Circuits and Systems, 2016, 7, 350-359
Published Online April 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.74030

Dual Authentication Hashing for Security Enhancement in MANET

L. Raja, Dr. P. S. Periasamy

Department of ECE, KSR College of Engineering, Tiruchengode, Tamilnadu, India
Email: rajabvni@gmail.com

Received 11 March 2016; accepted 25 April 2016; published 28 April 2016

Abstract

Mobile Ad hoc Network (MANET) is a collection of mobile hosts with wireless interfaces that form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. The dynamic and cooperative behaviour of ad hoc networking without any centralized or unified controlling authority for authentication and monitoring is sensitive to attacks that damage or exploit the cooperative behaviour of ad hoc routing. Routing attacks lead to the most disastrous damage in MANET. The main objective of this paper is to enhance the security against routing attacks in MANETs. Intrusion detection based on DAHT (Dual Authentication Hash Technique) entirely depends on the end to end communication between the source and destination is employed here. The proposed technique identifies the misbehaving nature of current node and the previous node where it receives the information. DAHT is simulated with various parameters in NS2. The results obtained are compared with existing mechanism. The results show that malicious detection, overhead reduction and delay are better when compared to the existing system that is employed in protecting the routing information.

Keywords

MANET, Dual Authentication Hashing Technique (DAHT), Security, Routing Attacks, Digital Signature

1. Introduction

For more than a decade, mobile ad hoc networks have found considerable interest as an area of research. An attention-grabbing and complicated issue associated with ad hoc networks is its potential usage in areas where a

How to cite this paper: Raja, L. and Periasamy, Dr.P.S. (2016) Dual Authentication Hashing for Security Enhancement in MANET. *Circuits and Systems*, **7**, 350-359. http://dx.doi.org/10.4236/cs.2016.74030

required infrastructure support that is available in traditional networks no longer exists. Some applications include, an isolated remote space, a disaster affected area and virtual classrooms, etc. All the individual nodes associated with the ad hoc network are fully responsible for running the network services, implying that each and every individual node in the network co-jointly functions as a router so as to forward the packets to their destination. It's a hectic task for researchers to provide a comprehensive security for ad hoc networks with particularized quality of service from all of its potential threats [1]. It becomes even tougher when the collaborating nodes are mostly less powerful mobile devices.

A MANET with desired characteristics described above was initially developed entirely for military purposes, as nodes are speckled over a battlefield and there is no specific infrastructure to help them to form a network [2]. In the years that followed, MANETs were developed rapidly and have found increased usage in many applications, transforming from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or human interaction. Some examples are search and rescue missions, data collection, virtual classrooms and conferences where laptops, Personal Digital Assistant (PDA) or other mobile devices share wireless medium and communicate between each other. As MANETs have been used widely, the security issue has been looked as one of the primary concerns. For example, most of the existing routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. There are possibilities for the nodes in the network to be malicious or selfish. Therefore, even a single compromised node can lead to failure of the entire network.

2. Routing and Security

In ad hoc networks, each node acts as a router. Routing is the process of selecting path in a network along which to send network traffic. A specific set of communication rules by which nodes can communicate with each other is a protocol. Routing protocol specifies how routers can communicate with each other. It use metrics to find which path is best for the packet to travel in the network Metrics is the stand of measurement like Bandwidth, Delay, Reliability and current load on the path. Establishing a valid, efficient and secure route between a pair of node is the goal of the routing protocol so that messages are delivered in a timely manner. Routing protocols are generally classified into three types [3].

i) Proactive Routing Protocols
ii) Reactive/Ad Hoc Based Routing Protocols
iii) Hybrid Protocols

2.1. Proactive or Table Driven Protocol

In Table driven routing protocol, every node maintains the network topology information in the form of routing table. It periodically exchanges routing information. Routing information is generally flooded in the network. Whenever node requires path to destination, it runs appropriate path finding algorithm. Frequent update of routing table results in high routing overhead. In this type of routing protocol, each node should maintain at least one table to store the routing information.

