2T_{slot}+8T_{ack}+T_{max}$ (2)

$T_{cp\text{-}stretch} = T_{rts} + 2T_{sisf} + T_{cts} + T_{max}$ (3)

Where $m = \left[\frac{S_{maxSDU}}{f} \right]$ (4)

and T_{last}

$$T_{last} = \frac{S_{maxSDU} - f(m-1) + h + P}{R} + T_{ack} + 2T_{sisf} \quad (5)$$

To compute the maximum number of voice calls that can be admitted, it will be divide the time left over for the CFP after allowing for a "stretched" CP. In the case of a stretched CP, the CFP is foreshortened and hence the number of beacons is $(T_{SF} - T_{cp})/T_b$. Thus, the maximum number of calls that can be admitted using the CBR mode is

$$Np = \frac{Tsf - Tcp - Tovhd}{Tv}, \text{ where} \quad (6)$$

$$T_{ovhd} = \left(\frac{B+P}{R} + T_{sisf} \right) \cdot \left[\frac{T_{sf} - T_{cp}}{Tb} \right] + \frac{CF_{end} + P}{R} \quad (7)$$

For the VBR mode of operation, it was computed the maximum number of calls for two voice models: Brady's model [2] and May and Zebo's [3]. Both of these models are ON - OFF Markov - Modulated Fluid (MMF) models, where in the ON state data is generated at the voice codec rate. The two models differ in the mean holding times of the two states as shown in table 1.

Tabel 1. Voice Models

Mode	Mean ON period	Mean OFF period	p
Brady's model [2]	1 sec	1.35 sec	0.43
May and Zebo model [3]	352ms	650ms	0.35

By admitting more calls than N_p it is statistically guaranteeing that loss will be less than some number ε. N_s is given by (8)

$$\frac{1}{2pN_S}\sum_{k=2N_p-1}^{2N_S}\left(k-2N_p\right)\binom{2N_S}{k}p^k(1-p)2^{N_S-k}\le\varepsilon \quad (8)$$

where p is the probability that a sending end is active. Equation (8) is based on the assumption that if a voice call is not polled in one super frame it is better to drop the packet rather than transmit it on the next super frame due to delay considerations.

2.3 Computation of bulid–out delay

As it was mentioned above, the CTI schemes for timing and RTP for transport were selected. A receiver uses a build - out delay when it reconstructs the voice signal. The build - out delay should be as small as possible. We first determine that the build - out delay should be the maximum possible delay difference between two packets.

Fig.3 Build-out delay

For example, assume the first packet took d_1 seconds, (which is unknown) and the total delay d from the start of packet to delivery at the receiver, is within the range $d_{min} \le d \le d_{max}$. How long should be this first packet hold at the receiver before play out? Let's say this is h as shown in Fig. 3. Thus the total delay experienced by the first packet is $d_1 + h$. If the second packet took $d_1 + y$ seconds (where y is known through the relative timestamp), then this packet should be delayed by $h - y$ seconds so that it experiences the same total delay $d_1 + h$ as the first packet, $h - y \ge 0$, which means the smallest value of h is equal to the maximum value of y. The maximum value of y is d_{max}-d_{min} and hence the build-out delay is set to the jitter. Even if $y < 0$, this result holds. In this section, will be determined jitter for voice packets of this solution. To determine jitter, it is necessary to identify how the two 802.11 ends of a voice call are placed on the polling list. For example, if a call, say A, has two ends Al and A2, Al is placed on the polling list immediately followed by A2. The Al to A2 packets experience short delays because on the A2 poll data received from Al can be delivered immediately. However the A2 to Al packets will experience a greater delay. In the CBR mode, all calls will have the same delay. The delay is computed in the two directions $k1$ —> $k2$, and $k2$ —> $k1$ assuming that the $k1$ end is placed on the polling list before the $k2$ end.

$$P_{min}+\frac{T_v}{2}\le D_{k1\to k2}\le P_{min}+T_{SF}+\frac{T_v}{2} \quad (9)$$

The best case is that a short packet is created in time P_{min} = *30 ms* and completes just before a poll arrives. Given the CBR mode of operation, even if the packet is short, the transmission time allocated for it and the response is T_v /2. Propagation delays are neglected since the radio link is short. The upper bound is determined by assuming that a poll just misses the creation of a voice packet (P_{min}) . The *k1 end then waits* T_{SF} for a poll (this includes the stretching period). On the next poll, when the *kl* end sends the packet, it is delivered immediately to the *k2* end. The transmission time is T_v /2. In the opposite direction, *k2* —> *k1* the delay will be larger. This delay is bounded by

$$P_{min}+T_{SF}-T_{CP-stretch}\le D_{k2\to k1}\le P_{min}+2T_{SF} \quad (10)$$

The lower bound is again determined assuming a small packet delay. Further, in the best case, there will be no stretching period; in which case, the time for the *k2* end is T_{SF} – $T_{cp\text{-}stretch}$. The *k1* end gets polled T_v /2 sooner than the *k2* end on the second poll. This means the time from when the *k2* end is polled to when the *k1* end is polled is $T_{SF} - T_{cp\text{-}stretch} - T_v$ /2. The transmission time adds T_v /2. The upper bound occurs when a poll just misses a packet (P_{min}). This is followed by a wait of T_{SF} for the next *k2* poll. This data then waits another T_{SF} - T_v /2 time to be delivered to the *k1* end on the next super frame. The transmission time is T_v /2. Given the jitter values (maximum delay – minimum delay) for the two directions of the voice call, the receiving end in each case, can be provided a reconstruction delay by the AP. Build - out delays used by the receiver during the transition will need to be managed by signaling. For the VBR mode of operation, delay computation is a lot more complex since if a voice call is silent, some other voice call or data packet can take advantage of the silence. This makes the period highly variable with a possibility of being larger than T_{SF} (unlike in the CBR case, where the inter poll period is a maximum of T_{SF}). Three factors control delay: value of T_{SF}, position of the call in the polling list and whether a call is polled multiple times per super frame, once every super frame, or once every multiple super frames. For calls to ATM / IP end - points, the 802.11 portion of the call from the wireless user to the AP of voice gateways needs to be kept small.

3. Numerical Results

In this section, will be determined numerical values for the various parameters described until now, the maximum call count used in the CAC algorithm at the AP and the total delay in the CBR mode .

Table 2 shows the values of certain parameters needed for MIB variable settings. These are determined for both the 2 Mbps and 11 Mbps date rates.

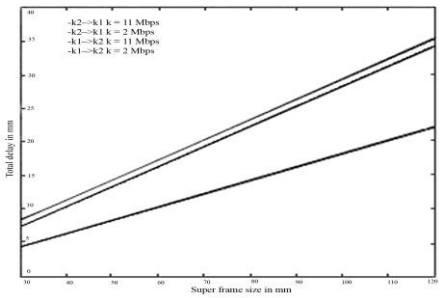
Table 2. Values in ms

Data rate (R) Mbps	$T_{cp\text{-}min}$	$T_{cp\text{-}stretch}$	$T_{SF\text{-}min}$
2	11,9	10.7	14.9
11	4,4	3,2	5,8

Fig. 4. shows the maximum number of voice calls that can be accommodated in the CBR mode for 2 Mbps and 11 Mbps at two values of the fragmentation threshold

Fig. 4. Maximum number of voice

For example, with a super frame size of 90 ms, 14 respectively 26 calls can be admitted on the 2 Mbps respectively 11 Mbps LANs. We note that the fragmentation threshold does not have a significant effect on the maximum number of voice calls that can be admitted with the relatively large fragment sizes used in Fig. 4. Table 3 compares the maximum number of calls admissible in the CBR mode (N_p) and VBR mode (N_s) using both Brady's and May and Zebo's voice mo-



dels for super frames of 75 ms and 90 ms. The conclusion is that a packet should be dropped if not served in a super frame holds.

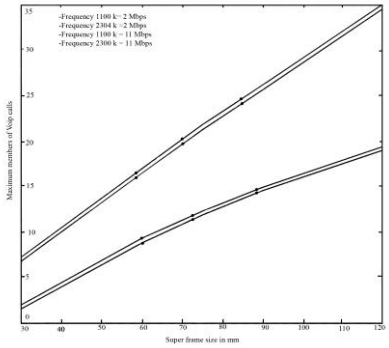
Table 3 Maximunm number of voice calls

T_{SF} (ms)	FH (2Mbps)			DS (11Mbps)		
	Np	Ns (B)	Ns(MZ)	Np	Ns (B)	Ns(MZ)
75	12	22	27	22	41	51
90	14	26	32	27	52	65

Since the VBR mode exploits silences, the maximum size of a voice packet is larger than $c\ (T_{SF} + P_{min})$. We also note that while the maximum number of calls that can be supported in the VBR mode is about double that can be supported in CBR mode, delays will be larger in the VBR mode. Delays for both directions *k1* → *k2* and *k2* → *kl* at both LAN rates, 2 Mbps and 11 Mbps, are shown in Fig.5

Fig.5. Total delay

For example if a super frame size of 90 ms is



used, then total delays of 121 and 303 msec will be experienced in the *kl* → *k2* and *k2* → *kl* directions, respectively, for the 802.11 portion of the voice call (on a 11 Mbps LAN).

4. Error Analysis

The 802.11 MAC protocol supports retransmission to handle transmission errors in both PCF and DCF modes. However, retransmissions are typically avoided for real-time traffic due to delay constrain. Here, will be examined whether or not some form of error correction is required for voice traffic.
This analysis takes into account two burst error models. Both are two-state continuous time Markov chains as shown in Fig. 5 [22].
The parameters for the models are given in Table 4.

Tabel 4 Parameters for burst error models

Model	BERG	BERB	α	λ
1	10^{-10}	10^{-5}	10/sec	30/sec
2	10^{-4}	10^{-2}	20/sec	10/sec

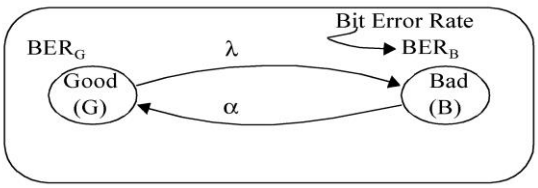


Fig.6. Model of a wireless channel

The first burst error model used to characterize fading is from [22], Fig.6. The second model is more realistic with higher BERs. The holding times are rough estimates. The time to transmit a voice packet of pay load size v bits is given by:

$$T_{v-pkt} = \frac{(v + h + P)}{R} \qquad (9)$$

Using the memory less property of the exponential distribution and by neglecting propagation delays, the probabilities of the three cases can be derived to be:

$$p_{case1} = p_G P(G > Tv - pkt) = \frac{\alpha}{\alpha+\lambda} e^{-\lambda Tv - pkt} \quad (10$$

$$p_{case2} = p_B P(B > Tv - pkt) = \frac{\alpha}{\alpha+\lambda} e^{-\lambda Tv - pkt} \quad (11)$$

$$p_{case3} = 1 - p_{case1} - p_{case2} \quad (12)$$

where p_G and p_B are the probabilities of starting a packet transmission when the channel is in the good or bad state and are given by:

$$p_G = \frac{\alpha}{\alpha+\lambda} \qquad p_B = \frac{\alpha}{\alpha+\lambda} \quad (13)$$

Combining the probabilities of the three cases, given by (10) to (12), with the probability of packet errors in the three cases, yields the total packet error probability as

$$p_e \le \begin{pmatrix} p_{case1}\varepsilon_{case1} + p_{case2}\varepsilon_{case2} \\ + p_{case3}\varepsilon_{case3} \end{pmatrix} \quad 14)$$

where a worst - case error rate is assumed if case 3 happens, that all bits are subject to BER_B

Fig.7. represents the upper bound of p_e plotted against T_{SF} for error models 1 and 2.

