DESIGN AND IMPLEMENTATION OF HYBRID CRYPTOGRAPHY INMANETS

[1]Dr A. Ramesh Babu
Professor & Head Department of Science and Humanities
Hindustan Institute of Technology and Science, Rajiv Gandhi Salai, Old Mahabalipuram Road,
Padur, Kelambakam, Chennai, Tamil Nadu 603103
Email :arbbabu67@gmail.com

[2]M V S SNagendranath
Research Scholar, Department of Computer Science and Engineering ,
Hindustan Institute of Technology and Science, Rajiv Gandhi Salai, Old Mahabalipuram Road,
Padur, Kelambakam, Chennai, Tamil Nadu 603103
Correspondence Email :shivamaganti@gmail.com

Abstract

An effective way of short range communication are Mobile ad Hoc Network (MANET),but due to their t inbuilt characteristics such as dynamic topology, minimal physical security, constrained functionality, which all makes them vulnerable to both passive and active attacks in network. In such environment, verifying the nodes authenticity and achieving data confidently is a challenging task and therefore, a great deal of research has been dedicated to securing routing and management of keys. A novel concept has been presented in this paper for designing an efficient security solution that can protect ad hoc network from heterogeneous attacks. The Ad hoc-On Demand Distance Vector (AODV) routing protocols has been optimized for ad hoc network, among all other protocol AODV is efficient for path establishment and this paper has improvised the protocol further using cryptographic technique, a solution that provides most of the security requirement. We have applied AODV protocol and the proposed cryptographic solution with amalgamation of AES, ECC, RC5, SHA-2 (AERS) to generate the asymmetric and symmetric keys to secure communication and routing along with integrity and confidentiality over cipher text in MANETs on secure AODV (SAODV). The proposed cryptographic technique is implemented through NS3 network simulation. The performance of the proposed solution was evaluated through energy consumption, packet delivery ratio of black AODV, SAODV, throughput and the AERS and the proposed solution was fast, reliable and computationally less expensive.

Keywords: *Wireless sensor networks, Routing protocol, mobile sensor, Cryptography technique, MANET*

1. Introduction

Mobile Ad-hoc Network (MANET) refers to a cluster of wireless devices that are termed as wireless nodes. The wireless nodes are known to connect dynamically which is then utilized to convey information. Wireless nodes could be anything ranging from personal digital assistants (PDAs) or it could also be personal computers such as laptops / desktops or any other kind of mobile or wireless devices for communication having wireless LAN cards [1]. Usually, any equipment used for computing which utilizes the space as medium for transmission is considered as wireless nodes. It is possible to physically attach a wireless node to an individual, an airplane, a vehicle ,which facilitates a smooth communication wireless in nature amongst them [2].

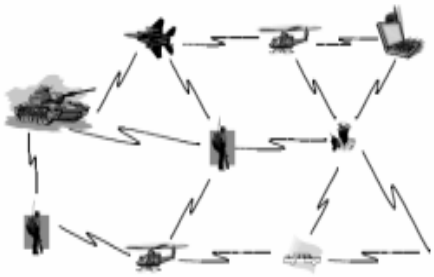


Fig. 1 Overview of Mobile Ad-Hoc Network [2].

A wireless node could either be the destination, the source or a midway node for transmission of data within MANET. Wireless nodes, when they take the role of a midway node tends to act as a router which has the capability of

BUPT

forwarding and receiving data packets to its immediate neighbors that are nearby to the target node [3]. Owing to the uncertain nature of the ad-hoc network where movement exists which are frequent within wireless nodes and do not remain continuously in a state of rest. This is instrumental to effect a change in the network's topology periodically [4].

The assumption's basis that existence of nodes within the transmission path of data can acquire information of the node within the path rather than making an assumption of the existence of connections that are stable and end-to-end [5]. Considering that the node has definitely passed through the path, the creation of connection occurs there. Taking into account the physical and social intimacy, the preciseness of choosing a node for the relay is enhanced. The findings from simulation indicate that as compared with the current algorithms for routing, the performance of data forwarding can be dynamically enhanced.