2.2. Reactive or on Demand Routing Protocol

Routing protocols under this category do not maintain network topology information. Here, the routing protocols create routes only when requested by the source node. A route discovery process is initiated by the source node. These routing protocols do not exchange routing information periodically. Once the route is established, it will be maintained by route maintenance procedure until either the destination becomes inaccessible or the route is no longer desired.

2.3. Hybrid Protocols

Combination of proactive and reactive is hybrid protocol. To overcome the drawbacks in proactive and reactive protocol it is used. It reduces the control overhead of proactive routing protocol and delay which occur due to initial route discovery in reactive routing protocol. Nodes within a certain distance from node concerned or within particular geographical region are said to be within routing zone of given node. For routing within zone, table driven approach is used and for routing beyond zone on demand approach is used.

2.4. Security

One of the primary and most important concerns associated with ad hoc networks is to provide a secure and reliable mode of communication among the mobile nodes in a hostile environment [4]. The nature of mobile ad hoc networks poses a wide range of threats to the security. These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. This is the area where the MANET faces the main problem *i.e.*: the ad hoc networks can be reached very easily by users and malicious attackers. If a malicious attacker approaches the network, they easily may exploit or even disable the mobile ad hoc network. Conventional methods of identification and authentication [5] are not applicable since the availability of a Certificate Authority or a key Distribution Center cannot be assumed to be available.

Considerable improvements have been formulated relating to different characteristics of MANETs that focuses on the fields related to routing protocols, clustering protocols, locations and mobility predictions. However, the security aspects of MANETs have been rarely addressed. The security [6] attributes of MANET is shown in the **Figure 1**.

- **Confidentiality** is to keep the information sent unreadable to unauthorized users or nodes.
- **Authentication** is to be able to identify a node or a user, and to be able to prevent impersonation.
- **Integrity** is to be able to keep the message sent from being illegally altered or destroyed in the transmission.
- **Non-repudiation** is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it.
- **Availability** is to keep the network service or resources available to legitimate users.

3. Related Work

Kejun Liu *et al*. [7] proposed the Two Acknowledgement (TWO ACK) scheme to mitigate the undesirable effects of misbehaving nodes. The basal idea of the TWO ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called TWO ACK which indicates that the data packet has been received successfully. Such a TWO ACK transmission occurs only for a fraction of data packets, but not all. Hence a "selective" acknowledgment is anticipated to reduce the increased routing overhead caused by the TWO ACK scheme. The behavior of the node is judged only after observing its behavior for a certain period of time. In this paper, they present the details of the TWO ACK scheme and their assessment of the 2ACK scheme as an add-on to the Dynamic Source Routing (DSR) protocol.

Balakrishnan *et al*. [8] proposed a network-layer scheme called TWOACK, which is implemented as a simple extension to any source routing protocol such as DSR. When a node forwards a packet, the nodes routing agent verifies that the packet is received successfully by the node that is two hops away on the source route. This is done through the use of a special type of acknowledgment packets, described as TWOACK packets. TWOACK packets have very similar functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer. A node acknowledges the receipt of a data packet by sending back a two-hop TWOACK packet *al*ong the active source route. If the sender/forwarder of a data packet does not receive a TWOACK packet cor-

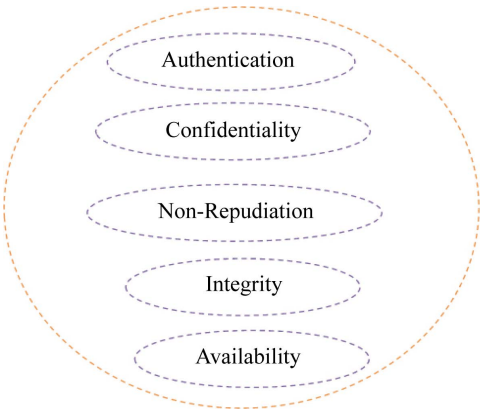

Figure 1. Cryptography based hard security services.

responding to a particular data packet that was sent out, the next-hop's forwarding link is claimed to be misbehaving and the forwarding route is broken. Based on this claim, the routing protocol avoids the accused link in all future routes, resulting in an improved overall throughput performance for the network. The S-TWOACK (Selective-TWOACK) scheme is a derivative of the basic TWOACK scheme, aimed at reducing the routing overhead caused by excessive number of TWOACK packets. They discuss their schemes in the framework of the DSR protocol as an example of source routing schemes. The operation of the TWOACK schemes when used with other source routing schemes is similar.

