Performance Analysis of Malicious Node Aware Routing for MANET using Two-Hop Authentication

Sanjeev Rana
Assoc. Professor, CSE Deptt., M. M. Univeristy, Mullana, Ambala, India

Manpreet Singh
Professor, CSE Deptt. M. M. University, Mullana, Ambala, India

ABSTRACT

The inherent features of the MANET [1] make it vulnerable to a wide range of attacks. There is no guarantee that a communication path is free from malicious and compromised nodes which deliberately wish to disrupt the network communication. In this paper, we present a security mechanism that provides message integrity, mutual authentication and two-hop authentication mechanism without the assistance of online certification authority. Our mechanism not only prevents identity impersonation, replay attacks, but also enables node to regulate the behavior of its neighbors to foil active attacks. The effectiveness of the proposed scheme is analyzed to DSR and OLSR routing using simulator NS2.34

Keywords

Malicious nodes, DSR, OLSR, Authentication, MANETs.

1. INTRODUCTION

With the fast development and deployment of mobile devices, Mobile Ad Hoc Networks (MANETs) become an important component of modern distributed systems. Because of the infrastructure-less property, MANETs can be easily deployed. They are very attractive to applications such as military operations and first response to disasters. These applications, however, have very strict requirements on security of network topology and data traffic. Mechanisms must be properly designed for these applications before the advantages of MANETs can be fully exploited. Security in such infrastructure-less networks has been proven to be a challenging task. Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks where an aggressor in order to launch an attack has to gain access to a wired infrastructure, firewalls and gateways, in ad hoc networks there is no clear line of defense. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination. The insecure open medium combined with poor physical protection presents another disadvantage. Each node is able to roam independently running the risk to be easily compromised by a malicious attacker. Furthermore, when more sophisticated attacks take place nodes can be easily exploited. In addition, wireless ad hoc networks lack a centralized monitoring and management point. As far as the MANET is concerned, the following types of attacks have been reported: Impersonation or spoofing: Such an attacker will try to spoof a node that resides in the route of the data Flow of interest [4]. Such an attack can be materialized since the conventional routing protocols, i.e. AODV [3], DSR [2], do not support authentication of IP addresses. A similar threat is called Sybil attack [5]. An attacker does not only impersonate one node, but it assumes the identity of several nodes, and, thus, undermines the redundancy of many routing protocols [6].

Sinkhole: where an attacker tries to attract all the data sent by its neighbors. This attack is the basis for example, eavesdropping [6]. Sinkhole attackers present themselves to adjacent nodes as the most attractive relay in a multi-hop route. Wormhole: where a malicious node uses a path outside the MANET (tunnel) to forward packets to another, colluding, node in the fixed network [7]. According to [7], the route discovery methods of on-demand routing protocols are violated by avoiding the normal route and by forwarding the RREQ packets directly to the destination.

Routing fabrication: where an attacker tampers with the normal routing procedures. It is achieved through alteration of the routing messages' fields (e.g., poisoning of DSR routing caches) or by the insertion of false routing messages (e.g., falsifying route error messages). Routing 'fabrication' produces denial-of-service (DoS) and partitioning of a MANET. In [8] several threats are identified, which are materialized through the modification of the routing messages' fields, such as modified sequence number, hop counts, or source route. DoS and flooding: They are considered as indirect results of the aforementioned attacks [9]. A direct DoS attack, introduced in [9], is the sleep deprivation torture. One node, or colluding nodes, continually request the services offered by the target node. This consumes the battery of the target, which goes into an idle or power preserving state.

All active attacks are due to lack of strong authentication mechanism. In this paper, we introduce a Two-Hop Authentication Scheme which not only provides authentication but also regulates the behavior of data forwarding nodes. Section 2 describes the literature review. Section 3 gives the overview of the proposed scheme. Implementation of proposed scheme to DSR and OLSR is described in section 4, section 5 shows the effectiveness of the proposed scheme using simulator NS2.34. We conclude the paper in section 6.