Expanding the longevity of a Wireless Sensor Network (WSN) that is heterogeneous would warrant the routing protocol for the network e considering sensors heterogeneity. Due to the traits of clustering which hinges on robustness and stability, attempts have been made to address the issues related to routing within WSN.

Networks based on MANET have to bear the brunt of attacks owing to mobile node misconduct. In brief, it can be said that MANET is devoid of any such fixed infrastructure. This network is exposed to two kinds of attacks where each one of them is classified in one of them [6]. The first kind of attack is the external attack where attackers who are not authenticated have the capability to replay routing information which is old or such types where the intention of the attacker is to create congestion or broadcast routing information that is incorrect or create disturbance within nodes and restricting them from extending services. The second kind of attack would pertain to attacks that are internal which occurs when nodes within the network are compromised. Considering the fact that nodes that have been compromised can be authenticated, it is comparatively difficult to identify internal attacks, and such attacks can lead to severe repercussions. According to the two categories of attack mentioned above, attacks experienced in the wired network could be same as its adversary which is close but may not be one amongst the trusted nodes within the network. Therefore, there is a need to explore the scope for using hybrid cryptography to secure routing networks [7].

This paper will look at designing and implementing hybrid cryptography with a view to enhance the routing protocol security in MANET. This paper presents a novel design concept of effective security solution for protection of ad hoc network from heterogeneous attack. The optimized Ad hoc-On-Demand Distance Vector (AODV) routing protocols for ad-hoc network, among all other protocol AODV is efficient for path establishment, and this paper has improvised the protocol further using the cryptographic technique, a solution that provides most of the security requirement. We have applied AODV protocol, and the proposed cryptographic solution is the amalgamation of AES, ECC, RC5, SHA-2 to generate the asymmetric and symmetric keys to secure communication and routing along with integrity and confidentiality over ciphertext in MANETs on AODV.

2. Related Works

The key performance benefits of a regular triangular structure and clustering within wired networks were presented by Kayastha[8]. In a research conducted by Johari[9] a cluster-head based election scheme for a heterogeneous network was proposed by the SEP protocol. In this, there existed sensor nodes of two kinds where it was revealed that as compared to normal nodes, high energy nodes exhibited more energy.

Vahdat and Becker[10]statethatto enhance a ratio of successful delivery of messages, the easiest manner would be to leverage the duplicate message with the help of flooding routing. Replicating the message without any limitation is considered to be a waste in bandwidth resource. According to Lin[11], this mechanism is improvised when duplicate messages are transferred to every other neighboring node right at the time of the first communication. Later, messages are directly delivered through such

BUPT

nodes directly which brings down the quantum of duplicates. However, the ratio of successful delivery is definitely affected. The tradeoff in resource utilization and the ratio of successful delivery are extensively considered by Lee and Kim[12]. The successive transfer nodes are presented with messages with a reduction in probability till such time that the message reaches the target node eventually.

2.1 Algorithms to Enhance Routing Security in MANET

Wedde[13] outlined an innovative algorithm for routing in MANET that was energy efficient. The algorithm draws inspiration from the principles of foraging as followed by honey bees. Two types of primary agents,namely scouts and foragers are utilized by the algorithm for carrying out the routing activity in mobile ad-hoc networks (MANET). The authors have termed this algorithm as 'BeeAdHoc.' This algorithm is considered as the routing algorithm with a reactive source that is known to consume less energy in contrast to the currently prevalent state-of-the-art algorithms for routing. Owing to the fact that a lower number of control packets used for routing is also comparatively lesser. The findings from comprehensive simulated experiments reveal that the quantum of energy consumed by Bee AdHoc is significantly lower in comparison with Ad-hoc On-Demand Distance Vector (AODV), Demand Signal Repository (DSR) and Destination Sequenced Distance Vector Routing (DSDV). The Bee AdHoc surpasses these routing algorithms of state –of- the art caliber without making any compromises on the conventional metrics for performance (throughput, delay and packet delivery ratio).