Syeda Iffat Naqvi, *et al*. [9] proposed a method that improves the strength of Hash Message Authentication Code (HMAC), so that its resistance increases against the birthday attack and the exhaustive key search attack. The Secret key which has been used in the calculation of HMAC is public to the sender and the receiver. They generate the key by using a pseudorandom Message Digest 6 (MD6) hashing functions so that it becomes more sheltered and hard to envisage by a forgery. HMAC uses a cryptographic hash function denoted by h, and the secret key k. Authors assumes h as a hash function in which data stream is hashed by repeatedly applying a fundamental compressing function on data divided in to l blocks where l is the number of blocks in m after being padded. The length of these blocks in bits is denoted as b (where l*b is the length of padded message m in bits), and the length of hash result in bits by n (for Message Digest 5 (MD5) n = 128 bits, for SHA-l n = 160 bits and n = S12 bits for MD6). The length of the key K could be up to b, equal to the block size of the hash function. Those applications which use the key larger than b bits will initially compress key by using h and later on uses the resulting n bit string as the tangible key for HMAC. For any situation the minimum suggested length for K is n bits (equal to the length of the hashed output).

P. Kiran Rao, *et al*. [10] used secure Hash Algorithm-1 (SHA-1) in ad hoc networks to guarantee the integrity. By using SHA-1 algorithm authors believe that hash value could to protect the hop count. To the hop count field, hashed value are send along with the packets, by this the node which forward the false routing information *i.e.* malicious node can be defended effectively. CA-AOMDV (Channel Aware ad hoc multipath distance vector routing) protocol is proposed in this to achieve secure routing in MANET. SHA-1 is used to detect man-in-the-middle attack in MANET.

Vanesa Daza *et al*. [11] proposed cryptographic techniques to set up a secure mobile ad hoc network. The entire process is self-managed by the nodes themselves, without any trusted party. New nodes are able join the network and can obtain the same capabilities as initial set of nodes; further, every individual node obtains a pair of secret/public keys to secure and authenticate its communication. Two extended features of this system are, it permits the implementation of threshold operations (signature or decryption) involving subgroups of nodes in the network and that any subgroup with a small number of nodes can obtain a common secret key without any communication after the set up phase. The first property is attained by the use of secret sharing techniques. The second property is derived from the usage of symmetric bivariate polynomials to allow dynamic sets of nodes. The third property is the abstention of individual secret/public keys, they propose two possibilities, depending on the type of scenario where these keys are going to be used. Authors believe that interesting extensions can be done to the threshold cryptography. Suppose the MANET is splitted into different subgroups of nodes based on some common characteristics (for example, members of the same team in multiplayer computer games). Then it exhibits how it can be extended to allow threshold decryption; that is, a message intended for a certain group SG can be decrypted only if enough number of nodes in subgroup cooperate.

Elhadi M. Shakshuki *et al*. describes an intrusion-detection system termed as Enhanced Adaptive AC Knowledgment (EAACK) [12] specially designed for MANETs. This system is primarily designed to overcome three of the six flaws of Watchdog method namely false misbehavior, limited transmission power and receiver collision, *i.e*. it detects packet dropping attack. The three main and essential parts of the proposed system are Acknowledgment (ACK), Secure-ACK (SACK), and Misbehavior Report Authentication (MRA) along with the Digital signature technique. ACK is typically an end-to-end acknowledgement scheme. S-ACK is an improved form of TWOACK scheme. The sink node needs to send back an acknowledgement packet to its corresponding source node. If this source node does not receive any ACK packet then the system switches to S-ACK. Detecting the misbehaving nodes is the primary function of S-ACK. In this detection, authors consider a group of three nodes (N1, N2, and N3); the data is sent in the sequence of N1 → N2 → N3. Now N3 has to send the ack back to N1. If node N1 doesn't receive any ack from node N3 within a particular time then nodes N2 and N3 are considered as misbehaving nodes. The Misbehavior Report Authentication (MRA) scheme is designed to resolve the problem of identifying the misbehaving nodes with the presence of false misbehavior report. Here RSA and

DSA digital signature schemes are employed as mechanisms to ensure security.

