Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 49(63), Fascicola 1, 2004

Mobility Related Protocols in IP Networks

Pál István Borbás[1], Csaba Simon[2] and Miranda Naforniţă[1]

Abstract – The significant aspect of current networks is the mobility. The Mobile IPv6 protocol has been designed to accomplish these requirements. We compiled a test network in order to make some performance measurements and to study the characteristics of the Mobile IPv6. The scope of this paper was to measure the typical behavior in the indoor environment and test the deficiencies of Mobile IPv6. We have found that the Duplicate Address Detection protocolshould be further refined to assures quicker reaction times during handovers.

Keywords: Mobile IPv6, IP Mobility, Performance measurement.

I. INTRODUCTION

In the last decades the number of equipments, which needed connection to the Internet have grown exponentially. All of them claim an Internet Protocol (IP) address, but we know that the Internet is a thirty years technology, with a small address domain. However, during the lifetime of IP a lot of experience has been accumulated. The transfer speed and the QoS (Quality of Service) developed a lot till then. The ever-developing set of applications and the evolving technologies always fetched new opportunities to the communications industry. So the present IP version should be developed. This new IP version is IPv6 [1] (Internet Protocol version 6).

As the dimensions of the computing devices are becoming ever smaller, the mobility issue rises as an important requirement. The mobile equipments are prevailing not only in telecommunication or PC worlds, but in every branch of technology. Mobile users have the natural expectations that all services available through cable network, such as telephone, Internet. etc., should be accessible from their mobile terminals, too. However, the accomplishment of this is a huge challenge and brings up a number of problems. The goal is to achieve that the mobile equipment remains reachable when it is connected to the IPv6 Internet.

Without specific support for mobility in IPv6, packets destined to a mobile node would not be able to reach it while the mobile node is away from its home link. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link. However, then the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a substantial fraction of the population of the Internet during the lifetime of IPv6. The protocol introduced for this purpose, known as Mobile IPv6 [2], allows a mobile node to move from one link to another without changing the "home address" of the mobile node. The movement of a mobile node away from its home link is transparent to transport and higher-layer protocols and applications.

II. MOBILE IPv6

In Mobile IPv6 the moving nodes will have assigned to their network interface(s) at least three IPv6 addresses whenever they are roaming away from their home subnet. One is its home address, which is permanently assigned to the mobile node in the same way as any IP node. The second address is the mobile node's current Link-Local address. Mobile IPv6 adds a third address, known as the mobile node's care-of address, which is associated with the mobile node only while visiting a particular foreign subnet. The network prefix of a mobile node's care-of address is equal to the network prefix of the foreign subnet being visited by the mobile node, and thus packets addressed to this care-of address will be routed by normal Internet routing mechanisms to the mobile node's location away from home.

Each time the mobile node moves its point of attachment from one IP subnet to another, the mobile node will configure its care-of address by stateless address autoconfiguration, or alternatively by some means of stateful address autoconfiguration such as DHCPv6 or PPPv6 [5]. The decision about which manner of automatic address configuration to use is made according to the methods of IPv6 Neighbor Discovery [6]. A mobile node may have more than one care-of address at a time, for example if it is link-level attached to more than one (wireless) network at a time or if more than one IP network

[1] Electronics and Telecommunications Faculty, "Politehnica" University Timişoara, E-Mail: mona-naf@etc.utt.ro
[2] Department of Telecommunication and Media Informatics, Budapest University of Technology and Economics, E-Mail: simon@tmit.bme.hu

prefix is present on a network to which it is attached. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a binding. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a Binding Cache.