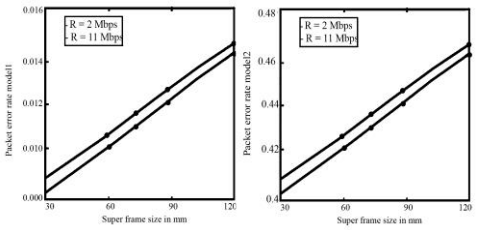


Fig.7. Packet error rates

The 11 Mbps network experiences a higher packet error rate even though the packet transmission time can be expected to be shorter owing to the higher data rate. This is because DS packets have a larger preamble than FH packets. For 90 ms T_{SF}, a packet error rate of approximately 10^{-2} and 0.44 for model 1 and model 2, respectively, are observed from the graphs. For voice, with a loss tolerance of 10^{-3}, these error rates are high. This shows a need for error correction. Errors can be handled in one or more of the three ways described in section 2.

5. Conclusions

In this paper was demonstrated that the PCF mode of the 802.11 MAC protocol (which uses a polling scheme) can indeed be used to carry telephony traffic. Using a connection admission control algorithm to control the number of voice calls admitted to the polling list, the network can provide delay guarantees. The simplest mode in which to run the LAN during the PCF operation is a Constant Bit Rate (CBR) mode. In this mode, if a voice user is silent, its time is not assigned to any other voice or data user. Ostensibly, this limits the number of calls that can be admitted, but in reality, by limiting delay jitter and hence the maximum delay, the CBR mode allows for a reasonable number of calls to be accommodated. For example, with a 11 Mbps 802.11 LAN, 26 voice calls can be admitted if the super frame size (sum of the polling and random - access periods) is 90 ms at a maximum delay of 303 ms. Also, in this mode, voice calls with different delay requirements (e.g., intra-LAN calls or calls to wired PSTN users vs. calls to Internet phones) can be accommodated by varying the number of times a call is placed on the polling list. Finally, it was carried out an error analysis that showed that voice packets can be expected to suffer a high packet error rate.

6. References

[1] ISO/IEC and IEEE Draft International Standards, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *ISO/IEC 8802 - 11, IEEE P802.11/ D10,* Jan. 1999.

[2] P. Brady, "A Model for Generating On-Off Speech Patterns in Two-Way Conversation," *Bell Syst. Tech. Journal*, *vol. 48, no 7, pp. 2245- 2272,* Sept. 1969.

[3] C. E. May and T. J. Zebo, "*A summary of speech statistics measured during the TASI - E Rego Park - Ojus field trial*," submitted for publication.

[4] ITU-T, "General Characteristics of International Telephone Connections and International Telephone Circuits One - Way Transmission Time" *G.114*, Feb. 1996.

[5] S. Tanenbaum, *Computer Networks*, 3rd ed., Prentice-Hall, 1996.

[6] D. Goodman, R. Valenzuela, K. Gayliard, B. Ramamurthi, "Packet Reservation Multiple Access for local wireless communications", *Proc. 39th IEEE Vehicular Technology Conference,* pp. 701 - 6, 1988.

[7] Leon-Garcia and I. Widjaja, *Communication Networks*, McGraw Hill, 1999.

[8] M. J. Karol, Z. Liu, P. Pancha, "The design and performance of wireless MAC protocols," in *Broadband Wireless Communications*, pp. 225-236, Springer - Verlag, 1998 (papers from the 9th Tyrrhenian Intl. Workshop on Digital Comm., Sept. 1997).

[9] O. Kubbar and H. Mouftah: "Multiple access control protocols for wireless ATM: problems definition and design objecti-

ves", IEEE *Comm. Mag.*, vol. 25, no. 11, pp. 93 - 9, Nov. 1997.

[10] I. Akyildiz, J. McNair, L. Martorell, R. Puigjaner, Y. Yesha, "Medium access control protocols for multimedia traffic in wireless networks," *IEEE Net. Mag*., vol. 13, no. 4, pp. 39 - 47, Jul. / Aug. 1999.

[11] J. Sanchez, R. Martinez, M. Marcellin, "A survey of MAC protocols proposed for wireless ATM," *IEEE Net. Mag*., vol. 11, no. 6, pp. 52-62, Nov. / Dec. 1997.

[12] M. Moroney and C. Burkley, "Multiple access protocols for indoor wireless communications", *Proc. IEEE Intl. Conf. on Selected Topics in Wireless Communications,* pp. 406 - 8, 1992.

[13] M. Visser and M. El Zarki, "Voice and data transmission over an 802.11 wireless network", *Proc. Sixth IEEE Internationa Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 648 - 52, Sep. 1995.

[14] B. Crow, I. Widjaja, J. Kim, P. Sakai, "Investigation of the IEEE 802.11 medium access control (MAC) sublayer functions", *Proc. Infocom*, pp. 126 - 33, Apr. 1997.

[15] B. P Crow, I. Widjaja, J. G. Kim, P. T. Sakai: "IEEE 802.11 Wireless Local Area Networks", *IEEE Comm. Mag*., vol. 35, no. 9, pp. 116 - 26, Sep. 1997.

[16] J. Stine and G. de Veciana: "Tactical communications using the IEEE 802.11 MAC protocol", *Proc. IEEE Military Communications Conference (Milcom),* pp. 575 - 82, Oct. 1998.

[17] J. L. Sobrinho and A.S. Krishnakumar, "Real-Time Traffic over the IEEE 802.11 Medium Access Control Layer," *Bell Labs Technical Journal*, Autumn 1996.

[18] T. Chen, J. Walrand, D. Messerschmitt, "Dynamic Priority Protocols for Packet Voice," *IEEE JSAC*, vol. 7, no. 1, June. 1989, pp. 632 - 643.

[19] W. Montgomery, "Techniques for packet voice synchronization," *IEEE JSAC*, vol. 1, no. 6, pp. 1022 - 8, Dec. 1983.

[20] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real Time Applications," IETF RFC 1889, January 1996.

[21] K. Sriram, T. Lyons, Y - T. Wang, "Anomalies due to delay and loss in AAL2 packet voice systems: Performance and Methods of Mitigation," *IEEE JSAC*, vol. 17, no. 1, Jan. 1999, pp. 4 - 17.

[22] E. Gilbert, "Capacity of a Burst Noise Channel," *Bell Syst. Tech*. J., vol. 39, Sept. 1960, pp. 125

Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 53(67), Fascicola 2, 2008

Security of Mobile VoIP

Mirela Ioanesiu[1]

Abstract - The rapid growth of computing, Internet and telecommunications systems have created a broad range of ways to communicate and access information. Voice over Internet Protocol is a solution that transports voice traffic over a data network as an alternative to the classic telephony. This paper addresses the issues of VoIP security and mobility through the integration of robust security features into a lightweight VoIP protocol that is tailored for mobile devices. A theoretical approach is realized with the development of a software prototype whose security and mobility proper-ties are analyzed.

1. Introduction

Telephone and computer systems are two technologies that impact many aspects of our daily lives. These technologies drive the world's economy and are central to the operation of virtually every enterprise. Although handsets have become more sophisticated, and operators are no longer required to connect calls in telephone exchanges, the basic operation remains the same. Conversely, computing has grown significantly throughout its lifespan. Computer Telephony Integration (CTI) incorporates computers and telephony systems [1]. Computer features such as data handling, media processing and graphical user interface are combined with telephone features such as call handling and routing. Currently CTI is predominantly used to drive software-based Private Automatic Branch eXchanges (PABX). However, CTI is heading toward the con-vergence of voice and data services over a data network. Voice over Internet Protocol (VoIP) is a CTI solution that is commonly used as an alternative to the Plain Old Telephone Service (POTS). Generally, VoIP refers to the transport of voice traffic over a packet-switched data network where hardware and software act as an Internet transmission medium for telephone calls. Packet switched networks route data packets on a hop-by-hop basis. These networks have the following properties:

- Telephone calls can be transmitted with little or no loss in functionality, reliability, or voice quality;
- Reduced telephony and infrastructure costs.
- Useful when there is limited or financially prohibi-tive access to alternative telephony networks;
- Increased line efficiency due to single lines being dynamically shared by many packets over time. By contrast, circuit switched networks rely on synchronous time division multiplexing where links are often idle;
- Packet-switched networks can perform data-rate conversions. Two nodes utilizing different data rates can exchange data because each can connect at its optimal data rate;
- When traffic becomes heavy on a circuit switched network, additional calls are blocked. On a packet-switched network, response time slows down gradually without immediate service interruption;
- Priorities can be used on packet-switched networks to give precedence to more important traffic;
- New levels of integration are possible for voice and a variety of data services.

VoIP has rapidly emerged as a popular alternative to existing telephony networks. Many sources [2, 3, 4, 5] indicate that VoIP will grow from approximately 100,000 US households in 2004 to more than 12 million by 2009. VoIP products are rapidly gaining market with home users who have reaped the benefits, uptake in the enterprise market has remained slow as a result of security and mobility concerns.

1.1 VoIP security

Corporate customers are generally more security conscious. They require that potential new technologies are proven not to be a security risk. Most current VoIP offerings do not offer a practical security solution. However, an important aspect behind the corporate success of

the VoIP technology is security. As VoIP technology becomes more heavily integrated into so increase the opportunities for hackers. Voice information during a VoIP call is generally outed unsecured through data packets on a public network. There is software that can capture, reconstruct and/or modify these sensitive voice conversations. Standard VoIP imple-mentations offer numerous undesirable opportunities for creative hackers [6]:

- Eavesdropping and recording phone calls;
- Tracking calls;
- Stealing confidential information
- Modifying phone calls
- Making free phone calls
- Pranks / Practical jokes
- Board room bugging
- Sending spam (voice or email)
- There are currently several competing VoIP standards in the market (such as SIP [7], IAX [8] and H.323 [9]), and very few practical security standards available to secure them. Furthermore, many enterprises that have adopted VoIP technology have not been able to effectively secure these solutions as a result of multi-vendor incompatibilities [10]. A standard installation of VoIP using SIP, H.323 or IAX protocols does not provide any kind of security for voice traffic. To alleviate this, it is necessary to add some form of protection, such as encryption, at the transport or network layer. To facilitate secure mobile VoIP, security must be addressed at each layer of the network. We must secure the VoIP devices, segregate the network, encrypt the traffic and introduce intrusion detection systems [6]. By incorporating security at each level of the network, it makes successful attacks much more difficult. While this may not compete with desktop machines, the amount of processing power and other PDA features have improved rapidly and could reasonably be expected to continue to advance.

