Asian Journal of Information Technology 13 (2): 58-67, 2014
ISSN: 1682-3915

A Secure Authentication Framework for Mobile Ad Hoc Networks

E.A. Mary Anita
S.A. Engineering College, Chennai, India

Abstract: The main assumption of ad hoc routing protocols is that all participating nodes do so in good faith without disrupting the operation of the protocol. However, due to the absence of properly protected media and well trusted infrastructures and the reliance on unknown third parties for data forwarding, Mobile Ad hoc Networks (MANETs) are intrinsically vulnerable to various attacks. The security issue of MANETs is even more challenging because of the involvement of multiple senders and multiple receivers. Achieving trustworthy and secure and reliable communication is a major technical challenge in MANETs. The main focus of this study is to propose a secure framework for routing attacks by authenticating nodes using localized certificate chains. This proposed architecture combines the certificate chaining techniques with the existing route discovery scheme of on-demand multicast routing protocols.

Key words: MANET, security, attack, certificate, routing

INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous collection of mobile users forming a temporary network that communicate over relatively bandwidth constrained wireless links. Since, applications in ad hoc network are mostly group applications like information sharing in a conference room and the multi-player game, efficient multicast technology is needed in the ad hoc network. The existing routing protocols are optimized to spread updated routing information quickly when network topology changes without considering the security problem. Routing security in wireless networks appears to be a non trivial problem that can be solved easily (Dinger and Hartenstein, 2006). It is impossible to find a solution that can work efficiently against all types of attacks as every attack has its own distinct characteristics. Much vulnerability in network protocols is caused by the lack of integrity and authentication mechanisms which allows an attacker to alter or fabricate packets (Deng *et al*., 2002). Proper authentication scheme is the key to solve security problems in ad hoc networks. The authentication mechanism suitable for MANET should be feasible for highly changing network topology with low computational complexity and low bandwidth consumption.

In this context, a certificate based authentication mechanism has been proposed for security enhancement in reactive multicast routing protocols to counter the influence of malicious nodes. The concept of secured routing strategy is applied in reactive multicast routing protocols to enhance their performance in the presence of malicious nodes. Solutions are proposed for black hole, worm hole and Sybil attack by authenticating nodes using localized certificate chains. Security is implemented on top of the route discovery process of the routing protocols. There are no modifications made to the RREQ and RREP messages. Certified RREP messages are appended with the certificates to allow authorized nodes to participate in the routing process. This authentication mechanism eliminates the need for a centralized trusted authority which is not practical in MANETs due to their self organizing nature (Hashmi and Brooke, 2008). Also, the proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which most of the nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the overhead incurred in this process is reasonable with a good network performance in terms of security.

SECURITY CHALLENGES OF MANETS

Security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Unlike the wired line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology (Hu *et al*., 2006). These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. One of the fundamental

vulnerabilities of MANETs comes from their open peer to peer architecture (Nguyen and Nguyen, 2006). Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place or infrastructure where researchers may deploy a single security solution. Moreover, portable devices as well as the system security information they store are vulnerable to compromises or physical capture, especially low-end devices with weak protection (Levine *et al*., 2006).

Attackers may sneak into the network through these subverted nodes which pose the weakest link and incur a domino effect of security breaches in the system. The stringent resource constraints in MANETs constitute another nontrivial challenge to security design (Murthy and Manoj, 2004). The wireless channel is bandwidth constrained and shared among multiple networking entities. The computation capability of a mobile node is also constrained. For example, some low-end devices such as PDAs, can hardly perform computation-intensive tasks like asymmetric cryptographic computation. Because mobile devices are typically powered by batteries they may have very limited energy resources (Zhang *et al*., 2009). The wireless medium and node mobility pose far more dynamics in MANETs compared to the wired line networks. The network topology is highly dynamic as nodes frequently join or leave the network and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Despite such dynamics, mobile users may request "anytime anywhere" security services as they move from one place to another.