2. RELATED WORK

Misbehavior detection and reaction are described in [13], by Marti, Giuili, Lai and baker. The paper present two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies the misbehaving nodes by listening promiscuously to the next transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations [6], it is highly effective in source routing protocols such as DSR. The path rater uses the knowledge from the watchdog to choose a path most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes n the path, where each node maintains a rating for all the nodes it knows in the network. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior.

Buchegger and Le Boudec [11] present the CONFIDENT protocol. Each node monitor the behavior of its next hop neighbors in a similar manner as in watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting a node as part of a route and so on. When neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node's rating turn out to be intolerable, the information relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial dropping.

Michiardi and Molva propose the CORE scheme and various related issues in [12] [13]. In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbors past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended. In [17], a security extension to the on demand ad hoc routing protocol is proposed which deals with the lifetime or the validity of the control messages. In this, intermediate nodes do not introduce any authentication. Thus, even external nodes can take part and disrupt the routing process. The approach proposed in [19] to secure ad hoc on demand routing protocol used a challenge-response mechanism. A three-way communication occurs between every pair of intermediate nodes increasing overhead considerably and assuming bi-directionally.

In [14],[15] the uses of timestamps are proposed in order to counter against replay attacks. The authors of [16] also proposed the use of signature to ensure authentication in order to prevent identity spoofing attacks. In Ariadne [17] every intermediate node appends a HMAC based on a TESLA a key that will not be disclosed at least until the destination receives the RREQ. The TESLA keys used for authentication during the forward path are released during the reverse path. Thus, at the end of RREP, the destination can discover node deletion attacks. But this approach [20] assumes prior distribution of secret between every pair. In [20] the authors present many different forms of authentication strategies for securing route discovery. The main focus of the protocol in [21] is to reduce the overhead for carrying over authentication by employing authentication strategies that can be aggregated to save bandwidth. A self-organized public-key infrastructure is developed by Hubaux, Buttyan and Capkum [21]. The certificate directories are stored and distributed by users. The shortcut hunter algorithm is proposed to build local certificate repositories for the users. Between any pair of users, they can find certificate chains to each other using only their local certificate repositories. New mechanisms are to be proposed if decentralization is introduced in self-organized mobile ad hoc networks.

3. THE PROPOSED TWO-HOP AUTHENTICATION SCHEME

The proposed authentication scheme is consisting of two modules One-hop authentication and two-hop neighbor authentication module. The purpose of One-hop authentication module is to identify and authenticate its one hop neighbor. Where, two-hop neighbor authentication module enables a node to regulate the behavior of other node. Proposed scheme uses public key cryptography and assumes the existence of certification authority. A certificate signed by the CA for node I also includes a valid time and expiration time and has following format: $\mathrm{Cert}_i = \{ID_i, K_i^+, T_V, T_e\}K_{ca}^-$

3.1 One-Hop Neighbor Authentication

Each node gets a pair of public/private key and its certificate from CA in a secure fashion before communication. We propose a simple and efficient algorithm to authenticate two nodes each other that also use a challenge-response mechanism to foil replay attack during One-hop authentication module. Step1: Node A introduces itself to node B using its certificate. $A \rightarrow B : C_A$

Step2: Node B introduces itself to Node A and also sends a challenge (Nonce) signed using public key K_A^+ of Node A. $B \rightarrow A : C_B \parallel \{N_B\}K_A^+$.

Step3: Node A receives the above message and gets N_B , Node

A sends its challenge N_A to Node B and also add the reply of B challenge.

$A \rightarrow B : \{N_A , N_B\}K_B^+$

Step 4: Node B decrypt the message, N_B shows that this message is the response of previous message and also verify that this message is originated by Node A. Node B prepares the response of Challenge play by Node A.

$B \rightarrow A : (N_A\}K_A^+$

Node A will decrypt the message and ensure that this message is the response of previous challenge and it is originated from Node B.