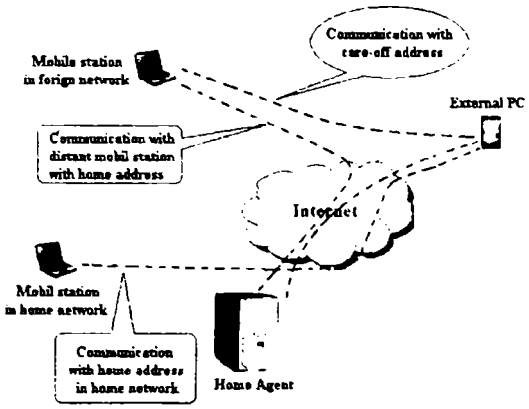

Figure 1. Mobile IPv6 overview

Fig. 1 present the function algorithm of the mobile IPv6. While away from home, a mobile node registers one of its bindings with a router in its home subnet, requesting this router to function as the home agent for the mobile node. The care-of address in this binding registered with its home agent is known as the mobile node's primary care-of address, and the mobile node's home agent retains this entry in its Binding Cache, marked as a ``home registration,'' until its lifetime expires. While it has a home registration entry in its Binding Cache, the home agent uses proxy Neighbor Discovery [7] to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet, and tunnels each intercepted packet to the mobile node's primary care-of address indicated in this Binding Cache entry. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation.
In addition, Mobile IPv6 provides a mechanism for IPv6 correspondent nodes communicating with a mobile node, to dynamically learn the mobile node's binding. The correspondent node adds this binding to its Binding Cache. When sending a packet to any IPv6 destination, a node checks its Binding Cache for an entry for the packet's destination address, and if a cached binding for this address is found, the node routes the packet directly to the mobile node at the care-of address indicated in this binding.

III. THE TESTBED

In this section we will introduce the basic considerations for the testbed been used. The testbed has to provide a flexible platform for research in the case of the mobility under IPv6. Therefore we used open source operating systems on PCs to implement the routers, the home agent, the gateway and the access routers. The operating systems and the modules used to add mobility to these equipments were selected to natively support IPv6.

A. Software elements

Linux [8] is a Unix-like multitasking, multiuser 32 and 64 bit operating system for a variety of hardware platforms and licensed under an open source license. Linux uses mos ly he same abs rac ions as he nix system. For example, the way processes are created on olle is e sa e i ix a Li u I ur ca OS is hc Debian Linux with 2.4.22 kernel [9].
MIP [8] Mobile IPv6 for inux is an imp'ementation of the IETF mobile-ip working group draft Mobility Support in IPv6. The project goal is to create a high quality implementation of Mobile IPv6 for inclusion in the mainline Linux kernel tree. Version 0.9.2 used by us is the 7th public release. It complies with the Mobile IPv6 draft revision 15. MIPL implementation includes all three MIPv6 entities Correspondent Node, Mobi'e Node and Home Agen . Re'ease inc'udes a kernel patch and a set of user tools and scripts.

B. Network topology

The most important sight when we framed the test network was the simplicity, thrift and efficiency. The principal consideration was to realize with a few components a well functioning network, with more sub networks, where we can take some versatile measurements. All parts of the network (the router, the home agent, the gateway and the three access points) are usual PCs, and the operation system has open source code.
We designed a closed network and we used six common-purpose PCs, a laptop and a switch to build it (see Fig. 2). Only the gateway had direct access to the Internet, the other components have access across the gateway, only.

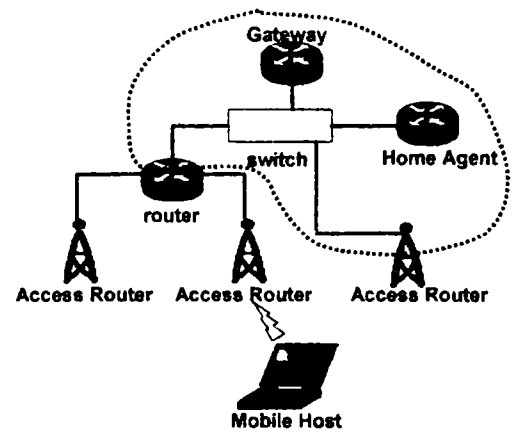

Figure 2. Testbed topology

In the test bed are three base stations (access points = corresponding nodes). Every one of them represents a separate foreign network and the mobile node moves between these networks. In practice the laptop

position has a constant physical location; it changes only its domain identifier and so it can handover between the access points. So in every moment the network is composed of two network
The first one is the home network, and it contains the gateway, switch, home agent and the router. The second one is the foreign network, having the base station and the laptop. Among the components are Fast Ethernet connections, only the laptop has wireless connection toward to the access points.
On Fig. 2 we also show the IPv6 addresses of each networking element. The larger IP subnetwork (delimited with the dotted line in Fig. 2) is the home network, while the other three are the foreign networks.