Drawbacks

From the above survey it is observed that node false misbehavior plays a vital role. Those mechanisms mentioned above ensures security but at the cost of increased overhead and delays. The digital signature technique that is used can delay or prevent the exchange of routing information which may lead to reduced routing effectiveness, and also may consume excessive network or node resource, that leads to many new chances for possible Denial-of-Service (DoS) attacks through the routing protocol. DSA provide security to MANET with large delay and overhead. Signature file size and key size is around 89 byte and 1024 bits respectively and output size is very large.

4. Proposed System

In our proposed method a secured routing mechanism called the Dual Authentication Hashing Technique is employed to protect the routing packets instead of digital signature. Here it is assumed that no two compromised nodes are colluding and are within two hops of each other. In the initialization phase, a common secret is distributed among the two hop node group through management of the local node group.

4.1. Dual Authentication Hashing Technique

The digital signature technique is expensive and can produce huge overhead. But the security mechanisms of DAHT are sufficient. At the same time each node can detect its neighboring nodes malicious behavior immediately. In this approach, each node needs to distribute a common secret shared by its two-hop node group [13]-[15]. For example source node needs to distribute secret key K to its two-hop node. This secret key has to be maintained as secret, and the distribution is based on PKI. Each individual node in the ad hoc network has a digital certificate signed by CA, *i.e*. each of these nodes has a pair (public key, private key), and the public key is widely known. The security mechanism of DAHT use key size of 160-byte. It has no signature file size and the output size is less (when combined with MD5). The RREQ packets are authenticated with two hash values which are used to check whether the received routing packet has been modified and to prevent the current node from modifying the packet. The cryptographic hash function [6] used here takes as a message of arbitrary length as input and generates as output a 128-bit (16 byte) message called digest also termed as MD5 hash or checksum which is used to check data integrity.

Two local node groups are maintained by each node in ad hoc network. First group includes nodes within one-hop range (1-H) and Second group includes nodes within two-hop range (2-H) except the nodes in first group as shown in **Figure 2**.

The nodes resides in each other's radio range can exchange their information with its first group so that it can learn about the second group. Instead of digital signature to authenticate routing information Hash function is adopted. It is fast and efficient under the assumption that colluding between two compromised nodes is not possible and included that is within two hops of each other. Considering Dual authentication of hashing, one authentication is used to authenticate routing packets which are received and second is used to prevent routing information which is modified by the current (node ready to transmit) nodes.

Initial stage of this mechanism is to distribute common secret key to second group by makes use of local node group. Source node distribute secret key (K_s) to 2-H without the knowledge of 1-H. This distribution is based on PKI that is public key infrastructure. Each node in the network has public key and private key which is known globally and which is kept secret. Nodes in the 2-H receives the source generated key. Timely adjustment in the distribution of common secret key is applicable for two cases.

Case 1: S also needs to distribute k_s to the nodes which are newly joined to 2-H.

Case 2: S needs refreshing and redistributing k_s, if nodes in 2-H become the number of nodes in 1-H.

DAHT mechanism is explained in various steps

Node S in 1-H group will have

O_s = {A,B,C,D,E} through exchanging 1-H node with neighboring nodes, S can learn