3.2 Two-Hop Neighbor Authentication

The main purpose of two-hop neighbor authentication module (THNA) is to provide two-hop authentication by verifying the claim of any node about its neighbors. Node must provide a piece of information which ensures that the relationship with its neighbor node cannot be reproducing by some other node. This requirement can be achieved using digital signature of link information between two nodes. First, two nodes verify each other identity using one-hop authentication process, then, they generate a two-hop neighbor authentication ticket in the following format:

$$THNA_{A \rightarrow B} = [ID_A \,||\, ID_B \,||\, T_I \,||\, C_B \,||\, \{ID_A \,||\, ID_B \,||\, T_I\}K_B^-]$$

This is THNA ticket of Node A created for node B and can be read as "Node A ensures that Node B is its one hop neighbor and Node B approves the claim of node A". Thus, a remote node is able to verify the claim of node A by evaluating the ticket of node A to node B. The significance of THNA is if all connection in a path from a node to its destination is verified by respective THNA, from some initial or start time T_I to T_I + system_defined_valid_time, one can believe that the route is secure and trustworthy. Each node collects THNA and uses it to build a trusted and secure routing path. In reactive routing protocol such as DSR, the trusted and secure routing information can be distributed in the route request and route reply messages. Each hop appends respective THNA at the end of the control message. This module allows a remote node to build a trusted and secure relationship without the assistance of online trusted authority. The link status must be confirmed by both the nodes hence compromised nodes cannot forge link that don't exist.

4. IMPLEMENTATION OF PROPOSED SCHEME

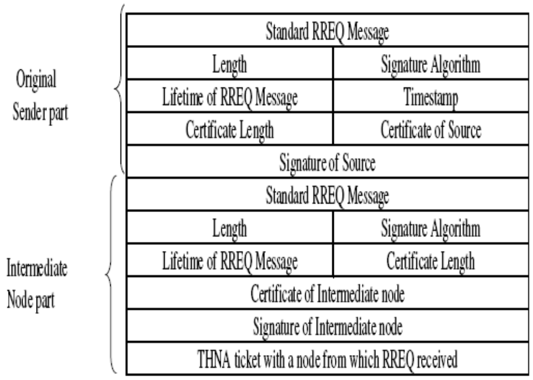
We have implemented the proposed two-hop authentication scheme on two routing protocols. First one is DSR a reactive routing protocol and second one is OLSR a proactive routing protocol.

4.1 Proposed Two-Hop Authentication Scheme on DSR

Security services are implemented by extending existing control messages of the DSR protocol for add some security related attributes such as timestamp, lifetime, signatures and THNA ticket. There are no changes to the protocol operation itself but each node now performs additional, security related functions, when DSR messages are exchanged. As the source node and destination node initiate the process of RREQ and RREP respectively, only intermediate nodes include THNA ticket when forward the control messages on the network. The route discovery process in DSR begins when the source node floods the network with RREQ message. Upon receiving route request message, next intermediate receiving node performs following actions:

- First, verify the identity of RREQ forwarding node using one-hop authentication to ensure that it is a genuine one hop neighbor or not.
- Second, evaluate THNA tickets included in the message for two-hop authentication to prevent node deletion attacks.
- Third, validates the signature of signed element using the public key of sender by its certificate.
- Fourth, receiving node checks for replay attack using the RREQ ID and timestamp.
- Fifth, validates the life time of the message to determine whether it has expired or not.

If any of these tests fail then receiving node must discard this message otherwise, receiving node rebroadcast the route request. Assume that a source node S is trying to discover a route to a destination node D and that such a route exist, with intermediate nodes A and B. The source node S must authenticate itself to other nodes when passing its request to locate a target destination. The source node S achieves this by broadcasting the RREQ with security extension as shown in figure 1 in step1. RREQ message contains a lifetime L_S that indicates how long this request is valid. If a target node receives the message and finds the period L_S has expired, then discard it. A time stamp T_S together with the RREQ ID in the original message format will indicate the freshness of the message and help to prevent replay attacks. This message content is signed using private key of the sender so that receiving nodes can verify the integrity of message. The sender certificate is included for the benefit of those nodes that do not already have that certificate. The sender identity is not separately included in the signed part as it is already the part of $RREQ_S$. Node A performs all the actions described earlier and if successful then node A first authenticate node S as its one-hp neighbor using one-hop authentication and then create $THNA_{A \rightarrow S}$ with node S. Now node A rebroadcast route request as in step2.