Ji[14] present a technique to hasten point multiplication through hybrid encryption of an improved AES-ECC system comprising of keys that are cross encrypted for a key exchange that is secure, keeping in mind the threat presented due to transmission of data on WSN. The scheme presented by the authors facilitates data encryption using AES algorithm. The AES algorithm also utilizes for private key encryption, whereas SHA -1 algorithm and ECC algorithm is implemented for digital signature generation. The massive developments that have been witnessed in VLSI technology, an FPGA design that is largely parallel are utilized within their scheme which helps improve the algorithms computing efficiency. The encryption module for AES and there is an optimization in the multi-scalar multiplication algorithm. Security protocols of ZigBee.

WSN in MAC layer was proposed by Al-Alak[15]. Security in data transfer is provided by AES 128-bit algorithm for encryption in CCM mode. Nonetheless it is possible to break the secret key of AES in the near future. In order to ensure a public key algorithm that is efficient, there is an amalgamation of ECC with AES to save the ZigBee WSN from any attacks arising out of replay as well as ciphertext. Further, it is possible for the integrity function to draw parallels with the proposed protocol to enhance the performance of the system.

Vanishreeprasad and Pushpalatha[16] state that in the present day that is rapidly progressing, one of the key concerns secure data communication Several mechanisms for security have been developed in this regard.. One such mechanism is cryptography. Cryptography pertains to scrutinizing techniques with a mathematical base which is linked with various dimensions of information security like; data integrity availability, confidentiality and Authenticity. The architecture proposed by the authors combines algorithms based on cryptography, advanced encryption standard algorithm (symmetric) as well as the hash function, SHA-2 to enhance security in data to a substantial degree.

3. Proposed Solution to Enhance Routing Protocol Security in MANET

In this section the discussion pertained to the routing and cryptographic technique used for execution of the proposed routing protocol security in MANET.

AODV routing protocols:

Generally, the role of routing protocol significant tin packet identification and transform it to the destinationfrom source node via intermediate nodes. Subsequently, the AODV is the reactive routing protocol. It provides a network connection

BUPT

which is dynamic in nature and consumes less memory, takes less processing time and share less loads. The routing message is broad cast in the network which is divided into path and path discovery. In addition, it contains the route reply (RREP), messages route request (RREQ) and route error (RERR) [17,18].

Type	Flags	Reserved	Hop count
IP address of Destination node			
Destination node sequence number			
Source IP address			
Source sequence number			

Fig. 2 RREP

Type	Flags	Reserved	Hop count
RREQ(Broadcast) id			
Destination node IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Fig.3RREQ

Type	N	Reserved	Destination count
Unreachable destination IP address			
Unreachable destination sequence number			
Additional unreachable destination IP address(if needed)			
Additional unreachable destination sequence number (if needed)			

Fig. 4 RERR

All the mobile nodes are conserved in a routing table updation of each field of content whilst getting a routing message. Furthermore, the fields are associated with RREP, RREQ and RERR. The pictorial representations of these fields are discussed in figure 2, 3, 4 and 5.

Destination IP address
Destination sequence number
Hope-count
Next-hop
First-hop
Valid bit
Count

Fig. 5 Fields of SAODV Routing Table

At the point when a source node has to send information to destination node, first, check in the source node steering table, if destination node address straight forwardly is exhibited and if discovered an RREQ message will be communicated to entire neighborhood hubs. In the system, the refresh course table which receives the RREQ from the moderate transitional hub decides if the moderate hub is a destination to receive RREP packet or else that hub re-communication of RREQ message to a neighbor thatsteps rehash, until that destination hub is discovered. In the event that discovered destination hub at that point produces RREP packets it is sent to the source. In AODV steering convention directing procedure must be founded on grouping number.

3.1 Overview of proposed cryptographic technique

The proposed cryptographic solution is the amalgamation of AES (Advanced Encryption Standard), ECC, RC5, SHA (Secure hash algorithm)-2 for generation of the asymmetric and symmetric keys to ensure secure communication and routing along with integrity and confidentiality over ciphertext in MANETs on AODV.

3.1.1 Advanced Encryption Standard (AES)

the National Institute of Standards and Technology (NIST) in December 2001 published the symmetric block cipher ,the AES method. This algorithm works by accepting a block size of 128 bits and a choice of three keys such as 128,192,256 bits. A number of AES parameters depend on the key length. For instance, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14

BUPT

for 192 and 256 bits respectively.currently , the most common size of the used is the128-bitkey[19]. The algorithm design was based on the features such as Speed and code compactness, resistance against all existing attacks and simplicity of Design.