The above characteristics of MANETs clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. First, the security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to research within its own resource limitations in terms of computation capability, memory, communication capacity and energy supply (Douceur, 2002). Second, the security solution should span different layers of the protocol stack with each layer contributing to a line of defense. No single-layer solution is possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection and reaction that work in concert to guard the system from collapse. Finally, the security solution should be practical and affordable in a highly dynamic and resource-constrained networking scenario (Jeong *et al*., 2008).

LITERATURE REVIEW

The secure routing protocols for MANETs are either new standalone protocols or those adding security mechanisms to the existing routing protocols. The proposed solutions for security are classified into five categories (Argyroudis and O'Mahony, 2005); solutions based on symmetric cryptography; solutions based on asymmetric cryptography; hybrid solutions; reputation based solutions and add-ons to existing protocols.

Secure routing based on symmetric cryptography: Routing functionality in MANETs, secured using methods based on symmetric cryptography, use common mechanisms such as hash functions and hash chains.

Time Efficient Stream Loss-tolerant Authentication protocol (TESLA) (Perrig *et al*., 2000) is a multicast stream authentication protocol where the packets are held in a cache at the receiving node until the hash key used to authenticate them has been disclosed by the sender. Lightweight Hop by Hop Authentication Protocol (LHAP) (Zhu *et al*., 2003) uses hop by hop authentication. GPS devices are used in all the nodes to ascertain whether a sending node should be within transmission range of the receiving node. Lu and Pooch (2005)'s algorithm builds on LHAP and also uses hop by hop authentication. It is efficient but unlike LHAP it uses only one key at every node instead of two. Hop by Hop, Efficient Authentication Protocol (HEAP) (Akbani *et al*., 2008) uses a modified HMAC based algorithm that utilizes two keys.

A new MAC will be generated for every individual neighbor using its pair-wise key. Hash to Obtain Random Subsets Extended (HORSE) is a signature based scheme proposed by Neumann (2004) that creates unforgeable signatures on messages that can be verified using public information. But it has high communication overhead and verifying signature cost. Papadimitratos and Haas (2002)

have proposed a Secure Routing Protocol (SRP) that is based on a security association between communicating nodes. This security association is achieved by establishing a shared secret key between the end nodes. Hu *et al.* (2002a) propose Secure Efficient Ad hoc Distance Vector (SEAD) that makes use of hash chains to authenticate hop counts and sequence numbers. Hu *et al.* (2002b) also propose a secure on demand routing protocol Ariadne based on Dynamic Source Routing (DSR) protocol. The complex key exchanges in Ariadne make it infeasible in the current ad hoc environments.

Secure routing based on asymmetric cryptography: Asymmetric cryptography based solutions for secure routing requires the existence of a Trusted Third Party (TTP). The TTP issues certificates that bind a node's public key with a node's persistent identifier. The TTP can be either online or offline. In online systems, revocation of issued certificates is accomplished by broadcasting certificate revocation lists in the network. In offline systems, revocation involves exchange of messages between participating nodes and hence becomes a complicated problem.

Sanzgiri *et al.* (2005) propose a standalone solution ARAN (Authenticated Routing for Ad hoc Networks) for secure routing based on asymmetric cryptography. It uses cryptographic certificates from trusted entities and public key cryptography for authenticating route request, reply and error packets. Secure Position Aided Ad hoc Routing (SPAAR) (Carter and Yasinsac, 2002) uses position information in order to improve the efficiency and security of mobile ad hoc networks. ISMANET (Identity based Signcryption scheme for MANET) (Park and Lee, 2005) uses authentication algorithms based on identity based signcryption scheme. Zhang *et al.* (2008) have proposed a Cooperative Secure Routing protocol for Ad hoc Networks (CSRAN) to prevent and detect malicious attacks and selfish behaviors.

Secure routing based on hybrid solutions: Some of the secure routing protocols are based on both symmetric and asymmetric cryptographic techniques. The most common approach is to digitally sign the immutable fields of routing messages in order to provide integrity and authentication and to use hash chains to protect the hop count metric.