1.2 Existing solutions

There are various existing options to secure VoIP traffic. Unfortunately, no solutions are offered that pro- vide suitable security characteristics while running on a mobile device. The following gives a briefly summary of the existing solutions in the areas surrounding secure VoIP communication.

1.2.1 Secure real-time transport protocol

The Secure Real-time Transport Protocol (SRTP) was developed for securing the media stream of VoIP protocols (such as H323 and SIP) that rely on the Real-time Transport Protocol (RTP). However, the protocol is not designed for mobile use. Solutions sur- rounding the RTP protocol suffer NAT traversal problems which create serious issues for mobile users.

1.2.2 IP security/Virtual private networks

Another option to secure media streams is to pass all traffic through an existing VPN. This approach has several problems. The most obvious is that a Security Association must exist between the originating and destination networks.

Simply breaking one type of security will not expose the entire network; it would require multiple levels of protection to be compromised. This requires a lot of attentions.

To allow multi-vendor solutions to interoperate it is essential that such solutions to be integrated into the VoIP standard. Since VoIP protocols already use negotiation options to determine call parameters (such as codec), it is reasonable to suggest that security parameters could be agreed on in a similar fashion.

1.3 Mobility

People are no longer desk-bound. Enterprises have to consider the growing population of mobile users that would benefit from the next generation of Information Technology and Telecommu-nication (IT&T) services. As more sophisti-cated wireless devices emerge, the demand for mobile two-way communication will rise dramatically. Flexible, rich access to telecomm unications services is crucial in order to achieve optimum performance. New technologies offer innovative features that result in better ways of doing business.

To offer these VoIP services on mobile devices, it is necessary to consider the restrictions imposed by this platform. Mobile devices typically have limits.

This paper details the research and development of a secure VoIP client that is geared toward mobile devices. In particular, the key outcomes are the utilization of a light-weight VoIP protocol and proven encryption techniques to implement a fully functioning, lightweight VoIP peer client. Special considerations are given to the characteristics and operation environment of mobile devices.

Section II outlines the solution background. Section III describes the design and implementation of the prototype solution. Section IV provides performance analysis and evalua-

tion discussion. Section V conclu-des the paper.

II. Solution Background

There have been many attempts to provide secure services for the major VoIP protocols [6, 11, 12, 13]. Unfortunately, these systems typically suffer from the following problems:
- Complicated to deploy and maintain;
- Rely on proprietary and/or incompatible solutions;
- -Require an existing Public Key Infrastructure (PKI) and/or other resources;
- Experience Significant routing problems when passing through NAT.

2.1 Inter-asterisk eXchange (IAX)

The Inter-Asterisk Exchange protocol (IAX) is a new protocol that has recently been developed in conjunction with the open-source Private Automatic Branch eXchange (PABX) known as Asterisk [8] [14]. This protocol was created as an alternative signaling protocol to SIP and H.323 [8]. It is currently rapidly gaining market-share in the VoIP market and shows considerable promise in the near future. The primary features of IAX are [15]:
-Highly optimized for the existing requirements of VoIP;
-Superior efficiency to H.323 and SIP when passing VoIP traffic [16];
-Minimized efficient bandwidth utilization for both signaling and media transfers [16]. Native support for Network Address Translation (NAT) technology is able to share a single port number, and transfer all data over a well known UDP port;
-Single protocol without the requirement of a separate media transfer protocol. All call signaling information, sequencing, and timing information is included in the transferred IAX frames;
-Written in a lightweight fashion. -Designed to be easily implemented [15];
-Can be used with any type of streaming media data (including video).

2.1.1 IAX security

IAX has been demonstrated to provide significantly greater efficiencies than SIP or H.323 when running unsecured [16]. Its performance in a secure environment is investigated here. If IAX can provide the same comparative levels of efficiency it is an ideal protocol for deployments with NAT environments and mobile users.

2.2 VoIP quality considerations

The parameters that a user would normally associate with their determination of call quality are known as Quality of Service characteristics. When voice data is traversing a packet-switched network, the handling of the traffic will achieve certain operational perfor-mance levels under various demand levels. Interarrival delay, jitter and packet loss are used as intrinsic QoS measures [17].

2.3 Audio codec

All VoIP technologies rely on a codec to transform analogue signals into digital voice packets. The choice of codec is a trade-off between voice quality, processing power and bandwidth requirements. A selection of commonly used VoIP codecs is given in the table below [18]:

2.4 Encryption algorithm

In order to provide secure transmission of data, it is necessary to offer confidentiality and authentication. In other words, data must be valid and should not be available nor disclosed to unauthorized parties.

Table 1. Codec feature comparison chart

Codec Name	**Sample Rate (kHz)**	**Bit-rate (kbps)**	**Multi-rate**	**VBR**	**PLC**	**License**
Speex	**8, 32**	**2.15 -** 24.6	Yes	Yes	Yes	Free / open-source
iLBC	**8**	**15.2** or 13.3	**No**	**No**	Yes	Free / closed source
AMR	**8**	4.75 **12.2**	Yes	**No**	Yes	Proprieta-
G.729	**8**	**8**	**No**	**No**	Yes	Proprieta-ry
GSM	**8**	**13**	**No**	**No**	**No**	Patented
G. 723.1	**8**	**5.3 6.3**	**No**	**No**	Yes	Proprieta-
G.728	**8**	**16**	**No**	**No**	**No**	Proprieta-ry

In order to support different codecs, the encryption algorithm must be able to support variable length data payloads where the amount of data per frame is likely to be short but send at a high frequency (approximately 30-100 bytes 50 times per second). As the data payload is relatively small, it would be advantageous to use an encryption method that will not increase the size of the data to

be sent. Any small increases in size will add significant overhead to the transmission.

2.5 Mobile clients

A goal of this paper is to produce a secure VoIP client that can be run in a mobile device such as a PDA or smart phone. As there are currently no mobile open-source IAX clients suitable for testing, evaluations of my solution can be performed on a laptop. The table below compares a low end laptop with a high end PDA [11].

Table 2. CPU comparison of laptop and PDA

Device Name:	**IBM X30 Laptop**	**DellAximX51PDA[14]**
CPU Manufac-	Intel	Intel
CPU Speed:	800 MHz	624 MHz
Available RAM:	512MB	64MB
MIPS Rating:	2142	800
Comparative MIPS:	1.0	0.37

Although using MIPS (Million Instructions per Second) does not take into account the different instruction sets between CPUs, it is often used to give an approximate performance rating. Based on a simple MIPS comparison, a Dell Axim X51 PDA is able to perform 37% of the integer operations capacity of an IBM X30 laptop.

III.Design and implementation

To demonstrate the proposed modifica-tions to the IAX protocol, it was necessary to add these features to a VoIP client. An open source client was selected, the code examined, and an injection point to add the security code was identified. The tools and methodology to accomplish this are described below.

3.1 Kiax VoIP client

Kiax [19] is an open source soft-phone designed to exclusively utilize IAX. Like many other open source IAX clients, Kiax relies on the freely available "libiax", library to take care of the low level network functions. This library was constructed by the makers of Asterisk, and is commonly used by open source IAX clients. The code modifications necessary to support encryption were mostly required within libiax

3.2 Cryptlib

Cryptlib is a powerful, general purpose open-source cryptography package designed to provide security services to applications. Its main purpose is to provide cryptography functions that can be integrated into applications. The design of Cryptlib is based on a layered structure that can provide different levels of controll to the user. Using Cryptlib, it was possible to experiment with a variety of different encryption methods to assess their impact on performance. A complete architecture diagram is given in Fig 1, below [20] .

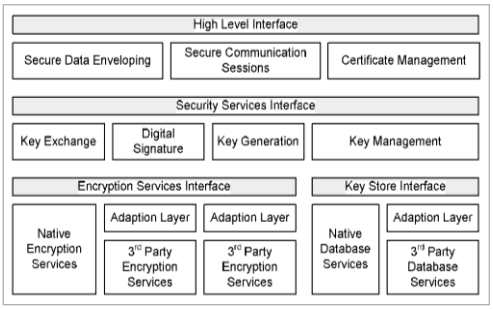


Fig.1 Cryptlib Architecture Diagram

3.3 Solution architecture

The block diagrams below give a basic description of the structure of the Kiax software layers. Fig. 2, below, shows the architecture of the original version of Kiax.

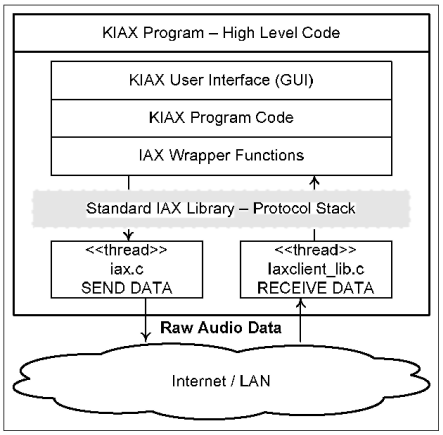


Fig.2 Standard Kiax architecture

Kiax provides a GUI interface to the user, which communicates the settings and preferences to the Kiax program code. The low level IAX protocol program code is provided in the form of a standard library known as libiax.c. This library package is also responsible for encoding and transporting the audio data captured from users.

The modified version of Kiax, Fig. 3, adds another layer of processing to the audio stream. After the voice data has been encoded via the audio codec, it is intercepted and encrypted before being sent across the network.

At the receiver's side, the audio is decrypted, and passed back through the normal Kiax processing stack.

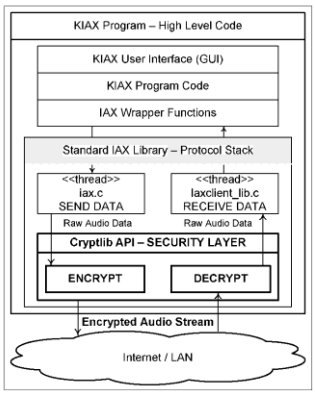


Fig.3 Modified Kiax Architecture Diagram

3.4 Results and evaluation

Testing was carried out to assess the impact of security modifications to the Kiax program. After configuring the Local Area Network and the client machines, calls were placed and the data was collected. All tests were repeatable and provided very consistent data. A summary of the results is given below:

Table 3. LAN test results 1

VoIP Client:	**Kiax**	**Kiax**	**Kiax**	**Kiax**
Encryption:	None	IDEA/CBC	IDEA/CF	RC4
Min. CPU Use:	5.812 %	17.818%	16.132 %	17.635 %
Max. CPU Use:	10.020%	28.629 %	26.226 %	27.756 %
Avg. **CPU** Use:	7.935 %	24.158%	22.756 %	23.090 %
Max.Bandwidth:	1.75 kB/s	2.08 kB/s	1.75 kB/s	1.75 kB/
Delay Range:	16-58 ms	16-58 ms	16-58 ms	16-58 ms
Jitter Range:	26-28 ms	26-28 ms	26-28 ms	26-28 ms

Table 4. LAN test results 2

VoIP Client:	**Kiax**	**Kiax**	**Firefly**
Encryption:	AES/CBC	AES/CFB	None
Min. CPU Use:	17.818%	14.629 %	8.719%
Max. CPU Use:	27.427 %	27.227 %	13.123%
Avg. **CPU** Use:	23.447%	22.592 %	11.364%
Max. Bandwidth:	2.48 kB/s	1.75 kB/s	1.69 kB/s
VoIP Client:	**Kiax**	**Kiax**	**Firefly**
Delay Range:	16-58 ms	16-58 ms	2-3 ms
Jitter Range:	26-28 ms	26-28 ms	2-4 ms

Using Kiax with no encryption, the average processor utilization is 7.9%, and the bandwidth used approximately 1.75 kilobytes per second. This provides a baseline for Kiax's performanceIDEA - in CBC mode, the quality of the call remainedsimilar to using no encryption, however the bandwidth use increased. This is to be expected, as the data size increased from 33 to 40 bytes. When using IDEA in CFB mode, although the bandwidth was identical to the baseline, the call quality was more frequently interrupted by audio drop outs.