3.1.2 Elliptic Curve Cryptography (ECC)

The identity of a node is used for public key generation, secure AODV, ECC, and bilinear pairing were used to generate the private key interactively and symmetric session keys non-interactively[20]. ECC is used due the high level of -security l with smaller key size[19]. Short keys are provided from ECC to mobile nodes and high- level of security. To prevent adversaries attack Key generation and key distribution security services are done by (t, n) threshold secret sharing algorithm. ECC provides an enhanced security level by using A Key of size 160 bits and 1024 bits equivalent strength of RSA are utilized by ECC to provide enhanced level of security. Pairing of technology ensures confidentiality and authentication with lower computational cost and reduced communication overhead[21]. Further, the RC5 to provide confidentiality over ciphertext and message digest[22].

3.1.3Secure Hash Algorithm-2 (SHA-2)

SHA-2 i comprises a set of cryptographic hash functions which derive the names as s SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 designed through the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS).SHA-2 is a hashing algorithm that computes the fixed length digits of theoriginal message or a test or a data file. The receiver also computes message digest The computed message digest from the receiver through the SHA-2 algorithm and comparison is done with the message digest it has received. SHA-2 has a high security levelbecause it is difficult to find an original message that corresponds to a particular message digest or two messages with the same message digest. If there is a message change during transmission, there is a change in message digests and the failure of signature verification t indicate that message has been modified. Since SHA-2 is also irreversible, given a message digest, it is computationally difficult to find the original message. SHA-2 is widely used in a number of security applications electronic fund transfer, electronic mail, software distribution, data storage and other application which require assurance of data integrity and authenticity of data origin [19].

4 Experimental results

4.1 Experimental setup

The configuaration of the computer system that was used to compile NS-3 and to run the simulation are presented in Table1, and the NS-3 simulation parameters used in our experiments are listed in Table 2.

Table 1: System Configuration

Processor	Intel® Core ™ Duo CPU 2.1 GHz
Operating System	Linux, Ubuntu 12.04 lts
Memory	2GB
C++ Compiler	gcc version 4.3.0
NAM version	3.104
Simulation version	NS3.19

Table 2: Simulation Parameters in NS-3

Parameter	Value
Simulator	NS-3.19
MAC Layer	Network Layer
Simulation Time	100 sec
Simulation Area	300*600
Transmission Range	200 meter
Routing Protocol	AODV, Secure AODV
Packet Size	512 bytes
Number of Nodes	50 Nodes
Network size	1000*700
Simulation duration	100
Initial Energy	10 j
Source node	1,4,8,13
Destination node	50,42,38

BUPT

Node size	10

The performance cryptographic technique implemented in the Ad hoc network relies on several factors. These are discussed as follows:

4.2 Parameters used

4.2.1 Throughput

Throughput is a measure amount of data transferred successfully from one place to another. It also defined as

$$Thoughtput = \sum_i \frac{P_d}{P_a - P_s}$$

Where P_d - packet delivered, P_s- packet start time and P_a- packet arrival rate

4.2.2 End to end delay time

In our study, the End-to-End delay time is a measure of time interval from the moment that the source node sends the first packet of data after completion of encryption procedure n until the moment that the destination node in the network receives the last encrypted packet.

4.2.3 Packet loss

Packet loss is difference between the total number of packets transmitted and the number of packets received at Access Point [23].

$$\text{Packets loss} = \sum \text{Packets transmitted} - \sum \text{Packets received}$$

$$\text{Packet loss ratio} = \frac{(Packetslosts * 100)}{\sum Packetstransmitted}$$

4.2.4 Packet Delivery ratio

The ratio of number of transmitted or sent data packet sends to the number of received data packet in the destination is termed as packet delivery ratio (PDR). This parameter is a measure of effectiveness of protocol to deliver the packet to the destination[24]. The large value of PDR indicates superiority of proposed algorithm. The mathematical representation of PDR is defined as,

$$PDR = \sum_i \frac{PD}{PS} * 100$$

Where PD-Packet delivery, PS- packet send, i^{th} packet

5. Results and Discussion

The proposed algorithm demonstrated the performance using NS3 simulation software.The specific simulation parameter and system configuration of proposed method are discussed in table 2 and 3. Moreover, evaluation of performance of proposed ad-hoc network measured under different parameters like energy consumption, throughput, and ratio of packet delivery. the performance of different protocols havebeen compared by considering a several number of simulations. The following results compared the performance characteristics of AODV in a simulated environment. The practical networks contain a significant number of malicious nodes, and their effects need to be countered. The results are exhibited in following figures.