O_A = {S,E,F,G}, O_B = {S,C,H,I,J}, O_C = {S,B,D,J,K}, O_D = {S,C,E,L}, O_E = {S,A,M}

Then S can get its 2-H node group,

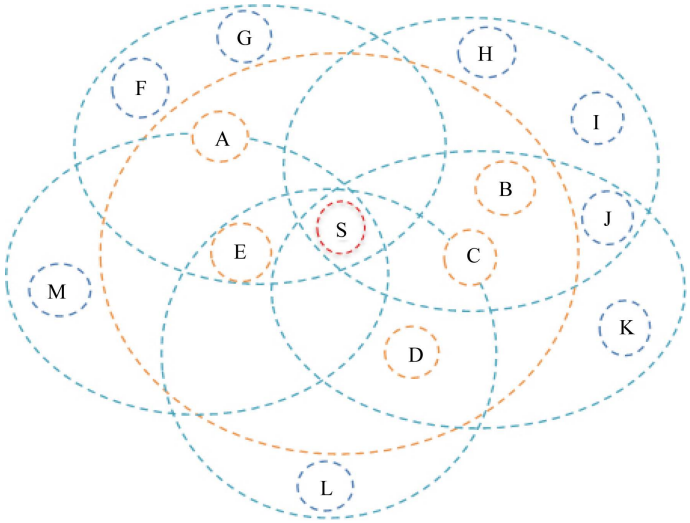

Figure 2. One hop and two hop node group from source node.

$$T_s = (O_A \cup O_B \cup O_C \cup O_D \cup O_E) - O_S - \{S\}$$
$$= \{F,G,H,I,J,K,L,M\}$$

Each node must maintain its local node group timely due to mobility of ad hoc networks,

H (.) Public one way hash function used to authenticate the RREQ twice. So packet not only include RREQ and also two hash value (A_1,A_2)

A_1, A_2 Two hash value

A_1 To prevent the current node modifying packet

A_2 To check whether the received routing packet is modified

Step 1: Source S generate RREQ ={ID_f, SN, HC, M} Where,

ID_f - Identity of forwarding node

SN - Sequence number of the RREQ

HC - Hop count

M - Original message

Step 2: Source node multicast {ID_f, SN, HC, M, A_1, 0} to 1-H

Any x node in 1-H receives and identify as A_1 = H (ID_f, SN, HC, M, K_s) and A_2 = 0 (initially).

Before forwarding to 2-H, x node in the 1-H it increases the hop count value and copy A_2 from A_1 and calculate new hash value, *i.e.* A_1 = H (ID_f, SN, HC + 1, M, K_x) and A_2 = H (IDf, SN, HC, M, K_s).

Where, K_s is the secret key share by S and 2-H and K_x is the common secret key between node x and its 2-H node group T_x.

Step 3: 1-H multicast {IDf, SN, HC + 1, M, A_1, A_2} to 2-H

In 2-H, the node which belongs to Z_x (*i.e.* only in 2-H but not included in 1-H) on receiving {ID_f, SN, HC + 1, M, A_1, A_2} use {ID_f, SN, HC + 1, M} and Hash functions A_1 and A_2,. Where, A_1 = H (ID_f, SN, HC + 1, M, K_x) and A_2 = H (ID_f, SN, HC, M, K_s) to calculate H (ID_f, SN, HC, M, K_s) and compare with A_2. From this accordingly validate whether the routing packet was modified by the node x.

Step 4: If x node in 1-H wants to modify the packet before forwarding to 2-H. It has to forge A_2. Since x belongs to 1-H it doesn't know about the K_s secret key shared by S and T_s. under this hash function is cryptographically secure and misbehavior of node x can be detect by the nodes within Z_s.

4.2. DAHT with MD5

Every time when a node originates RREQ, RREP or RERR message is generated. The concept of DAHT with MD5 is explained with the following steps:

1. Choose appropriate value of hash function h that is to be used to make message digest.
2. Set Hash_Function field by using h. Hash_Function = h, where, h is the value of hash function.
3. Get the value of Secret Key, from PKI system and add it to values of all the fields of message.

4. Add two hash values A1 and A2 to RREQ packet.
5. Set A2 = 0 (initially), A1 = H (IDf, SN, HC, M, K_s).
6. Calculate Message_Digest by passing the values of all the fields with secret key to hash function h. Message Digest = h (values of all the fields with added secret key), where, h is a hash function.
7. Broadcast RREQ packets with these A1 and A2 values to one-hop node group.
8. One-hop node group checks these A1 and A2 values to verify the authenticity of packet.
9. Obtain the value of Secret Key, and add it to values of all the fields of received message.
10. Applies the hash function h to the values of all the fields of received message with added secure key.
11. Verify that the calculated message digest is equal to the value contained in the Message_Digest field of received message.
12. Before rebroadcasting RREQ find new hash values using secret key and perform the same.