Original
Sender part
Intermediate
Node part

Standard RREQ Message	
Length	Signature Algorithm
Lifetime of RREQ Message	Timestamp
Certificate Length	Certificate of Source
Signature of Source	
Standard RREQ Message	
Length	Signature Algorithm
Lifetime of RREQ Message	Certificate Length
Certificate of Intermediate node	
Signature of Intermediate node	
THNA ticket with a node from which RREQ received	

Figure 1: Secure Extension of RREQ message in DSR

Route Request Phase

Step1:

$$S \rightarrow * = [RREQ_S || L_S || T_S || Cert_S || Sig_S] Where, Sig_S = \{RREQ_S || L_S || T_S\} K_S^-$$

Step2:

$$A \rightarrow * = [RREQ_A \; || \; L_S \; || \; T_S \; || \; T_A \; || \; Cert_S \; || \; Sig_S \; || \; Cert_A \; || \; Sig_A \; || \; THNA_{A \rightarrow S}]$$

$$Sig_A = \{RREQ_A \; || \; L_S \; || \; T_S \; || \; T_A \; || \; THNA_{A \rightarrow S}\} K_A^-$$

Route Reply Phase

Step3:

$$D \rightarrow B = [RREP_D || RREQ\_ID || L_D || T_D || Cert\_Sig\_List_{D\_RREP} || THNA\_List_{D\_RREP}]$$

$$Cert\_Sig\_List_{D\_RREP} = [Cert_S || Sig_S || Cert_A || Sig_A || Cert_B || Sig_B || Cert_D || Sig_D]$$

$$THNA\_List_{D\_RREP} = [THNA_{A \rightarrow B} || THNA_{B \rightarrow D}]$$

$$Sig_D = \{RREP_D || RREQ\_ID || D || S || L_D || T_D || THNA\_List_{D\_RREP}\} K_D^-$$

Route Error Phase

Step4:

$$B \rightarrow S = [RERR_B || RREQ\_ID || T_B || Cert\_Sig\_List_{B\_RERR} || THNA\_List_{B\_RERR}]$$

$$Cert\_Sig\_List_{B\_RERR} = [Cert_S || Sig_S || Cert_A || Sig_A || Cert_B || Sig_{B\_RERR}]$$

$$THNA\_List_{B\_RERR} = [THNA_{A \rightarrow B}]$$

$$Sig_{B\_RERR} = \{RERR_B || RREQ\_ID || T_B || THNA\_List_{B\_RERR}\} K_B^-$$

This message securely place node A in a possible route between node S and node D. Node A is including $THNA_{A \rightarrow S}$ in the control message, any next hop node can evaluate and verify it for two-hop neighbor authentication which ensures that node A receives this route request from node S. The is because node A cannot create this ticket alone without the consent node S (as node S private key is required to create ticket) that further need the successful completion of one-hop authentication process between them. Thus, all intermediate nodes can verify the route list using THNA tickets. Only difference in $RREQ_S$ and $RREQ_A$ is that the latter has added node A's address to the route list attribute in the RREQ message. So, Route request of any node can be reconstructed and can be verified their respective signature. If a node receives the same RREQ messages from two different intermediate nodes but with the same ID, it discards the later arrivals, according to the existing DSR definition.

The process of addition of node address to the route list, signature of message and THNA of intermediate nodes continues until reach to destination node D, if such a route exists. Here, destination node D analyzes and evaluates the message using different signatures and THNAs attached in the message for authentication, replay, validity or lifetime and identity impersonation. Furthermore, if node B tries to delete node A from route list, it need a THNA which cannot be created without the consent of node S. Our security mechanism does not consider two node colluding effect. If all tests validates, node D creates a route reply message and uses the route list attribute of route request message received, which is unidirectional as in step3. This message allows node D to authenticate itself to all nodes in the route as well as, eventually, to the source S. Node D add its certificate and THNA with its previous node and signature to those of node S, and all intermediate nodes. This will enable Node S to learn the identity of all nodes along the route.