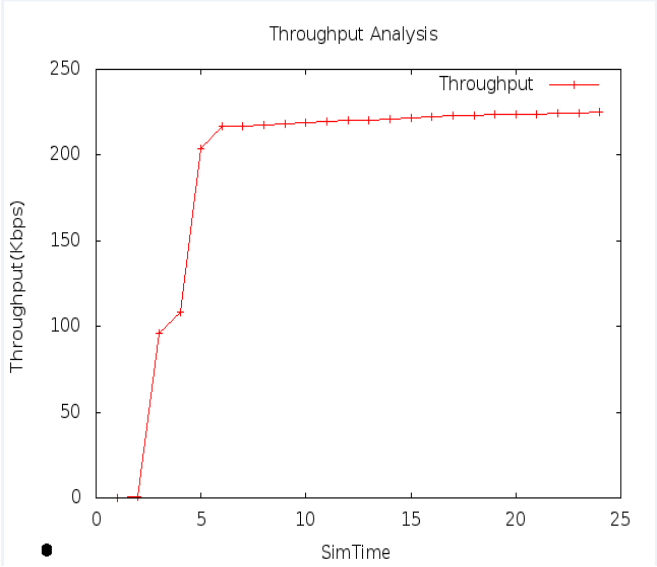


Fig. 6 Throughput analysis

The figure 6 illustrated the comparison done f for the proposed, basic AODV, SAODV and AERS

BUPT

in terms of throughput. the experimental results show

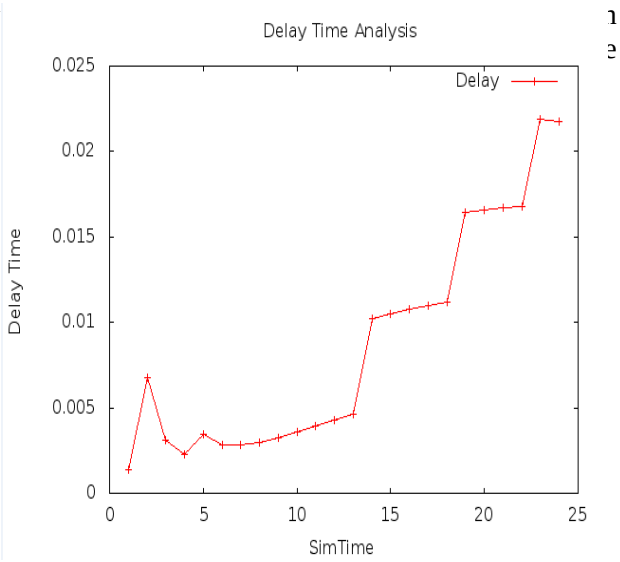


Fig. 7 Delay time analysis

The figure 7 shows the delay of the proposed, basic AODV, SAODV and AERS is done in terms of delay time analysis. The analysis show that delay of the proposed technique is least in comparison with the other three ad-hocnetwork.