AES-in CBC mode, AES had slightly lower CPU usage as compared to IDEA/CBC, and can be attributed to the AES algorithm being more efficient.This method used the highest amount of bandwidth, adding approximately 0.7kB p/s. The bandwidth increase is larger for AES than IDEA, since the AES algorithm has a block size of 128 bits compared to IDEA using only 64. AES using CFB produced the lowest average CPU utilization of the encryption methods tested, and did not require additional bandwidth.

RC4-the RC4 algorithm performed slightly worse than AES/CFB. This is surprising, considering that it is natively a stream cipher.

Overall, the results of both call quality and processor usage are similar for the different encryption algorithms. However, AES in CFB mode should be considered as the preferred method, as it gives the lowest average CPU load, does not add any additional bandwidth requirements and introduces a minimum number of problems in the audio stream.

IV. CONCLUSIONS

VoIP products promise converged telecommunications and data services that are cheaper, more versatile and provide higher voice quality as compared to traditional offerings. Although VoIP products are rapidly gaining market share with home users, uptake in the enterprise market has remained slow as a result of security and mobility concerns. This paper addresses these security and mobility issues through the integration of robust security features in to a lightweight VoIP protocol that is tailored for mobile devices. A theoretical approach is realized with the development of a software prototype whose security and mobility properties are analyzed. The prototype that was created to assess this approach had the following properties:

-Provided a choice of 5 different encryption:

methods;
-Successfully traverses NAT;
-Simulated key exchange by the use of pre-shared session key;
-Strong security;
-No change to bandwidth requirements;
-Relatively low processor requirements.

V. Remarks

A. Abbreviations and acronyms

CTI - Computer Telephony Integration
PABX - Private Automatic Branch eXchange
POTS - Plain Old telephony Service
SIP - Session Initiation Protocol
IAX - Inter - Asterisk Exchange Protocol
H.323 - H.323 is the international standard for multimedia communication over packet-switched networks, including LANs, WANs, and the Internet.
PDA - Personal Digital Assistance
SRTP - Secure Real Time Protocol
RTP - Real Time Protocol
NAT - Network Address Translation
VPN - Virtual Private Network
PKI - Public Key Infrastructure
QoS - Quality of Service
VBR - Variable Bit Rate
PLC - Power Line Carrier
MIPS - Million Instructions per Second
GUI - Graphic User Interface
IDEA - International Data Encryption Algorithm
CBC - Cipher Block Chaining
CFB - Cipher Feedback
AES - Advanced Encryption Standard
RC4 - most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks).

B. Further research

Kiax was selected as the basis for the proposed system as it was freely available under an open-sourcelicense. Although it provides a valid base for evaluating different encryption methods, the IAX library it provides does not give optimal perform-ance or call quality. Despite the limitations of the client, the results of the performance testing, clearly demonstrate the feasibility of this approach. in the future I intend to extend this research with the use of optimized clients and encryption libraries and test these solutions on mobile devices and mobile device emulators.

References

[1] C. R. Strathmeyer, "An Introduction to Computer Telephony", IEEE Common. Mag., 35(5), May 1996, pp. 106-11.
[2] S.Phil,F.Cary, You Don't Know ack About VoIP, Queue, 2004, 2(6), p. 30-38.
[3] W.Stallings, Data and Computer Communications (Seventh Ed.), Pearson Educational International, 2004
[4] Deloitte, "Getting off the Ground: Why the move to VoIP is a Decisionfor all CXOs",On-line at: http://www.deloitte.com/dtt/research/0,1015,sid%3D2245&cid%3D64027,00.html (2004)
[5] M.Grant, "Voice Quality Monitoring for VoIP Networks",Melbourne, 2005.
[6] D. Bilby, "Voice over IP: What You Don't Know Can Hurt You " 2005 [cited 11-04-06];Available from:http://www.Securityassment.com/Presentations/VOIP_What_You_Don't_Know_Can_Hurt_You.ppt.
[7] J. Rosenberg, RFC3261 - SIP: session initiation protocol. Internet Engineering Task Force, 2002.
[8] M.Spencer, "IAX: Inter-Asterisk eXchange" Version 2. 2006 30/03/06 [cited 24-04-06]; Available from:http://www.rfc-editor.org/internet-drafts/draft-guy-iax-01.txt.
[9] P.E. Jones, H.323 Protocol Overview. [Presentation] 2003 [cited 10-04-06]; Available from:http ://www.packetizer.com/voip/h323/papers/.
[10] N. Gohring, "Sysadmins express concerns on VoIP Security":http://www.techworld.com/security/news/index.cfm?newsID=6030&pagtype=samechan.
[11] Abad, "Secure Mobile VoIP", in Microelectronics and Information Technology, Royal Institute of Technology Stockholm, 2003, p. 137.
[12] J. Arkko, E. Carrara, RFC3830 - MIKEY: Multimedia Internet KEYing. Internet Engineering
[13] B. Fuhrmannek, IAX Encryption. 2006 [cited 24-04-06];http://voip info.org/wiki/view/IAX+encryption.
[14] B. Schwarz, "Asterisk open-source PBX system", Linux Journal, 2004. 2004(118): p. 6.
[15] M. Spencer, F. Miller, IAX Protocol Description. 2005.
[16] T. P. Abbasi, S. Seddigh, N. Lambadaris, "A comparative study of the SIP and IAX VoIP protocols", Canadian Conference on Electrical and Computer Engineering, 2005.

[17] W.C. Hardy, VoIP Service Quality: Measuring and Evaluating Packet-Switched Voice. New York: McGraw Hill,2003.
[18] Xiph.Org. Speex Homepage. 2006 [cited 2006 01-10-06]; Available from: http://www.speex.org.
[19] Kiax Team. Kiax Homepage. :http://www.kiax.org/.
[20] P. Gutmann, Cryptlib Security Toolkit Manual. 2005[cited 04-10-2006]; http://www.cs.auckland.ac.nz/~pgut001/cryptlib

An Experimental Analysis of Performances of MAC Multicast in 802.11b Networks for VoIP Traffic

Ing. Ioanesiu Mirela

Abstract–In this paper is studied the be-havior of VoIP traffic over MAC multicast networks in multihop scenarios with and without hidden stations. The experiments show that the maximal throughput achie-vable in such networks is 1.76 Mbps for an 802.11 Data Rate of 2 Mbps. Although VoIP traffic can tolerate some frame loss, MAC multicast can in general be used only if additional higher-layer mechanisms are in place to mitigate MAC frame loss. The paper presents also the effect of an addi-tional random backoff collision avoidance mechanism in hidden station situations.
Keywords: VoIP, MAC multicast network, collision avoidance

I. Introduction

IEEE 802.11 infrastructure-based wireless LANs [1] have been commoditized for data applications in enterprise networks. Amid the growing use of VoIP for telephony in enterprises, the use of wireless local area networks for telephony is expected to grow rapidly in the future as well. The problem investigates in this paper is a experimentally study of performance and reliability of MAC multicast transmissions in 802.11b wireless networks with particular emphasis on VoIP. Multicasting is an important concept in net-working as it allows sending a single packet to multiple recipients. In many cases, multicas-ting allows for a much more efficient usage of networks as it eliminates the need to send out multiple packets with identical payload but different destinations.
The maximal number of VoIP connections in an 802.11b network ranges from 2 to 7 when using ITU's G.711 Codec with 10 ms of audio data per packet. Consequently, the savings in terms of freed up capacity when using multcast on the MAC layer, if applicable, are highly significant. Moreover, the number of potential receivers of multicast traffic is unlimited. While the experiments were conducted in networks in Ad-Hoc mode, it should be noted that the results also apply to infrastructure-based networks.
This experimental study is aimed at determining the usability of MAC multicast for VoIP over 802.11, in particular with respect to two scenarios. The first scenario is the use of multicast for a downlink VoIP stream that is intended for multiple recipients in the same cell of a wireless network such as, e.g. con-ference calls, all-employee audio broadcasts in enterprises or emergency voice announce-ments. The second scenario is the use of 802.11 for walkie-talkie like VoIP broadcasts in small to medium size 802.11 Ad-Hoc network islands for emergency response or disaster recovery and communication in environments without infrastructures. In both scenarios, it was envision that most if not all participants in the network would be subscribers of the VoIP stream. However, the results are independent of this assumption. A more detailed presentation of such scenarios can be found in [5].
The paper focused on a single traffic source generating voice traffic with only marginal traffic being generated by other stations. The rationale behind this approach is two-fold. First of all, the results mirror the perceived quality in a true VoIP MAC multicast "walkie-talkie" scenario where only one participant at a time has "permission to send". More importantly, this scenario exhibits a "best-case" behavior experimental analysis for VoIP over multicast in the sense that any other traffic will only lead to a deterioration in the perceived VoIP quality.
Whereas in wired networks, such as Ethernet, multicast and unicast frames are transmitted identically on the the MAC layer, there are significant differences between unicast and multicast frame transmissions in 802.11 wireless local area networks. In order to cope with the higher frame loss and collision rates in the wireless network as compared to a wired network, the 802.11 MAC protocol mandates acknowledgments of received unicast frames and retransmissions of non-acknowledged frames. There transmission timer values are chosen such that higher layer transport protocols, in particular TCP, do not get affected by the loss of a frame on the wireless medium once in a while. In contrast, the 802.11 MAC mandates that multicast traffic is not acknowledged and thus never retransmitted on the MAC (the only exception being multicast traffic that is sent to the AP). Therefore, the loss ratios as seen on the IP-layer are higher than for unicast traffic.

Furthermore, the 802.11 Distributed Coordination Function (DCF) offers an RTS/CTS (request to send/clear to send) frame exchange sequence to protect unicast traffic from interference loss due to two simultaneous transmission attempts by stations that cannot sense each other (the hidden-station problem). DCF does not allow the use of RTS/CTS for multicast traffic (again with the exception of multicast traffic sent to the AP). Consequently, in such scenarios, high frame loss may be experienced.

As outlined above, the advantages of using MAC multicast for VoIP would be compelling if the quality of the VoIP stream was acceptable at most or all subscribers.