Upon receiving such a message an intermediate node A performs all the actions required for authentication and validation of RREP message as described earlier. If any of the tests fail intermediate node A discard the message otherwise return message in step5. The purpose this message in step4 is for node B to authenticate itself to its previous hop Node A and to correlate the request message forwarded by Node A with its response thereby preventing replay attacks from happenings. It also verifies if the reverse path taken by the message indeed matches with the original forward path and that no other node is either legitimate or any masquerading node in the route list or replaying a previously captured message. The signed element includes the original request and response identification number. This message is signed using the private key of node B. If, in our example, during packet transmission the node B is unable to reach node D, node B must send a RERR route error message back to the source node S as in step5. This message is unicast to source node S, either via node A or through some other route in the link between node B and node A if it was unidirectional earlier.

4.2 Proposed Two-Hop Authentication scheme on OLSR

OLSR reduces the control traffic overhead by using Multipoint Relays (MPR). A MPR is a node's one-hop neighbor which has been chosen to forward packets. Instead of pure flooding of the network, packets are forwarded by a node's MPR. OLSR uses HELLO and Topology Control (TC) messages to discover and then disseminate link state information throughout the network. Individual nodes use this topology information to compute next hop destination for all nodes in the network using shortest hop forwarding paths. Our mechanism extended the HELLO and TC messages to carry additional information to make the route secure.

1. Hello message Extension
2. TC message Extension

4.2.1 HELLO Message Extension

In OLSR, many attacks, i.e. wormhole attack, occurs due to wrong selection of two-hop neighbors. Thus, two-hop neighbors selection or MPR set selection must be done after mutual authentication and authentic route confirmation ticket process between two nodes. This will ensure that only legitimates or trusted nodes will be involved during secure route establishment. The format of modified HELLO message with extension is shown in figure 2. After the standard message header, digital signature that guards the entire message (non-mutable attribute). The HASH_HOP, Nonce fields are included to guard mutable fields in the message. Timestamp is included in the message to foil replay attacks. Different information may be appended after each neighbor interface address, depending on the authentication state that is indicated by the stat field. The Option field indicates what contents are included: this can be handshake, identity certificate or THNAs ticket. If node A wishes to authenticate node B then it follows all the steps of mutual authentication between two nodes as shown in figure2.

Message Header		
Originator's Certificate		
Message Signature		
Nonce	HASH_HOP	Timestamp
Neighbor 1 interface Address		
Stat	Option	Length
Neighbor 1 Two-Hop Neighbor Authentication ticket (THNAs ticket)		
Neighbor 2 interface Address		
Stat	Option	Length
Neighbor 2 Two-Hop Neighbor Authentication ticket (THNAs ticket)		

Figure 2. HELLO Message Extension Format in OLSR

After nodes authentication, they exchange THNAs ticket as the proof of their relationship. THNAs ticket is appended in the HELLO message. Both nodes verify the link status by validating their THNAs ticket. MPR selection will be calculated after verification success.

4.2.2 TC Message Extension

In security enhancement mechanism, TC messages will also carry node identity certificate and authenticate route confirmation ticket. The format of TC extension message is shown in figure 3 is similar to HELLO messages but with different contents of the authentication field. A remote node performs the following steps to construct a secure routing table by receiving the TC message with THNAs ticket.
Step1: Receiver authenticates the mutable and non-mutable fields. The message will be discarded if the authentication fails.
Step2: Check the validity of each THNAs ticket, the neighbor who is confirmed to have authentic ink to the originator will be marked as pending in the topology table. This is because the originator itself may not be reachable. The neighbor with invalid THNAs will be discarded.