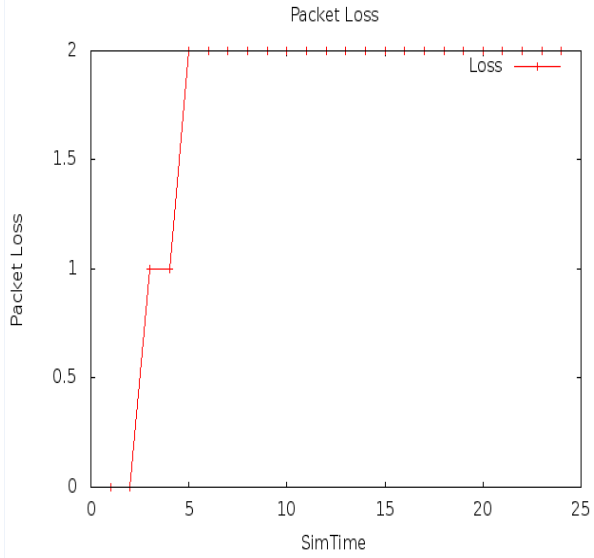
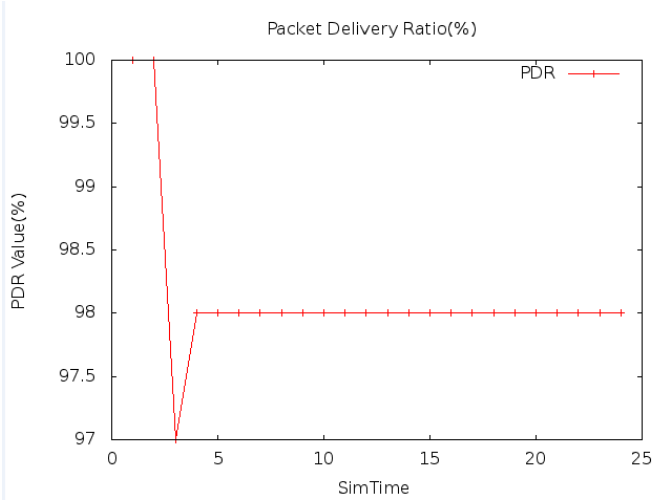


Fig. 8 Packet loss

The figure 8 illustrates the comparison carried out in terms of packet loss on the proposed, basic AODV, SAODV and AERS is done in terms of packet loss. The experimental results prove that the



packet loss is less as compared to the other three approaches.

Fig. 9 Packet delivery ratio

Table 3: Performance evaluation

Parameter	AODV	SAODV	AERS
Energy consumption	22 j	19 j	17.9 j
Throughput	182.9kbps	189kbps	283kbps
Packet delivery ratio	94.89%	95.71%	98.99%
Delay time analysis	0.70sec	0.72 sec	0.74sec
Packet loss	24%	23%	20%

The figure 9 illustrated the comparison is done of the proposed, basic AODV, SAODV and AERS is done in terms of packet loss. The experiment reveals the superior performance of proposed method which is depicted by large values obtained

6. Conclusion

In this paper, the application of AODV protocol and proposal of cryptographic solution is the amalgamation of AES, ECC, RC5, and SHA-2

BUPT

towards generate the asymmetric and symmetric keys to secure communication and routing along with integrity and confidently over ciphertext in MANETs on AODV. The proposed cryptographic technique is implemented through NS3 network simulation. The performance of the proposed solution was evaluated through energy consumption, throughput, ratio of packet delivery of black AODV, SAODV and the AERS and that proposed was fast, reliable and computationally less expensive. On the other hand, the proposed method enhances the performance of proposed AODV routing protocol. Further the experimental evidence shows that the increased throughput performance; decreased network delay as well as reduced packet loss.