The goal of this paper is the behavior of the wireless channel for plain, basic 802.11 MAC multicast. Therefore, it won't be studied the impact of mechanisms allowing for acknowledgments and retransmission of multicast traffic (see, e.g., [6]) on higher layers. It won't be investigate the effect of multicast routing protocols like, e.g., [7] or [8]. The properties of 802.11 MAC multicast under investigation here have not been studied experimentally before. Since, as outlined above, the behavior of MAC multicast and unicast is very different, an experimental study is needed to determine the actual properties of MAC multicast, in particular when used for VoIP. While the experiments study the properties in simple scenarios, the obtained results, such as loss ratios on a single link, loss due to hidden stations etc., can be used to set up simulations that study more complex network topologies and scenarios with respect to their MAC-layer behavior. While, in particular for large topologies, simulations are easier to set up, control, and modify, the data presented in this paper cannot be obtained through simulations. In conclusion this experimental study of the properties of 802.11 MAC multicast is well motivated.

The remainder of this paper is organized as follows. In section II, are determined loss and throughput of multicast UDP traffic as a function of payload length. In section III are studied the properties of multicast VoIP traffic when relayed over multiple hops. Section IV investigates VoIP traffic with hidden stations. In section V, the ramifications of using an additional backoff-mechanism are studied. The conclusions of the paper are in section VI.

II.Loss and throughput with MAC Multicast

The first experiment measured the available throughput for multicast traffic in terms of sent payload on Layer 4 with IP/UDP as bearer in a single-hop only scenario. It was used a program constantly sending out UDP frames over multicast to the wireless medium [4]. The stream was received by an endpoint in the wireless network listening to the multicast address used as destination address. For measuring throughput, sender and receiver were located next to each other in order to minimize loss. The results indicate that the maximal achievable payload data rate in this scenario is approximately 1.76 Mbps which is achieved when the payload of each UDP packet is chosen to be 1472 bytes (payloads larger than 1472 bytes get fragmented). When the 62 bytes of the IEEE 802.11 frame body and the IP/UDP headers (34+20+8) in each sent frame are accounted for, the overall throughput of the wireless network is approximately 1.83 Mbps. Between 0.1% and 0.35% of non-fragmented packets were lost with an average value of 0.15%. The loss was independent of the payload size of the frame. Fig.1 shows the measurements of payload throughput as a function of the payload size in a single multicast client scenario. Based on the number of frames sent per second and the fact that in this setup the payload of each frame is transmitted at 2 Mbps, it can be computed the fixed overhead for the transmission of each frame. For the measurements, the overhead evaluates to an average of around 815 ns per frame, equivalent to the transmission of approximately 200 bytes at 2 Mbps.

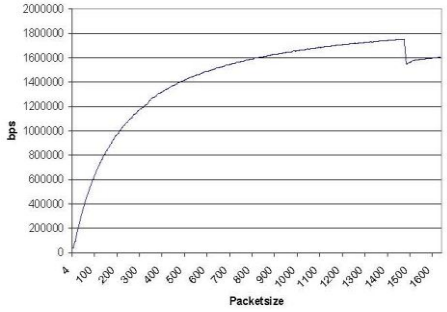


Fig. 1 Throughput as a function of the packet size for 802.11b multicast traffic at 2 Mbps. The drop in throughput for packet payloads larger than 1472 bytes is due to fragmentation.

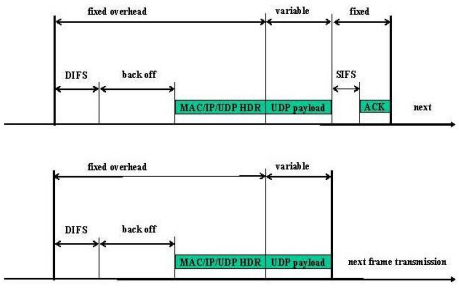


Fig.2 IEEE 802.11 CSMA/CA medium access scheme for unicast (top) and multicast (bottom) frames.

For space reasons, it wasn't presented a detailed description of the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) medium access scheme according to the Distributed Coordination Function (DCF) of the 802.11 standard [1]. A pictorial presentation of the mechanism and the transmission compo-nents of a frame is shown in Fig. 2. As depicted, multicast DCF transmissions are not acknowledged. Let R denote the data rate in bps and b the size of the data frame in bytes. Then, the time needed for transmitting frame components can be computed as shown in the following table 1.

Table 1

Part	Time
Data Frame	192ns+8b/R
SIFS	10ns
ACK	192ns+112/R
DIFS	50ns

Furthermore, in the scenario of a single client constantly transmitting, the average random back-off time is 310 ns (see [4]). The actual data frame have an overhead of 34 bytes for the 802.11 MAC header, 20 bytes of IP header and 8 bytes of UDP header totaling 62 bytes plus the UDP payload size. Summing up these values, the fixed overhead per frame as illustrated in Fig. 2 for multicast traffic at 2 Mbps can be calculated as 800ns.
This value matches well with the overhead measured in the experiment. The experimental values are a little bit higher due to the fact that the overhead of periodic beacons sent out by the stations in the Ad - Hoc networks is not included in the calculated value. As a multicast frame transmission does not include the transmission of an acknowledgment, the multicast transmission of a frame at 2 Mbps is 258 ns shorter than the unicast transmission of the frame at the same data rate. This was also experimentally verified. In the same scenario as described above, unicast traffic with 1472 byte of UDP payload achieves a maximal throughput of 1.68 Mbps as opposed to 1.76 Mbps observed for multicast traffic.

III.MAC Multicast Multihop Forwarding

It was studied the behavior of VoIP traffic when forwarded over multiple hops using 802.11 MAC multicast in an 802.11b Ad - Hoc network. The same results are, if the traffic is forwarded between access points that form a wireless distribution system (WDS) via MAC multicast. It were used five laptops as shown in Fig. 3. The laptops were deployed in an office environment. The distance between two communicating stations was between 25 m and 30 m. Non - adjacent stations were not in line of sight of each other with heavy wall structures between them. Thus, each station could receive transmissions only from its immediate neighbors in the Fig. 3. The signal strength between immediate neighbors was excellent. The sender synthesized a traffic stream equivalent to a VoIP stream generated by an ITU G.729 codec with 30 ms of audio data per sent packet (42 bytes UDP payload per packet). It were used this codec as it is commonly used in wireless environments. Experiments with other codecs lead to similar results. In order to reach the rightmost receiver (4th Hop), the frame needed to be forwarded by all stations in between. For frame forwarding and voice synthesis, it was used a framework that is described in detail in [5]. In this framework, flooding is used for multicast packet distribution in the network. In other words, each receiving station forwards each received MAC multicast frame the first time it receives it. A multicast storm is avoided by memorizing which packets have already been forwarded. Transmitted packets are stored for 1 second, amounting to a maximal memory usage of 245 KB at a data rate of 2 Mbps. It should be noted that the focus of this paper is strictly on experimentally investigating the behavior of the 802.11 MAC multicast transmissions. It was chose flooding for the experiments because it constitutes the simplest way of facilitating a framework for the experiments. This choice has no influence on the results of the experiments. As any other MAC multicast routing framework must forward packets the same way in the studied topology, the obtained results in terms of MAC multicast properties would not change for any other routing mechanism.

Fig. 3. Schematic Laptop Configuration in Multihop Forwarding Experiment.

In order to calculate the round trip time, receiving stations randomly responded to about every 50th voice packet received. Each experiment lasted 105 seconds, i.e., consisted of 3500 voice packets. At each receiver, it was calculated loss and jitter as specified in [9]. The round trip time to / from all receivers was computed at the sender based on the responses from the receivers. Apart from the VoIP stream and the sporadic responses from the receivers as described above, no other traffic was present. The obtained values for loss, jitter and round trip time were as follows:

Tabel 2

Feature	1st	2nd	3rd	4th Hop
Loss Ratio avg. Loss Ratio std. dev.	0.007 0.003	0.012 0.004	0.015 0.006	0.017 0.007
Jitter avg. Jittter std. dev.	0.18 0.06	0.21 0.09	0.47 0.22	0.80 0.16
RTT avg. [ms] RTT std. dev.	2.96 1.55	6.46 0.95	9.79 0.44	13.04 1.58

Fig. 4 shows the loss ratios in all experiments for all receivers. The rates for loss, jitter and round trip time were fairly consistent. The values for delay, loss and jitter increase with the number of hops. In this four hop scenario, round trip time and jitter are more than acceptable for VoIP traffic. The loss ratio of 1.7% at the forth hop can be considered just acceptable for VoIP. In the studied forwarding configuration, it is clear that every frame lost at a hop cannot be forwarded and thus also counts as lost at subsequent hops. The per - hop loss ratio is between 0.2% and 0.7%. While this is significantly higher than in the previous experiment where sender and receiver were immediately co - located, we obtained identical values for per - hop loss when we checked the individual link loss ratios in this setting.

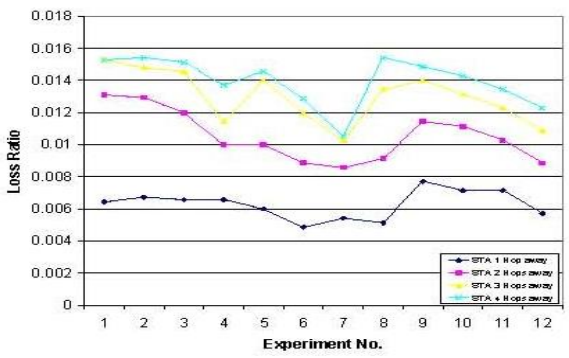


Fig.4 Loss Ratio for Multihop Experiment

The loss ratios in the instances of this experiment varied significantly. The increase in round trip time of 3 ms to 4 ms per hop is expected. The transmission time for a frame is roughly 1 ms which amounts to a minimal round trip time of 2 ms per hop. The additional time is due to the neces-sary additional processing for forwarding. The observed jitter values increase with the number of hops; they are very low at all four receivers.

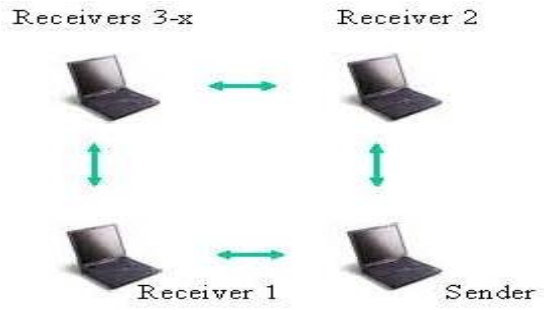
To summarize, the quality of the VoIP multicast stream was acceptable at all four receivers. Assuming a similar per-hop increase in loss ratio (between 0.2% and 0.7%), the quality of the VoIP traffic would no longer be sufficient or at least critical at a potential fifth hop.

IV.MAC Multicast Multihop Forwarding with hidden Stations

In the next experiment, it was studied multihop forwarding with hidden stations. For this experiment, four to six Laptops were deployed as schematically depicted in Fig. 5. The sender could send to receivers 1 and 2 directly. receivers 1 and 2 could not receive each other's transmissions. Up to three laptops, receiver 3-1, 3-2 and 3-3 were co-located in a position such that all could listen to receivers 1 and 2 but could not listen to the sender. Of course, 3-1, 3-2 and 3-3 could receive each other's transmissions. All ma-chines forwarded each packet exactly once as described before.

It were conducted three variants of this experiment. In Experiment 1, only receiver 3-1 was active. In experiment , receivers 3-1 and 3-2 were active and in experiment 3, receivers 3-1, 3-2 and 3-3 were active. Each experiment consisted of 3500 sent frames and was repeated 50 times.