The flowchart of the security mechanism is given in the **Figure 3**. This system is well capable of detecting routing attacks mainly impersonation, hop-count modification, packet dropping, RREQ fabrication in MANET in an efficient manner. DSR (Dynamic Source Routing) is used as the routing protocol here. The system performance is compared with other routing protocol AODV.

5. Results and Discussions

Two security mechanisms *i.e*. Digital Signature Algorithm and DAHT are compared and results are obtained here. In this set of simulation we consider a set of 50 nodes that are randomly deployed in flat space with a size of 670 × 670 m^2. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512B. Transmission range of nodes is set to 200 m. Here we consider various performance metrics.

Packet Delivery Ratio (PDR): PDR can be defined as the ratio of packets received at the destination node to the number of packets sent by the source node. Both security schemes provide the same packet delivery ratio. In both the cases, as the number of malicious nodes increases the value of PDR decreases as shown in **Figure 4**. As the number of malicious nodes increases, more packet drops occurs, more message modifications occur and thus the number of packets reaching the destination decreases. Both the schemes provide more or less the same security.

Routing Overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERR or (RERR)] to the amount of data transmissions.

In both these schemes the routing overhead increases as the number of malicious nodes increases as shown in **Figure 5**. Less routing overhead is employed in DAHT when compared to DSA technique. In DSA, keys and signatures have to be generated along with the input message. This results in large output size and the processing power consumption is high. But in DAHT no signature files are generated only two hash values are added to the route request packets.MD5 hash function is used and output size is around 128 bits only. Hence RO is less for DAHT when compared to DSA.

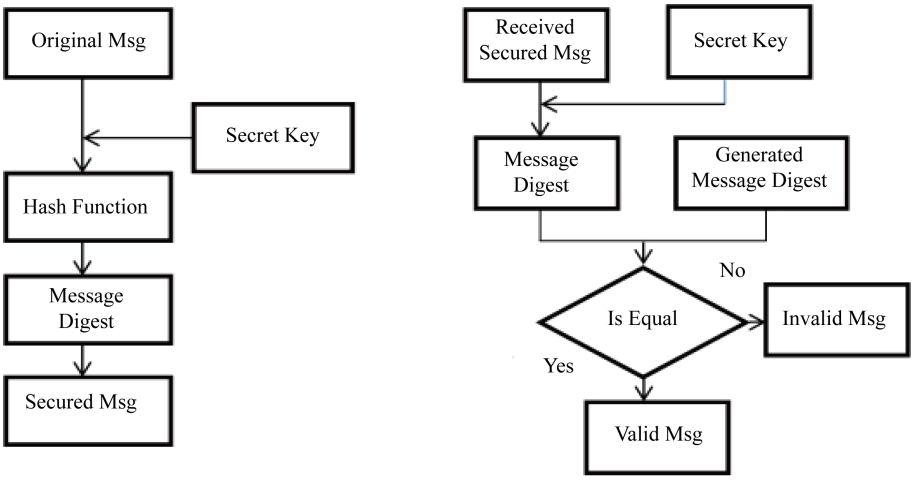

Figure 3. MD5 with secret key.

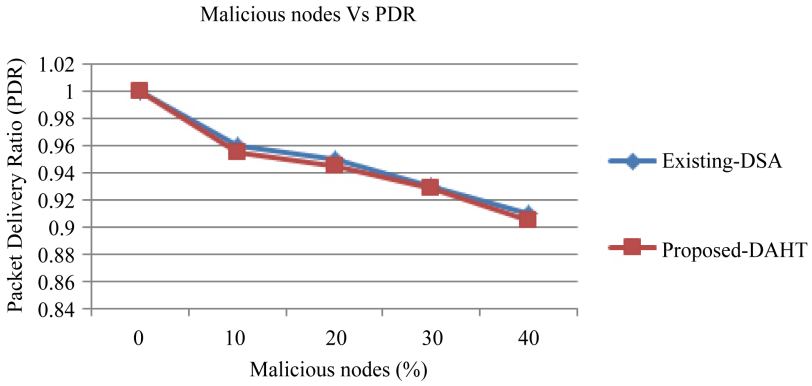

Figure 4. Comparison of existing system and proposed system in terms of packet delivery ratio.