Message Header		
Originator's Certificate		
Message Signature		
Nonce	HASH_HOP	Timestamp
Neighbor 1 interface Address		
Option	Length	
Neighbor 1 Two-Hop Neighbour Authentication ticket (THNAs ticket)		
Neighbor 2 interface Address		
Option	Length	
Neighbor 2 Two-Hop Neighbour Authentication ticket (THNAs ticket)		

Figure 3. TC Message Extension Format in OLSR

Step3: If the TC message originator address is found in the routing table, all verified neighbors in the TC message will be added in the routing table otherwise they must wait till originator is reachable.
Step4: Each reachable address has a valid time in the topology map, which is determined by the THNAs ticket. The valid time must be updated for every new THNAs ticket received. If the valid time for an address is expired, the node is considered unreachable and will be removed from the routing table.

5 PERFORMANCE ANALYSIS

For the performance analysis of the proposed scheme, we used Network Simulator 2.34 [22], a simulator for mobile adhoc networks, which runs on Red Hat Linux Enterprise Server. The simulation parameters are provided in Table 1.

Table1: Simulation parameters

Parameters	Values
Examined protocols	DSR, Proposed DSR OLSR, Proposed OLSR
Application Traffic	CBR
Packet size	512 bytes
Pause time (sec.)	10
Transmission range	250m
Number of malicious nodes	5-20 nodes
Area	1000m X 1000m
Speed	0-2 m/s
Number of nodes	10-100 nodes

We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time of 10 sec, and then moves to another random position with a velocity chosen between 0 m/s to 2m/s (the maximum simulation speed). The scenario assumed for the simulation with 50 nodes including malicious nodes (ranging from 5 to 20) is shown in figure 4.

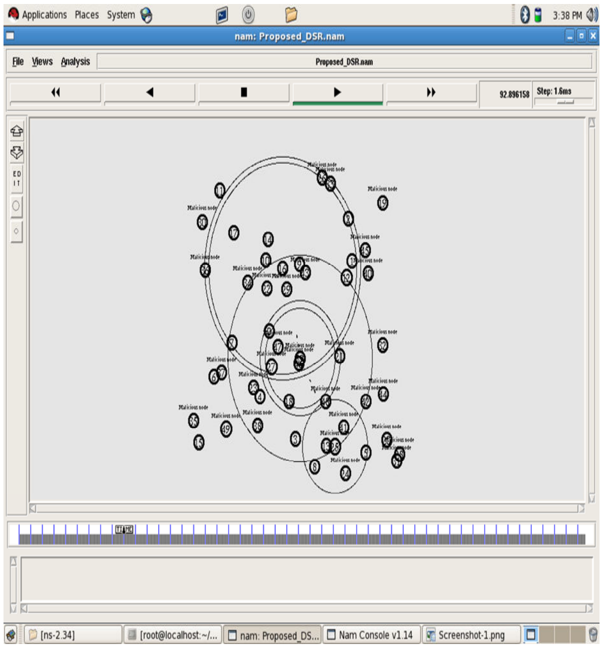


Figure 4: Scenario used for simulation with 50 nodes including 20 malicious nodes

We simulate the proposed security mechanism to determine the percentage of route discovery attempts between randomly chosen node pairs that succeeds. We assume that route discovery attempt between two nodes fail if every such RREQ path includes a malicious node. We simulated RREQ propagation between every pair of good nodes. The simulation result are shown for two cases first, bad RREQs are detected only by the destination node that is late detection and second, good RREQs are detected within two hops that is fast detection and stopped for further propagation. Our simulation result shown in figure 5 that the red line represents late detection and the blue line represents fast detection. As seen from the plots, fast detection of RREQ inconsistencies can substantially improve the performance of on demand routing solution by preventing preemption of good path by defective RREQs. Figure 3.7 also shows that as the number of intermediates nodes increases, chances of malicious nodes in the route also increases which ultimately dropped more number of packets than that of standard DSR. These results show that about 30% of packets that were possibly altered by malicious nodes in the network remained undetected and could potentially make their way through authentic nodes when using Standard DSR, as compared to the proposed DSR. This is a significant increase in the degree of security level.

Figure 6 shows that the number of packets dropped in the proposed OLSR is higher than that of standard OLSR because of two reasons. First, nodes can authenticate its neighbor to prevent link spoofing. Second, THNAs ensures that the information pass by a neighboring node is authentic. After both the successful steps a node build its MPR selection set, otherwise drop the packets. As the number of malicious nodes increases in the network, much large fraction of inconsistent packets increases which ultimately dropped.