Fig. 5 Schematic Laptop Configuration in Multihop



Forwarding with Hidden Stations Experiment.

For delay and jitter, was observed an average jitter value of below 0.3 for all stations in all experiments and the round trip time varied between 3 ms and 8 ms depending on the number of hops. As these values are excellent for VoIP and expected, the discussion will be focus on the observed loss ratios. The follo-

wing table shows the loss ratios for all stations.

Tabel 3

Exp. No.	Feature	Recv. 1	Recv. 2	Recv. 3-1	Recv. 3-2	Recv. 3-3
1	Loss avg.	0.0187	0.015	0.137		
	Loss std.	0.043	0.041	0.125		
2	Loss avg.	0.006	0.005	0.021	0.021	
	Loss std.	0.0023	0.029	0.615	0.614	
3	Los avg.	0.002	0.001	0.009	0.012	0.008
	Loss Ratio std.	0.002	0.002	0.009	0.009	0.009

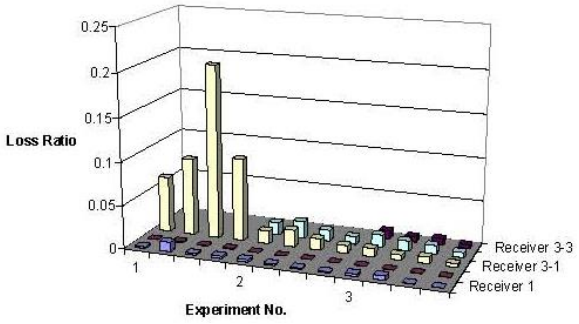


Fig. 6 Loss Ratio in Multihop Forwarding with Hidden Stations Experiment.

In experiment 1, the loss ratio for receivers 1 and 2 is 1.9 % and 1.5 % respectively and for receiver 3 - 1 it is around 14%. The loss ratios at receivers 1 and 2 is higher than in the previous experiment. This is due to five experiments in the series with very high loss ratios at receivers 1 and 2 (up to 26%). When these effects are discounted, loss at 1 and 2 is comparable to the loss at the first hop in the previous experiment. The reason for the very high loss ratio at receiver 3-1 (in the previous experiment, the loss ratio at the second hop was only 1.2%) is the hidden station problem. Receiver 1 and 2 receive the same packet to forward from the sender. As 1 and 2 cannot sense each others transmission, they start transmitting at the same time.
The CSMA/CA backoff mechanism of the 802.11 MAC does not help because it can only prevent collisions between transmissions of stations that can sense each other. If stations cannot sense each other, depending on the chosen backoff value, each station defers its transmission between 0 ms and 0.62 ms, but the transmission of a frame takes around 1 ms. Thus, receiver 1 and 2 transmit virtually always simultaneously which results in interference at receiver 3 - 1. This station is able to recover about 74% of the sent frames (not every interference leads to frame loss) but it cannot recover 26% of the traffic.
Experimentally was confirmed this conjecture. In a variant of experiment 1 with receiver 1 (receiver 2, respectively) switched off, the loss ratio at receiver 3-1 was in the same range as the loss ratio at the second hop in the preceding experiment. In other variations, was tested how sensitive the loss ratio is to minor movements of receivers / senders, tilting of the antennas and the like. It turned out that the general multiple forwarding path effect remained pronounced or even increased, however the actual loss ratio at receiver 3 - 1 varied significantly (from 10 % to 39 %, each variation was only tested once). In all of the tested cases, the loss ratio was unacceptable for VoIP streams.
Given the nondeterministic nature of interference, the co - located stations were set up to forward received frames. Therefore, a receiver that lost a frame when transmitted from 1 and 2 could still receive it when retransmitted by one of its peers. If different frames were lost at different receivers, the overall loss ratios should decline. Indeed, experiments 2 and 3 confirmed this conjecture. When one machine is co - located with 3 - 1, the loss - rate at stations 3 - 1 and 3 - 2 drops to around 2%. When two machines are co - located with 3 - 1, the loss ratio drops further to attain 1 % for all of the co - located stations

Tabel 4

Source \ At	Station 3 - 1	Station 3 - 2	Station 3 - 3
Station 1	0.925657	0.402895	0.94474
Station 2	0.010925	0.46052	0.007871
Station 3 - 1		0.078595	0.018527
Station 3 - 2	0.030412		0.02058
Station 3 - 3	0.024247	0.045799	
Loss	0.008751	0.012191	0.008605

Table 4 shows the immediate sources of newly received frames at receivers 3-1, 3-2 and 3-3 in experiment 3. Receivers 3-1 and 3-3 receive most of their packets from receiver 1, receiver 3 - 2 receives equally from receiver 1 and 2. Each of the stations receive at least 5 % of the frames from one of their peers, and the received ratio from both peers is comparable for all receivers. As can be observed, the derived loss ratios for receivers 3-1, 3-2 and 3-3 when discounting packets received from peers varies between 5 % and 13 %. When considering the quality of the VoIP stream, it would be insufficient in this experiment at each of the receivers 3-x without retransmissions from the peers.

This experiment shows that the forwarding of MAC multicast traffic is not always advisable. A spanning tree approach (as pursued by most multicast routing protocols) could easily avoid the interference loss at receiver 3 in the above scenario. However, consider an extended scenario with two additional stations 4 (5, respectively) which can only receive transmissions from receiver 1 (2). In this case, both receiver 1 and 2 need to be in the spanning tree. As it turns but, apart from Receiver 1 and 2 both immediately forwarding after receiving a transmission from the sender, only two additional variants are possible, namely the forwarding sequences S–1–3-2 and S–2–3-1. These transmission sequences would lead to significantly increased round trip time and jitter as well a higher loss ratio at receiver 5 (4) since traffic from the sender to 5 (4) is relayed over three hops as opposed to one before. It is not difficult to construct other configurations in which multiple forwarding paths with hidden stations lead to similar problems less obvious to solve. Preventing hidden station phenomena by spanning tree approaches for MAC multicast traffic can be difficult.

V.Effect of randomized forwarding delays

The goal of this section is the study of the effect of randomized forwarding delays on loss ratio, round trip time and jitter. In general, the idea is to avoid collisions due to multiple forwarding paths by a random back off mechanism similar to the one used in the 802.11 MAC. This approach will be referred as "additional back off (AL-back off). Except for the traffic source, each station draws a random value between 0 and the AL–back off value (which is similar to the CW-value in 802.11). This value in milliseconds is the time the station waits before forwarding the packet. The timing values are chosen such that two frames with different back off are transmitted at different times.

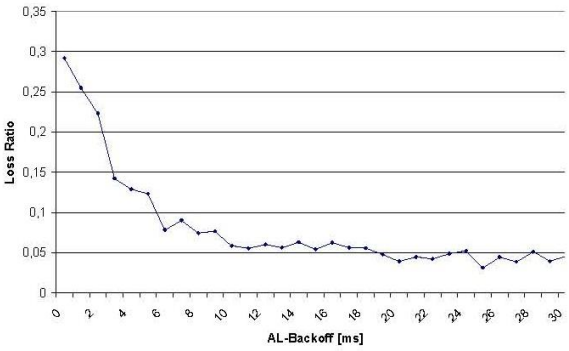


Fig. 8 Loss Ratio with Additional Backoff in Multicast Multihop with Hidden Stations Experiment

Fig. 8 shows the loss ratio as a function of the used AL-backoff in an experimental setup similar to the Multicast Multihop with Hidden Stations Experiment. The placement of the stations in this experiment is not identical to the one described in the previous section and the loss ratio without additional backoff in this experiment is somewhat higher. The following table 5 shows jitter and round trip time.

Tabel 5

AL-Backoff [ms]	Loss Ratio	Jitter	RTT [ms]
0	0.292	0.12	6.47
5	0.123	0.93	7.64
10	0.059	2.57	9.04
15	0.054	3.83	11.00
20	0.039	5.33	13.37
25	0.031	6.50	15.85

The loss ratio in the experiment drops from 29 % to below 5 % with increasing AL-backoff. The most significant decrease in loss ratio occurs for small AL -backoff values. As would be expected, jitter and RTT do increase with increasing AL-backoff values. So, in this scenario, using an AL - backoff could help to decrease the loss ratio while not increasing round trip time or jitter to unacceptable levels.
The results of the effect of an AL-backoff in the Multicast Multihop Forwarding scenario are shown in Fig. 9, Fig. 10 and Fig. 11. As the two scenarios show, such a mechanism may be helpful, in particular with low AL backoff values. The loss ratios improve significantly when using such a mechanism in the multiple forwarding path scenario.

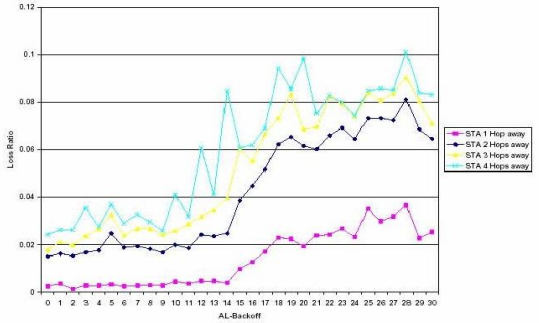


Fig. 9. Loss Ratio with Additional Backoff in Multicast Multihop Forwarding Experiment

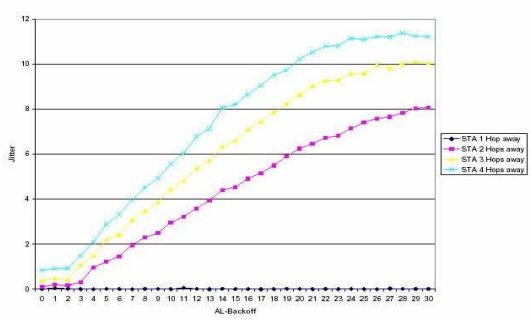


Fig. 10. Jitter with Additional Backoff in Multicast Multihop Forwarding Experiment

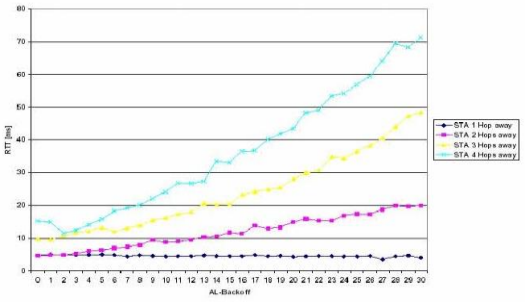


Fig. 11. Round Trip Time with Additional Backoff in Multicast Multihop Forwarding Experiment.

VI.Conclusions

This paper presented the experiments with MAC multicast traffic over IEEE 802.11 networks. The results show that even in a simple linear topology, the per-hop loss ratio is between 0.2 % and 0.7 %. Hence, even when using such networks exclusively for multi cast - VoIP traffic, frame loss becomes critical if traf fic is relayed over more than four hops in such a topology. The hidden terminal problem can lead to significantly higher frame loss, rendering VoIP unusable. Thus, the experiments suggest that, even for VoIP traffic that tolerates some loss, MAC multicast can in general only be used if additional higher - layer mechanisms are in place to mitigate MAC frame loss. Despite the results obtained in this experimental study, unreliable multicast transmissions may still be "good enough" in many scenarios, in particular if the station density is high.