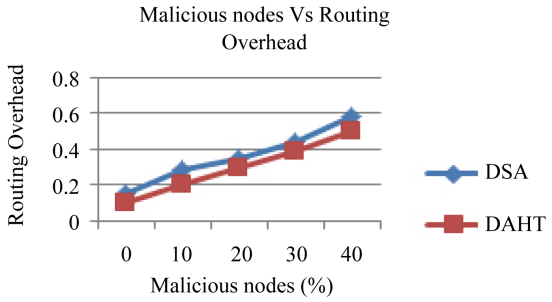

Figure 5. Comparison between existing system and proposed system in terms of routing overhead.

Here as the number of malicious nodes increases the delay increases as shown in **Figure 6**. In the proposed system the delay is reduced when compared to that of the existing system, since the processing time required for DAHT is less. In the existing system, DSA technique is used where signature files are generated along with input messages and its encoding and decoding consumes more time.

Here the performance metric PDR is calculated for the DAHT technique using two protocols DSR and AODV as shown in **Figure 7**. DSR protocol has higher PDR compared to AODV protocol. In both DSR and AODV, PDR decreases as the number of malicious nodes increases.

DSR protocol exhibits higher end-end delay compared to AODV protocol. AODV protocol is loop free and hence has lesser delay. In both, these protocols end-end delay increases as the number of malicious nodes increases as shown in **Figure 8**.

Here the performance metric end-end delay for the DAHT technique is compared for different number of nodes. The delay increases as the number of nodes increases. Since the delay is calculated with number of malicious nodes, higher the number of malicious nodes in the network, higher the processing time required and also more time is required for transferring greater number of advertisement packets. Hence this result in increased delay as the number of nodes gets increased.

6. Conclusion

Here the two security mechanisms DSA and DAHT are compared for different protocols. Both these mechanisms ensure reliable security with high malicious detection rate. These systems are capable of preventing the routing attacks in MANETs very effectively. DAHT also provides less routing overhead and delay compared to DSA. So DAHT is considered as a better technique to ensure security in MANETs. Further this work can be extended to prevent Denial of Service (DoS) and other attacks. The proposed DAHT identifies the intruder who modifies packet and isolates it from the routing path. In the future, the temporary and permanent isolation of nodes can be considered so that delay can be reduced further.

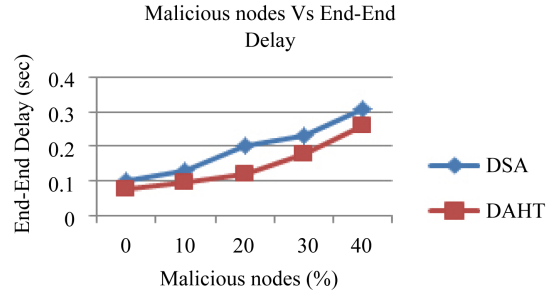

Figure 6. Comparison between existing system and proposed system in terms of end-end delay.

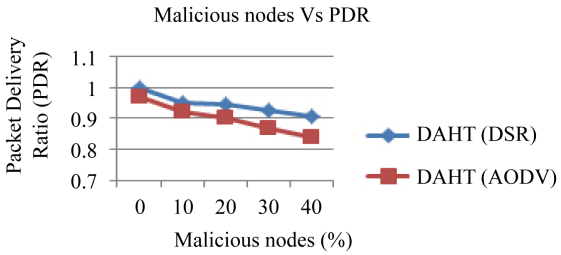

Figure 7. Comparisons of two protocols DSR and AODV in terms of PDR.