C. Configuring routing advertisments on AR

When MN comes to a new network, it does a link-local address configuration, going to the next phase if that succeeds. The next phase of autoconfiguration involves obtaining a Router Advertisement or determining that no routers are present. If routers are present, they will send Router Advertisements that specify what sort of autoconfiguration a host should do. If no routers are present, stateful autoconfiguration should be invoked. Routers send Router Advertisements periodically, but the delay between successive advertisements will generally be longer than a host performing autoconfiguration will want to wait. To obtain an advertisement quickly, a host sends one or more Router Solicitations to the all-routers multicast group.
We had different ESSID on the the foreign networks. Generic movement detection uses Neighbor Unreachability Detection to detect when the default router is no longer bi-directionally reachable, in which case the mobile node must discover a new default router (usually on a new link).

IV. MEASUREMENTS

Without reference to the environment, when it is cabled or wireless, the most important and the most interesting measurements are the throughput analysis. During the measurements we have to obtain, when the packet loss is minimal, as possible, in addition to the transfer speed a predefined value.
To ensure, that the function of this network is continuous we constantly paid attention to the different messages, we measured every delay in transmissions and the Round Trip Time (RTT). The most important in this test network is to correctly configure the frequency of Router Advertisement (RA). We set this value at 1 second, in this way the packet loss is minimal. When this value is too high, the packet loss is ascendant, but when the RA period is to low (high message frequency) it can overload the channel.
First we wanted to find what the maximum range is where we still can measure exactly, without packet loss. Theoretically the WLAN transmission range is 100m, but this is an outdoor value. Our measurements has shown that this range is reduced in indoor environment, as presented in Fig. 3. Indeed, between 0 and 25m the transfer was perfect, but after this range in short distance (2m) the connection was completely interrupted.

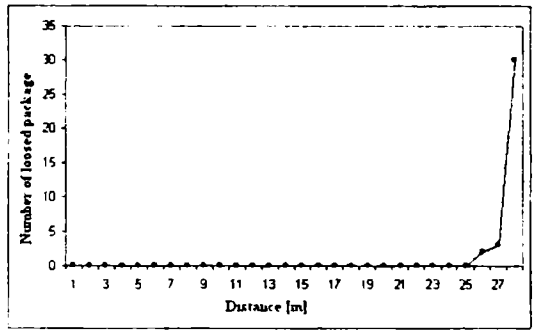

Figure 3. Packet losses and radio range

To follow the perpetual functioning I measured the RTT (Round Trip Time) usong the ping utility. The RTT is the period under that one message has covered the distance between source and destination in either direction. I have chosen 1 second interarrival periods for Router Advertisements, otherwise at higher values packet losses may appear due to delayed reaction. When the mobile node is not moving, so we do not have any binding updates, the packet loss rate is 0. This is presented in Fig. 4.

```
---2001:738:2001:4001::5 ping statistics---
2154 packets transmitted, 2154 received,
0% loss, time 1805840ms rtt
min/avg/max/mdev=1.917/2.058/3.422/1.848 ms
```

Figure 4. Packet losses without binding update

When the mobile node is changing its position, namely its moving between the two access routers, it sends one binding update. In this case appears the loss, as indicated the Fig. 5.

```
---2001:738:2001:4001::5 ping statistics---
610 packets transmitted, 603 received,
1,14% loss, time 605840msrtt
min/avg/max/mdev=1.962/2.181/9.714/1.725 ms
```

Figure 5. Packet losses at the binding update

If we represent the RTTs graphically we get the chart of Fig. 6.

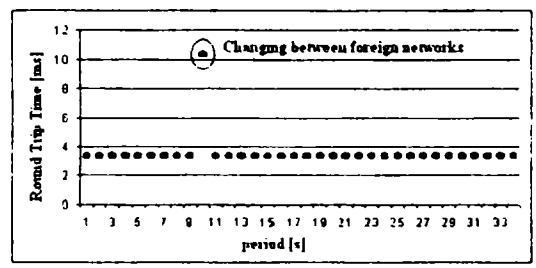

Figure 6. RTT between the gateway and mobile host

It is easy to observe that during handovers, at the 10th second, the value of the RTT grows drastically. This

is caused by Duplicate Address Detection (DAD) [3], an indispensable protocol.