References

[1] IEEE 802.11, 11a, 11b standard for wireless Local Area Net works. http:// standards.ieee.org / getieee 802/ 802.11-html

[2] S. Garg and M. Kappes. Admission Control for VoIP Traffic in IEEE802.11 Networks. In Proceeding of IEEE GLOBE COM 2003, San Francisco, California, 2003

[3] S. Garg and M. Kappes. An experimental Study of Through put for UDP and VoIP Traffic in IEEE 802.11b Networks. In proceeding of the IEEE Wireless Communication and Networking Conference (WCNC) 2003, New Orleans, LA, 2003.

[4] M. Kappes. An Application–Layer Approach to Communi cation in 820.11 Ad–Hoc Networks. In proceeding of the IEEE Wireless Communication and Networking Conference (WCNC) 2004 , Atlanta, GA, 2004

[5] S. Garg and M. Kappes Can I Add a VoIP Call? In Proceeding of the IEEE International Conference of Communication (ICC) 2003, Anchorage, Alaska, 2003.

[6] K. Tang, K. Obraczka, S–J. Lee and M. Gerla. Reliable Adaptive Lightweight Multicast Protocol. In Proceeding of the IEEE International Conference of Communication (ICC) 2003, Anchorage, Alaska, 2003.

[7] J. G. Jetcheva and D. B. Johnson. Adaptive Demand Driven Multicast Routing in Multi–Hop Wireless Ad Hoc Networks. Proceeding of the 2001 ACM international Symposium on Mobile Ad Hoc Networking & Computing Long Beach, CA, 2001.

[8] S–J Lee, W.Su and M. Gerla. On - demand Multicast Rout ing Protocol in Multihop Wireless Network and Applications 7 (6): 441 – 453, 2002

The security in wireless networks based on 802.11 standards.Problems and solutions. Developments of 802.11 standards in connection with security problems

Post–Graduate Eng. Mirela Ioanesiu
Technical University of Timisoara
E-mail:ioanesium@yahoo.com

1 Introduction

Organizations are rapidly deploying wireless infrastructures based on the IEEE 802.11 standard [1]. Unfortunately, the 802.11 standard provides only limited support for confidentiality through the wired equivalent privacy (WEP) protocol which contains significant flaws in the design [2, 3]. Furthermore, the standards committee for 802.11 left many of the difficult security issues such as key management and a robust authentication mechanism as open problems. As a result, many of the organizations deploying wireless networks use either a permanent fixed cryptographic variable or key or no encryption what so ever. This fact, coupled with the fact that wireless networks provide a network access point for an adversary (potentially beyond the physical security controls of the organization), creates a significant long term security problem. Compounding this is the fact that the access control mechanisms available with current access points contain serious flaws such that an adversary can easily subvert them.

Organizations over the last few years have expended a considerable effort to protect their internal infrastructure from *external* compromise. As a result, the organizations have canalized their external network traffic through distinct openings protected by firewalls. The idea is simple. By limiting external connections to a few well protected openings, the organization can better protect itself. Unfortunately, the deployment of a wireless network opens a "back door" into the internal network that permits an attacker access beyond the physical security perimeter of the organization. As a result, the attacker can implement the "parking lot" attack, see figure 1, where the attacker sits in the organization's parking lot and accesses hosts on the internal network.

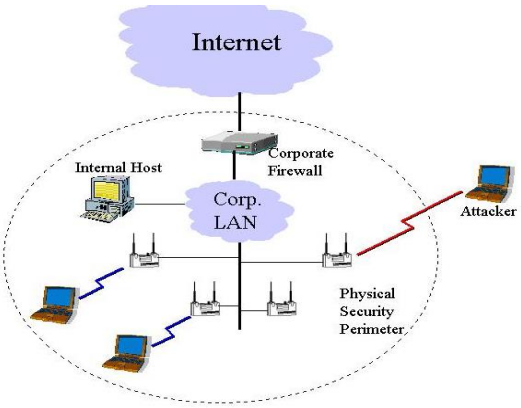


Figure 1: The Parking Lot attack

Ironically in some cases, the existence of the firewall may make the organization's hosts more vulnerable to the attacker because of the mistaken premise that the hosts are immune from attack and potential compromise. This paper describes the flaws in the two access control mechanisms that exist in access points and a simple eavesdropping attack against the 802.11 specified shared key authentication mechanism. Exploiting these flaws when encryption is not enabled permits an adversary immediate access to the wireless network and most likely the organization's local area network as well. The use of encryption prevents an adversary from gaining immediate access, but combining the attacks with the weaknesses found in WEP by others provides such access [2, 3]. The next section presents a short overview of the 802.11 wireless standard. This is followed an overview of the 802.11 security mechanisms and extension for access control. The next section describes attacks against the only two access control mechanisms avai-

lable in most current access points, and an attack against the 802.11 standard shared key authentication mechanism. Finally, I conclude the paper with recommendations or organizations with operational wireless networks.

2 802.11 Wireless Networks

802.11 wireless networks operate in one of two modes- *ad-hoc* or *infrastructure* mode. The IEEE standard defines the *ad-hoc* mode as Independent Basic Service Set (IBSS), and the *infrastructure* mode as Basic Service Set (BSS). In the remainder of this section, we explain the differences between the two modes and how they operate. In *ad hoc* mode, each client communicates directly with the other clients within the network, see figure 2. *ad-hoc* mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate.

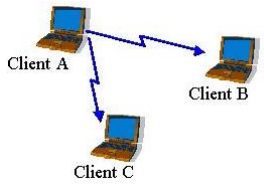


Figure 2: Example ad-hoc network

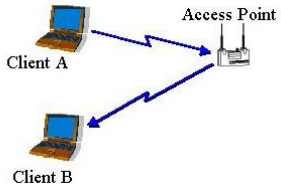


Figure 3: Example infrastructure network

If a client in an *ad-hoc* network wishes to communicate outside of the cell, a member of the cell *MUST* operate as a gateway and perform routing. In *infrastructure* mode, each client sends all of it's communications to a central station, or access point (AP). The access point acts as an ethernet bridge and forwards the communications onto the appropriate network–either the wired network, or the wireless network, see figure 3. Prior to communicating data, wireless clients and access points must establish a relationship, or an *association*. Only after an *association* is established can the two wireless stations exchange data. In *infrastructure* mode, the clients associate with an access point. The association process is a two step process involving three states:

1. Unauthenticated and unassociated,
2. Authenticated and unassociated, and
3. Authenticated and associated.

To transition between the states, the communicating parties exchange messages called management frames. I will now walk through a wireless client finding and associating with an access point. All access points transmit a *beacon* management frame at fixed interval. To associate with an access point and join a BSS, a client listens for beacon messages to identify the access points within range. The client then selects the BSS to join in a vendor independent manner. For instance on the Apple Macintosh, all of the network names (or service set identifiers (SSID)) which are usually contained in the beacon frame are presented to the user so that they may select the network to join. A client may also send a *probe* request management frame to find an access point affiliated with a desired SSID. After identifying an access point, the client and the access point perform a mutual authentication by exchanging several management frames as part of the process. The two standardized authentication mechanisms are described in sections 3.2 and 3.3. After successful authentication, the client moves into the second state, *authenticated and unassociated*. Moving from the second state to the third and final state, *authenticated and associated*, involves the client sending an *association* request frame, and the access point responding with an *association* response frame. After following the process described in the previous paragraph, the client becomes a peer on the wireless network, and can transmit data frames on the network.

3 802.11 Standard Security Mechanisms

The 802.11 standard provides several mechanisms intended to provide a secure operating environment. In this section, I describe each of these mechanisms.

3.1 Wired Equivalent Privacy protocol

The Wired Equivalent Privacy (WEP) protocol was designed to provide confidentiality for network traffic using the wireless protocol. The details of the algorithm used for WEP are beyond the scope of this paper. However, work by Walker and more recently by Borisov, Goldberg and

Wagner demonstrates that WEP, when used without a short key period, provides limited confidentiality [2, 3], and possible misuse of the network.

3.2 Open System Authentication

Open system authentication is the default authentication protocol for 802.11. As the name implies, open system authentication authenticates anyone who requests authentication. Essentially, it provides a NULL authentication process. Experimentation has shown that stations do perform a mutual authentication using this method when joining a network and our experiments show that the authentication management frames are sent in the clear even when WEP is enabled.

3.3 Shared Key Authentication

Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication.

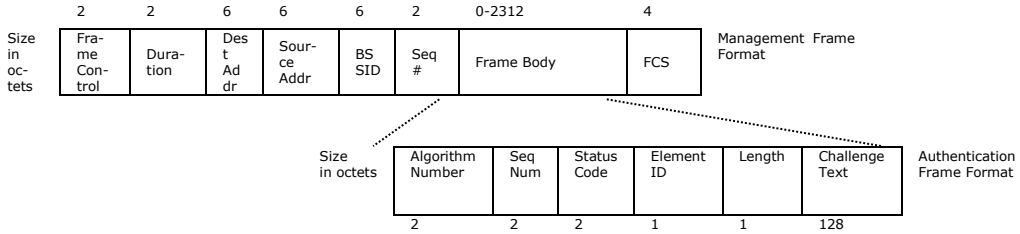


Figure 4: Authentication Management Frame

The station wishing to authenticate, the *initiator*, sends an authentication request management frame indicating that they wish to use "shared key" authentication. The recipient of the authentication request, the *responder*, responds by sending an authentication management frame containing 128 octets of challenge text to the *initiator*. The challenge text is generated by using the WEP pseudo-random number generator (PRNG) with the "shared secret" and a random initialization vector (IV). Once the *initiator* receives the management frame from the *responder*, they copy the contents of the challenge text into a new management frame body. This new management frame body is then encrypted with WEP using the "shared secret" along with a new IV selected by the initiator. The encrypted management frame is then sent to the *responder*. The *responder* decrypts the received frame and verifies that the 32-bit CRC integrity check value (ICV) is valid, and that the challenge text matches that sent in the first message. If they do, then authentication is successful. If the authentication is successful, then the initiator and the responder switch roles and repeat the process to ensure mutual authentication. The entire process is shown in figure 5, and the format of an authentication management frame is shown in figure 4. The format shown is used for all authentication messages. The value of the status code field is set to zero when successful, and to an error value if unsuccessful. The element identifier identifies that the challenge text is included. The length field identifies the length of the challenge text and is fixed at 128. The challenge text includes the random challenge string. Table 1 shows the possible values and when the challenge text is included based on the message sequence number.