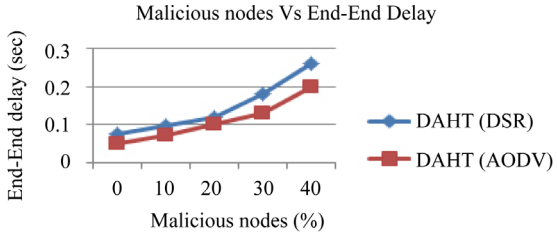

Figure 8. Comparisons of DSR and AODV in terms of end-end delay.

Conflicts of Interest

The Authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Anantvalee, T. and Wu, J. (2008) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. In: *Wireless/Mobile Security*, Springer-Verlag, New York, 159-179.

[2] Locke, G. and Gallagher, P. (2009) Digital Signature Standard (DSS). Federal Information Processing Standards Publication, Gaithersburg.

[3] Sivaram Murthy, C. and Manoj, B.S. (2004) Adhoc Wireless Networks: Architectures and Protocols. PHI Pearson Education Inc., India, 304-307.

[4] Nasser, N. and Chen, Y. (2007) Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile ad Hoc Network. *Proceedings of IEEE International Conference on Communication*, Glasgow, June 2007, 1154-1159. http://dx.doi.org/10.1109/icc.2007.196

[5] Sumimol, L. and Janisha, A. (2015) Security in Wireless Adhoc Networks Based on Trust and Encryption. *International Journal of Advanced Research in Computer and Communication Engineering*, **4**, 442-445.

[6] Zhong, S., Chen, J. and Yang, Y.R. (2003) Sprite: A Simple, Cheat-Proof, Credit-Based System or Mobile Ad-Hoc Networks. *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, 30 March-3 April 2003, 1987-1997. http://dx.doi.org/10.1109/infcom.2003.1209220

[7] Liu, K., Deng, J., Varshney, P.K. and Balakrishnan, K. (2007) An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs. *IEEE Transaction on Mobile Computing*, **6**, 536-550. http://dx.doi.org/10.1109/TMC.2007.1036

[8] Balakrishnan, K., Deng, J. and Varshney, P.K. (2005) TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks. *Proceedings of IEEE Wireless Communication and Networking Conference*, New Orleans, 13-17 March 2005, 2137-2142.

[9] Naqvi, S.I. and Akram, A. (2011) Pseudo-Random Key Generation for Secure HMAC-MD5. 2011 *IEEE* 3*rd International Conference on Communication Software and Networks* (*ICCSN*), Xi'an, 27-29 May 2011, 573-577. http://dx.doi.org/10.1109/ICCSN.2011.6014790

[10] Kiran Rao, P. and Vasundra, S. (2012) Channel Aware Routing in MANET'S with Secure Hash Algorithm. *International Journal of Scientific and Research Publications*, **2**, 1-4.

[11] Daza, V., *et al.* (2007) Cryptographic Techniques for Mobile Adhoc Networks. *Elsevier Computer Networks*, **51**, 4938-4950. http://dx.doi.org/10.1016/j.comnet.2007.08.002

[12] Shakshuki, E.M., Kang, N. and Sheltami, T.R. (2013) EAACK—A Secure Intrusion-Detection System for MANETs. *IEEE Transactions on Industrial Electronics*, **60**, 1089-1098. http://dx.doi.org/10.1109/TIE.2012.2196010

[13] Nikam, P.D. and Raut, V. (2015) Enhancement to EAACK for Improved MANET Security. *International Journal of Advanced Research in Computer Science and Management Studies*, **3**, 324-329.

[14] Capkun, S., Buttya, L. and Hubaux, J.-P. (2003) Self-Organized Public-Key Management for Mobile Adhoc Networks, *IEEE Transactions on Mobile Computing*, **2**, 52-64. http://dx.doi.org/10.1109/TMC.2003.1195151

[15] Zhou, L. and Haas, Z.J. (1999) Securing Ad Hoc Networks. *IEEE Network Magazine*, **13**, 24-30. http://dx.doi.org/10.1109/65.806983