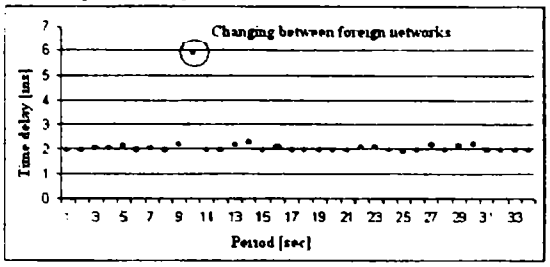

Figure 7. Delay of the Echo Request

The same behavior can be observed if we measure the propagation delays of both echo messages: echo request and echo replay. Obviously, since in this case the path is traversed in one direction, only, the differences are lower. The propa_ation delay of the echo request (up-link direction) is longer than that of the echo replay (down-link direction). On the up-link we must setup the tunnel, so it takes around 6-8 msec, the return path is faster, it takes around 3-4 msec (see Fig. 7).

We also tested the human perception of the effects of handovers of widel_ used services, such as telnet, ftp that run over TCP. The two mentioned services functionned „normally", they ru... wi.hou. problems in this respect. Note that telnet generates quite reduced traffic, while ftp based file transfer is not affected by short interruptions.

Next we measured the fluctation of the transfer speed of TCP flows in our testbed, because the most part of the Internet is based on TCP transfer protocol. The congestion avoidance mechanisms of TCP react to packet losses.

When we had a single mobile node connected to a server, the transfer speed is limited only by the radio technology. With IEEE 802.11b [4] this value is around 600-800 Kbyte/sec (5 – 6.6 Mbps). This is shown in Fig. 8.

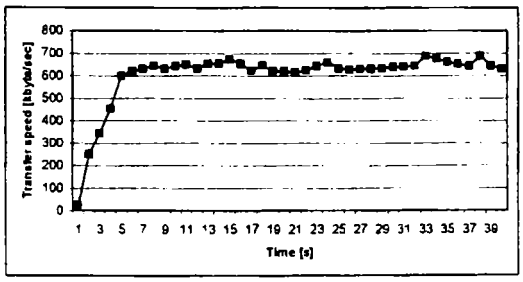

Figure 8. The maximum transfer speed

This value decreased, as other mobile nodes are connected to the same server. When we have three laptops connected, the transfer speed becomes proportionally smaller. This can be seen in Fig. 9, where the throughput of one mobile user is reduced twice, as other mobile terminals enter the same wireless subnetwork (at the 30th and the 68th seconds of measurement).

The throughput is quckly dropping and shares the available capacity with the newcomers in a fair manner.

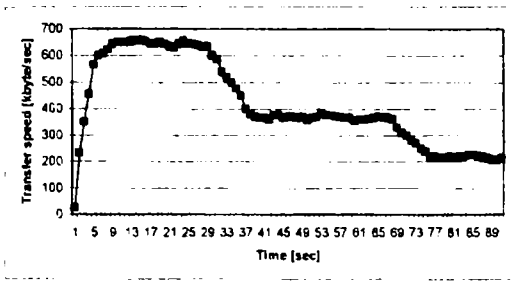

Figure 9. TCP transfer speed for multiple users

We have checked the transfer speeds of three mobile users commnuicating in the same subnetwork.

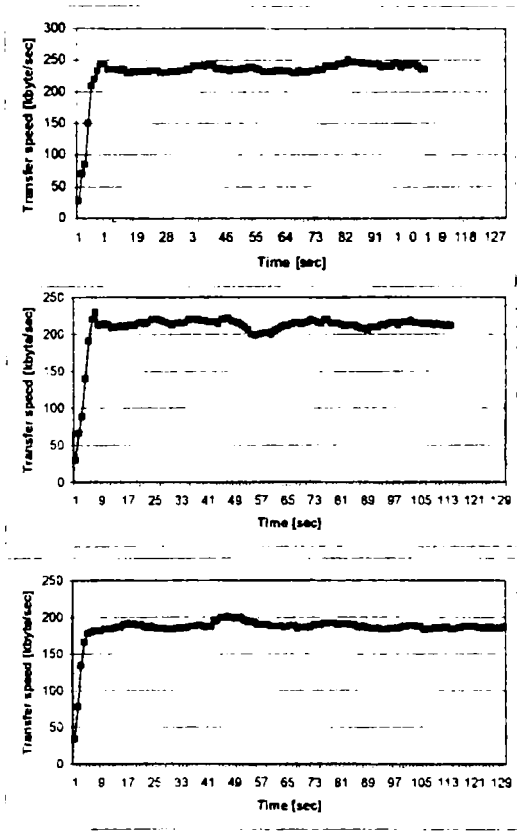

Figure 10. Transfer speed of the three users

Their throughput is approximately equal, so the bandwidth is shared in a fair manner, indeed. Fig. 10 shows the achieved transfer rate values of all the three mobile hosts.