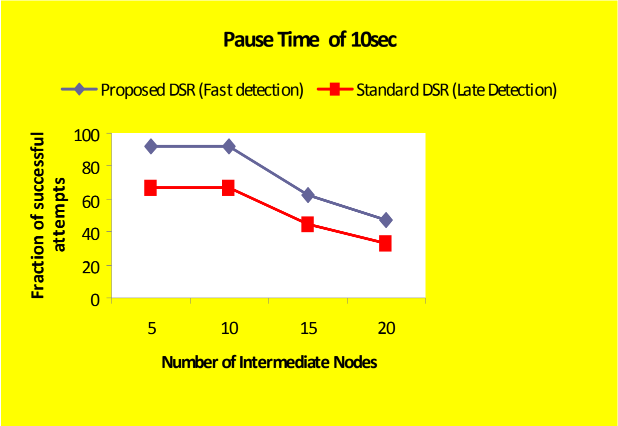


Figure 5: Fraction of successful attempts between proposed DSR and standard DSR

These results show that about 23% of packets that were possibly altered by malicious nodes in the network remained undetected and could potentially make their way through authentic nodes when using OLSR, as compared to the proposed protocol. This is a significant increase in the degree of security level.

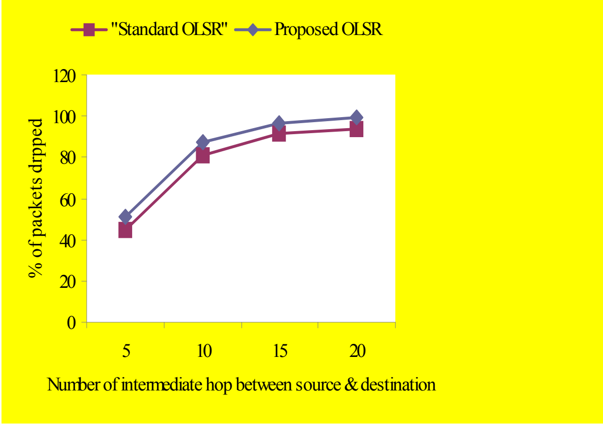


Figure 5 Proposed OLSR with large number of packets dropped than standard OLSR

Average End-to-End Delay

The delay experienced by packet from the time it was sent by a source till the time it reached the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times.

Average end to end delay can be calculated by averaging the send time and receive time for each packet sent. The security is achieved at the cost of additional computation and bandwidth overhead in the proposed scheme. With the usage of signatures and verifications method in the proposed DSR (red line) causes higher delays as compared to standard DSR (blue line) as shown in figure 7.

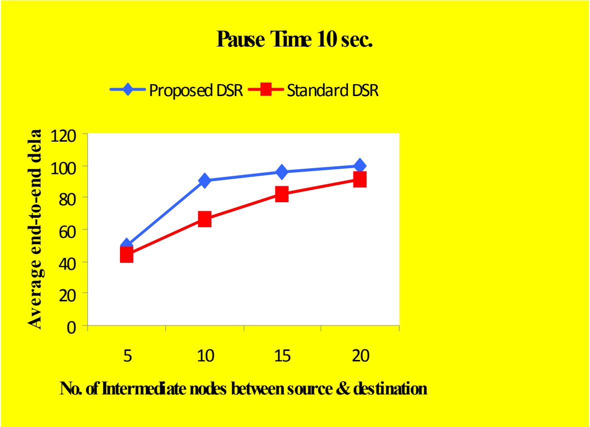


Figure 7: Average End-to-End delay with varying number of intermediate nodes

6 CONCLUSION AND FUTURE SCOPE

Secured ad hoc routing protocols are a necessity for securing the routing of data because participating malicious nodes may sabotage the network. In this paper, we propose a two-hop authentication mechanism which enables nodes to regulate the behavior of their neighbors. Our proposed scheme is equipped with technique to identify and isolate the tempered messages from unnecessary data forwarding. The results of simulation also show the effectiveness of the proposed scheme. To have security in the routing, one should sacrifice the performance of the data transmission. This paper shows that in the secure routing protocols, the usage of security techniques like digital signatures, authentications and hash chains have major impacts on the performance since it will use more processing power and time. Secure routing protocols available today still need further optimizations to minimize the processing overhead, delays.