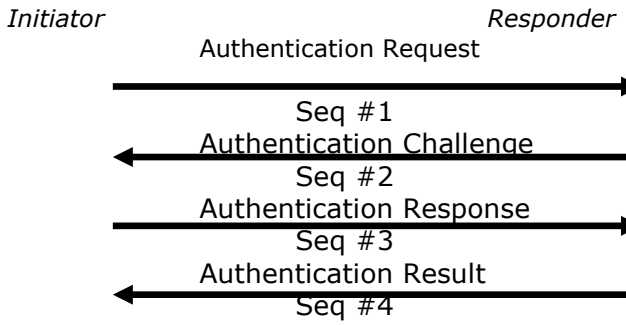


Figure 5: Mutual Station Authentication using shared keys

Table 1: Message Format based on Sequence Number

Sequence number	Status code	Challenge text	WEP used
1	Reserved	Not present	No
2	Status	Present	No
3	Reserved	Present	Yes
4	Status	Not Present	No

3.4 Closed Network Access Control

Lucent has defined a proprietary access control mechanism called *Closed Network* [5]. With this mechanism, a network manager can use either an *open* or a *closed* network. In an open network, anyone is permitted to join the network. In a closed network, only those clients with knowledge of the network name, or SSID, can join. In essence, the network name acts as a *shared secret*.

3.5 Access Control Lists

Another mechanism used by vendors (but not defined in the standard) to provide security is the use of access control lists based on the ethernet MAC address of the client. Each access point can limit the clients of the network to those using a listed MAC address. If a client's MAC address is listed, then they are permitted access to the network. If the address is not listed, then access to the network is prevented.

3.6 Key Management

Key management is a misnomer with respect to 802.11 as it is left as an exercise for vendors. As a result, only a few of the major vendors have implemented any form of key management or key agreement in their high-end products. Unfortunately, none of the vendors provide sufficient information to determine the level of assurance provided by their product. Worse, in some cases, the details that are available indicate that the vendors "solution" worsens the problem by using protocols with well-known vulnerabilities, e.g. un-authenticated Diffie-Hellman key agreement. The 802.11 standard does, however, provide for two methods for using WEP keys. The first provides a window of four keys. A station or AP can decrypt packets enciphered with any one of the four keys. Transmission, however, is limited to one of the four manually entered keys– the *default key*. The second method is called a key mappings table. In this method, each unique MAC address can have a separate key. The size of a key mappings table should be at least ten entries according to the 802.11 specification. The maximum size, however, is likely chip-set dependent. The use of a separate key for each user mitigates the cryptographic attacks found by others, but enforcing a reasonable key period remains a problem as the keys can only be changed manually.

4 Weaknesses in Current Access Control Mechanisms

This section describes the weaknesses in the access control mechanisms of currently deployed wireless network access points.

4.1 Access control mechanism

In practice, security mechanisms based on a shared secret are robust provided the secrets are well-protected in use and when distributed. Unfortunately several management messages contain the network name or SSID, and these messages are broadcast in the clear by access points and clients. The actual message containing the SSID depends on the vendor of the access point. The end result, however, is that an attacker can easily *sniff* the network name- determining the shared secret and gaining access to the "protected" network. This flaw exists even with WEP enabled because the management messages are broadcast in the clear.

4.2 Ethernet MAC Address Access Control Lists

In theory, access control lists provide a reasonable level of security when a strong form of identity is used. Unfortunately, this is not the case with MAC addresses for two reasons. First, MAC addresses are easily *sniffed* by an attacker since they MUST appear in the clear even when WEP is enabled, and second most all of the wireless cards permit the changing of their MAC address via software. As a result, an attacker can easily determine the MAC addresses permitted access via eavesdropping, and then subsequently masquerade as a valid address by programming the desired address into the wireless card– by-passing the access control and gaining access to the "protected" network.

5 Shared Key Authentication Flaw

The current protocol for shared key authentication is easily exploited through a passive attack by the eavesdropping of one leg of a mutual authentication.

The attack works because of the fixed structure of the protocol (the only difference between different authentication messages is the random challenge), and the previously reported weaknesses in WEP [2, 3]. The attacker first captures the second and third management messages from an authentication exchange, see table 1. The second message contains the random challenge in the clear, and the third message contains the challenge encrypted with the shared authentication key. Because the attacker now knows the random challenge (*plaintext*, *P*), the encrypted challenge (*ciphertext*, *C*), and the public *IV* , the attacker can derive the pseudo-random stream produced using WEP, *WEPK;IV*
PR , with the shared key, *K*, and the public initialization variable, *IV*, using equation 1.

$$WEP_{PR}^{K,IV} \equiv C \oplus P \quad (1)$$

The size of the recovered pseudo-random stream will be the size of the authentication frame, see figure 4 because all elements of the frame are known: algorithm number, sequence number, status code, element id, length, and the challenge text. Furthermore, all but the challenge text will remain the same for *ALL* authentication responses.

The attacker now has all of the elements to successfully authenticate to the target network– without knowing the shared secret *K*. The attacker requests authentication of the access point it wishes to associate/join. The access point responds with an authentication challenge in the clear. The attacker, then, takes the random challenge text, *R*, and the pseudo-random stream, $WEP_{PR}^{K,IV}$, and computes a valid authentication response frame body by *XOR-ing* the two values together. The attacker then computes a new integrity check value (ICV) as described in Borisov et. al. [3, 6]. Now, the attacker responds with a valid authentication response message, and he associates with the AP and joins the network3. Utilizing the network when WEP is enabled, however, requires the attacker to implement the WEP attacks [2, 3].

5.1 802.1X/Extensible Authentication Protocol

802.1X is an IEEE standard that allows authentication and key management for wireless (and wired) networks. 802.1X is used to control access to a network at the port level, and prevent unauthenticated/unauthorized devices from gaining access to a network. 802.1X is not a cipher (encryption algorithm, like WEP, AES, etc.), but rather, it focuses on authentication. 802.1X provides a framework, referred to as the extensible authentication protocol (EAP), to allow different types of authentication to be used. This allows 802.1X-enabled clients, access points, and switches to support a variety of authentication methods, including passwords, tokens, smartcards, certificates, etc. 802.1X is generally integrated with a backend authentication/authorization/accounting server, such as a RADIUS server. 802.1X enables mutual authentication, which prevents a rogue device from connecting to the wireless network, and prevents a rogue access point from tricking a device into connecting to it.

5.2 WPA, WPA2, and 802.11i

Due to deficiencies in WEP, enterprises and vendors began to supplement WEP with third-party solutions, some of which are proprietary. Around the same time, the IEEE began work on 802.11i, which defines strong security for wireless networks.

In order to try to maintain compatibility among the various solutions, the Wi-Fi Alliance (a group of wireless vendors) defined WiFi protected access (WPA). WPA was defined as a forward-compatible standard, which includes portions of the 802.11i standard, particularly those portions which would run on existing wireless access point and device hardware.
WPA replaces WEP with a strong encryption technology called temporal key integrity protocol (TKIP). TKIP provides enhanced data encryption, including a per-packet key mixing function. TKIP also provides a message integrity check (MIC), extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.
WPA also uses the 802.1X/EAP standard for authentication, employing different authentication schemes for enterprise and home users. Home users generally use shared secret keys, whereas enterprises generally use a stronger authentication technology aided by a central server based on RADIUS.
WPA2 is now available, and reflects the full 802.11i specification. WPA2 is very similar to WPA, but includes support for the advanced encryption standard (AES), which offers stronger encryption suitable for use in the U.S. Government. Note that AES is more computationally intensive than other kinds of encryption, and may require various access points and devices to be upgraded.
As of today, most wireless access points and devices support WPA, and support for WPA2/full 802.11i is increasing. These standards, along with a strong 802.1X/EAP authentication method, should be used for enterprise-class security, especially when such a critical service as wireless VoIP is made available. Unfortunately, this type of security requires set up and configuration, and even though it is available, it isn't widely used by enterprises.

5.3 Other Security Approaches

In addition to the link-level security offered by WEP, 802.1X/EAP, WPA, and WPA2/802.11i, other security approaches can also be used:
Virtual private networks (VPNs): connect wireless devices to the enterprise and provide authentication and encryption.

6 Conclusions and Future Work

These demonstrates serious flaws in *ALL* of the security mechanisms used by the vast majority of access points supporting the IEEE 802.11 wireless standard. The end result is that *ALL* of the deployed 802.11 wireless networks are at risk of compromise– providing a network access point to internal networks beyond the physical security controls of the organization operating the network. Unfortunately, fixing the problem is not easy nor straight forward. An interim short term mitigation (not a complete solution) is a robust key management system for WEP, and the use of higher level security mechanisms, e.g. IPsec. These mechanisms, however, just mitigate the problem until a new encapsulation algorithm is established by the IEEE 802.11 standards committee, and packet forgery will remain a problem until data authentication becomes standard. The only good long term solution is a major overhaul of the current standard which may require replacement of current AP's (although in some cases a firmware upgrade may be possible). Fortunately, the 802.11 standards body is currently working on significant improvements to the standard [7]. However, it is too late for deployed networks and for those networks about to be deployed. A number of vendors are now releasing high-end access points claiming that they provide an increase in security. Unfortunately, few of the products provide enough information to determine the overall assurance that the product will provide, and worse, several of the products that do provide enough information use un-authenticated Diffie-Hellman which suffers from a well-known *man in the middle* attack. The use of un-authenticated Diffie-Hellman introduces a greater vulnerability to the organization's network. The increase in risk occurs because an attacker can insert themself in the middle of the key exchange between the client and the access point– obtaining the session key, *K*. This is significantly worse than the current situation where the attacker must first determine the pseudorandom stream produced for a given key, *K*, and public *IV* , and then use the stream to forge packets.

References

[1] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer(PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

[2] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000.http://grouper.ieee.org/groups/802/11/Documents / DocumentHolder/0-362.zi%p.
[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." http://www.isaac.cs.berkeley. edu/isaac/wep-faq.html.
[4] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," Tech. Rep. RFC2284, Internet Engineering Task Force (IETF), March 1998.
[6] J. Walker, "Overview of 802.11 security." http://grouper. ieee.org/groups/802/15/pub /2001/Mar01/01154r0P802-15_TG3% -Overview-of-802-11-Security.ppt, March 2001.
[7] IEEE 802.11Working Group. http://grouper.ieee.org/groups/802/11/index.html.
[8] * * *: IEEE 802.11 and 802.11b Technology, Internet documentation
[9] * * *: Web Page from Wi-Fi Alliance, http://www.weca.net/OpenSection/index.asp
[10] Arbaugh, W.A., N. Shankar, Y.C.J. Wan: Your 802.11 Wireless Network has No Clothes, Univ. Maryland , documentaţie Internet, www.cs.umd.edu/~waa/wireless.pdf
[11] Brenner, P.: A Technical Tutorial on the IEEE 802.11 Protocol, Internet documentation, www.sss-mag.com/pdf/802_11tut.pdf
[12] * * *: DELL Co.-Wireless security in 802.11 (Wi-Fi®) networks, White papers 2003, documentatie Internet.
[13] Lough, D.L., T.K. Blankenship, K. J. Krizman: A Short Tutorial on Wireless LANs and IEEE 802.11, Politehnic Institute - Bradley–Virginia.
[14] SCHAFER, G.: Network Security & IEEE 802.11 Wireless LANs, Tutorial, Paris, 2002.
[15] SIMON, D., B. Aboba, T. Moore: IEEE 802.11 Security and 802.1X, doc IEEE 802.11 00/034rl, 2000.
[16] WALKER, J.: Unsafe at any Key Size: an Analysis of the WEP Encapsulation, doc IEEE 00-362, 2000.
[17] WALKER, J.: 802.11 Security Series, Intel Corporation, documentatie firma, 2002.