References

1. Aggarwal, D.: A Study On The Role Of Mobile Adhoc Networks (MANETS) In Disaster Management. Int. J. Adv. Res. Comput. Sci. 8, (2017)
2. Sivamurugan, D., Raja, L.: Secure routing in manet using hybrid cryptography. Int. J. Res. - Granthaalayah. 5, 83–91 (2017)
3. Sugumar, R., Hussain, S.J.: The Enhanced Network Architecture , Route discovery and Data Transmission of AODV. Int. J. Pure Appl. Math. 116, 453–460 (2017)
4. Kriplani, S., Kesharwani, R.: Malicious Nodes Identification and Classification of Nodes and Detection of UDP Flood Attack with ICMP using OLSR Routing Protocol in MANET. Int. J. Sci. Res. Sci. Eng. Technol. 1, 90–94 (2016)
5. Wu, Y., Zhu, Y., Yang, Z.: Routing algorithm based on ant colony optimization for mobile social network. In: 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). pp. 297–302. IEEE (2017)
6. Wadhwa, M., Sethi, A.: A Review on Various Attacks in Manets. Int. J. Comput. Sci. Netw. 3, 282–284 (2016)
7. Pawar, M. V., Anuradha, J.: Network Security and Types of Attacks in Network. Procedia Comput. Sci. 48, 503–506 (2015). doi:10.1016/j. procs.2015.04.126
8. Kayastha, N., Niyato, D., Wang, P., Hossain, E.: Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey. Proc. IEEE. 99, 2130–2158 (2011). doi:10.1109/ JPROC.2011.2169033
9. Johari, R., Gupta, N., Aneja, S.: DSG-PC: Dynamic Social Grouping Based Routing for Non-uniform Buffer Capacities in DTN Supported with Periodic Carriers. In: Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. pp. 1–15.
10. Springer, Berlin, Heidelberg (2013)
    Vahdat, A., Becker, D.: Epidemic routing for partially connected ad hoc networks. Tech. Rep. number CS-200006, Duke Univ. 1–14 (2000). doi:10.1.1.34.6151
11. Lin, Y., Zhang, J., Chung, H.S.-H., Ip, W.H., Li, Y., Shi, Y.-H.: An Ant Colony Optimization Approach for Maximizing the Lifetime of Heterogeneous Wireless Sensor Networks. IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev. 42, 408–420 (2012). doi:10.1109/TSMCC.2011.2129570
12. Lee, J.-W., Kim, W.: Design of Randomly Deployed Heterogeneous Wireless Sensor Networks by Algorithms Based on Swarm Intelligence. Int. J. Distrib. Sens. Networks. 11, 690235 (2015). doi:10.1155/2015/ 690235
13. Wedde, H.F., Farooq, M., Pannenbaecker, T., Vogel, B., Mueller, C., Meth, J., Jeruschkat, R.: BeeAdHoc: an energy efficient routing algorithm for mobile ad hoc networks inspired by bee behavior. Proc. 2005 Conf. Genet. Evol. Comput. 153–160

BUPT

(2005)

14. Ji, B., Wang, L., Yang, Q.: New Version of AES-ECC Encryption System Based on FPGA in WSNs. J. Softw. Eng. 9, 87–95 (2015). doi:10.3923/jse.2015.87.95
15. Al-Alak, S.., Ahmed, Z.., Abdullah, A.., Subramiam, S..: AES and ECC mixed for ZigBee wireless sensor security. World Acad. Sci. Eng. Technol. 81, 535–539 (2011)
16. Vanishreeprasad, S., Pushpalatha, K.N.: Design and Implementation of Hybrid Cryptosystem using AES and Hash Function. IOSR J. Electron. Commun. Eng. Ver. II. 10, 2278–2834 (2015). doi:10.9790/2834-10321824
17. Sharma, A., Bhuriya, D., Singh, U., Singh, S.: Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing. Int. J. Comput. Sci. Inf. Technol. 5, 5201–5205 (2014)
18. Liu, K., Deng, J., Varshney, P.K., Balakrishnan, K.: An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs. IEEE Trans. Mob. Comput. 6, 536–550 (2007)
19. Zalte, S.S., Ghorpade, V.R.: Secure Token for Secure Routing of Packet in MANET. Int. J. Comput. Sci. Inf. Technol. 5, 6916–6919 (2014)
20. Mahesh, K.K.., Sunitha, N.., Mathew, R., Veerayya, M., Vijendra, C.: Secure Ad-Hoc On-Demand Distance Vector Routing using Identity Based Symmetric Key Management. In: This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference. pp. 1–7. IEEE (2016)
21. Xiong, W.A., Gong, Y.H.: Secure and Highly Efficient Three Level Key Management Scheme for MANET. WSEAS Trans. Comput. 1, 6–15 (2011)
22. Agrawal, A., Patankar, G.: Design of Hybrid Cryptography Algorithm for Secure Communication. Int. Res. J. Eng. Technol. 3, 1323–1326 (2016)
23. Tyagi, P., Dembla, D.: Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egypt. Informatics J. 18, 133–139 (2017). doi:10.1016/j.eij.2016.11.003
24. Mandhare, V.V., Thool, V.R., Manthalkar, R.R.: QoS Routing enhancement using metaheuristic approach in mobile ad-hoc network. Comput. Networks. 110, 180–191 (2016). doi:10.1016/j.comnet.2016.09.023

BUPT