7 REFERENCES

[1] C. Siva Ram Murthy and B. S. Manoj, "*Ad Hoc Wireless Networks: Architectures and Protocols*" Prentice Hall, 2004.

[2]. Johnson DB, Maltz DA. "Dynamic source routing in adhoc wireless networks in Mobile Computing" *Imielinski T, Korth H (Eds). Kluwer Academic Publishers*: Boston, 1996; 153–181.

[3] Perkins CE, Royer EM. "Ad-hoc on-demand distance vector routing" *Proceedings of 2nd IEEE Workshop on Mobile Computer Systems and Applications,* February 1999.

[4]. Karlof C, Wagner D. "Secure routing in wireless sensor networks: Attacks and countermeasures*" Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications* May 2003.

[5] Douceur J. "The sybil attack" *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS02),* March 2002.

[6] Burg A. "Ad hoc network specific attacks" Seminar *Adhoc networking: Concepts, Applications, and Security. Technische Universitat* Munchen, '2003.

[7] Hu YC, Perrig A, Johnson DB. "Packet leashes: A defence against wormhole attacks in wireless ad hoc networks" Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[8]. Michiardi P. "Cooperation enforcement and network security mechanisms for mobile ad-hoc networks" *Ph. D. thesis, Ecole nationale supe´rieure des telecommunications*, December 2004.

[9] Jøsang A. "The right type of trust for distributed systems" *Proceedings of ACM New Security Paradigms Workshop,* September 1996.

[10] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehaviour in Mobile ad hoc networks" *Proceedings of MOBICOM 2000*. Pages 255-265, 2000.

[11]. Sonja Buchegger and Jean-Yves Le Boudec: "Performance analysis of the CONFIDANT protocol" *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing'02.* p.p:226 – 236

[12] P. Michiardi and R. Molva. Preventing denial of service And selfishness in adhoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[13] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, pages 107–121, Portorosz, Slovenia, September 2002.

[14] C. Adjih, D. Raffo, and P Muhlethaler, "Attack against OLSR: Distributed Key Management for security", 2nd OLSR interop/ Workshop, France, July 28-29, 2005

[15] D. Raffo," Security Schemes for OLSR protocol in Ad hoc Network", Ph.D thesis, universite Paris, 2005

[16] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Analysis of Node Isolation Attack against OLSR-based Mobile Ad Hoc Network," 7th international symposium on computer networks (ISCN) pp 30-35, IStabul, Turkey, June 2006.

[17] Hu, Y.-C., Perrig, A., Johnson, D.B.: Aridane: A secure on-demand routing protocol for ad-hoc networks. In: The Proceeding of 8th ACM International Conference on Mobile Computing and Networking (September 2002)

[18] Kim, J., Tsudik, G.: Securing Route Discovery in DSR. In: IEEE Mobiquitous 2005 (July 2005)

[19] Venkatraman, L., Agarwal, D.P.: An Optimised Inter-Router Authentication Scheme for Ad Hoc networks. In: Proceeding of the 13th International Conference on Wireless Communication, Calgary, Canada, July 9-11, p. 129 (2001)

[20] Zapata, M.G.: Secure Adhoc On-Demand Distance Vector Routing (SAODV), Mobile Adhoc Networking Group

Internet Draft (October 2001) draft-guerrero-manet-saodv-00.txt

[21] J.Hubaux, L.Buttyan, and Sc.Capkun.: The quest for security in Mobile Ad hoc Networks. In *proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing* (MobiHOC) 2001

[22] Kevin Fall, Kannan Varadhan: The ns manual, http://www.isi.edu/nsnam/ns/ doc/index.html