Based on the measurements we concluded that three mobile stations do not cause congestion due to extereme channel utilization and nor they overload the Home Agent. So the sistem under moderate load is scalable. A more frequent channel utilization and/or user density is required to test the scalability of the system. For these measurements a Mobile IPv6 emulator would be required to generate Binding Update messages at high rate, but these investigations exceed the limits of this paper.

In the last part of measurments we analysed, how the TCP reacts to packet losses. In this situation it is important to choose an optimal value for routing advertisments. A high frequency of this messages use needlessly the channel, but when the frequency of this messages is to low, the packet loss rate can drastically increased. With an optimal value (1 second) we exerienced between 3 and 5 packets losst. If during a handover we loose more than 4 packets (that is we have more than 3 duplicated acknowledgments), TCP enters in timeout, as presented in Fig. 11.

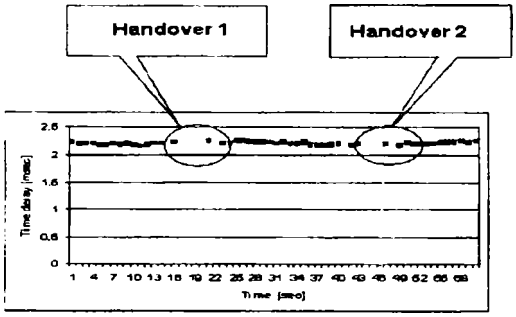

Figure 11. TCP timeout during handover

V. CONCLUSION

Today we are witnessing the spread of the wireless networks. The number of equipments connected to the Internet have drastically increased. These conditions made necessary the introduction of a new protocol, which is more dynamic and has a larger address domain. This revolutionary protocol is the Internet Protocol version 6 (IPv6).

One other very significant aspect of current networks is the mobility, which is fundamental both in data-, and telecommunication world. So we need one IPv6 based protocol, which fitly accomplishes these requirements and assures a large bandwidth for exigent applications at the expected QoS levels. To solve this issue the Mobile IPv6 protocol has been proposed. This architecture is similar with the IPv6 structure; differences are appearing only in functionality. On the data-link layer level this protocol is based on a wireless LAN technology. We used the IEEE 802.11 protocol family in our tests due to its huge installation base.

To study the characteristics of the aforementioned Mobile IPv6 protocol, we compiled a test network to make some performance measurements. The scope of this paper was to measure the typical behavior in the indoor environment and test the deficiencies of Mobile IPv6. We have found that the original Mobile IPv6 causes packet losses and induces high propagations delays during handovers. The responsibility for these events lies on the Duplicate Address Detection (DAD) protocol, an issue recognized by other researchers, as well. Therefore we focus our further research on developing a lighter DAD protocol that assures quicker reaction times during handovers.

REFERENCES

[1] S. Deering, R. Hinden "IP Version 6 (IPv6)", Internet Request For Comments RFC 2460, December 1998

[2] W. Fritsche, F. Heissenhuber "Mobility support for the next generation Internet", Internet Request For Comments RFC 946, February 2000

[3] S. Thomson "IPv6 Stateless Address Autoconfiguration", Internet Request For Comments RFC 2462, December 1998

[4] IEEE Standards Board "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", May 1999

[5] G. Egeland "Testing of PPPv6 over ISDN/xDSL", Tsunami Project, http://www.eurescom.de/~public-web-deliverables/P1100-se..es P1..._pppv...tml, September 200.

[6] T. Narten, E. Nordmark "Neighbor Discovery for IP Version 6 (IPv6)", Internet Request For Comments RFC 2461, December 1998

[7] T. Narten, E. Nordmark, and W. A. Simpson "Neighbor Discovery for IP version 6 (IPv6)", Internet Request For Comments RFC 2461, August 1996

[8] Linux homepage, http://www.linux.org

[9] Debian homepage, http://www.debian.org