Zapata and Asokan (2002) have proposed SAODV (Secure Ad hoc Ondemand Distance Vector Routing) as a security extension to AODV. SAODV uses public key encryption to authenticate nodes. Secure Link State Protocol (SLSP) (Papadimitratos and Haas, 2003) secures the discovery of neighbors and distribution of link-state information of proactive routing protocols using digital signatures and oneway hash chains. Kadri *et al.* (2009) have proposed an implementation of Public Key Infrastructure (PKI) to secure reactive routing protocols in MANETs. This method exploits the route discovery and route reply mechanisms of reactive routing protocols to publish self-issued certificates in a distributed fashion

Secure routing based on reputation mechanisms: Reputation based solutions address the problem of security by taking decisions regarding legitimate nodes and encourages behavior that leads to increasing trust. This relies on the monitoring of the behavior of nodes participating in the network operations.

Marti *et al.* (2000) have proposed an intrusion detection technique known as Watch dog to detect nodes that agree to forward packets but fail to do so. Another module known as Pathrater uses the information from the Watchdog and helps the routing protocol to avoid misbehaving nodes. Lundberg (2000) have proposed an On demand Secure Routing Protocol (OSRP) that can function in the presence of colluding nodes introducing Byzantine failures in the process of routing. CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad hoc Networks) protocol an extended version of Watchdog and Pathrater (Buchegger and Le Boudec, 2002) is designed as an extension to reactive source routing protocol such as DSR. CORE (Collaborative Reputation) is a reputation based system Michiardi and Molva (2002) similar to CONFIDANT. CORE is a generic mechanism that can be integrated with several network and application layer functions.

Balakrishnan *et al.* (2005) have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is the enhanced version of DSR protocol. The distributed and cooperative intrusion detection system proposed by Zhang *et al.* (2003), detects falsifying of route information and random packet dropping in MANETs. AODVSTAT (AODV State Transition Analysis Technique) is a state transition analysis technique based IDS designed for detecting attacks against AODV, proposed by Vigna *et al.* (2004). Alampalayam and Kumar (2004) have proposed a predictive security model for mobile ad hoc networks designed using a fuzzy feedback control approach. The model is based on identifying critical network parameters that are affected by various types of attacks and it continuously monitors these parameters. Pirzada and McDonald (2004) present Kaman; Kerberos Assisted Authentication in Mobile Ad hoc Networks a

pure-managed authentication service for Mobile Ad hoc Networks. Kaman is based on the time-tested and widely deployed Kerberos protocol and provides secure extensions to support the more challenging demands of ad-hoc networks.

TWOACK (Two Acknowledgement) proposed by Balakrishnan *et al.* (2005) detects packet dropping in ad hoc networks using source routing protocol like DSR that address the problems of limited transmission power, receiver collisions and directional antennas of Watchdog and Pathrater. Fue *et al.* (2005) have discussed the characters of security issues in ad hoc networks and proposed a Support Vector Machine (SVM) based distributed hierarchical intrusion detection system that adapt to the characters of current ad hoc networks. Dhillon *et al.* (2006) have proposed intrusion detection in OLSR (Optimized Link State Routing) based MANETs by detecting anomalies in OLSR semantics. Oh *et al.* (2006) have suggested a comprehensive mechanism for discovering the most secure and shortest paths. This proposed mechanism is based on the Dijkstra algorithm and regards distance weight and trust weight highly. Tang *et al.* (2006) have presented a scheme called Privacy preserving Secure Relative Location Determination (P-SRLD) which securely determines the relative locations of a set of wirelessly connected vehicles based on the relative locations of each vehicle's surrounding vehicles.

Manickam *et al.* (2007) have proposed a Resiliency Oriented Secure (ROS) routing protocol which includes a detection phase to identify the presence of malicious nodes in the network. Mehfuz and Doja (2008) have proposed a Secure Power-Aware Ant Routing Algorithm (SPA-ARA) for Mobile Ad hoc Networks that is inspired from Ant Colony Optimization (ACO) algorithms. Yin and Madria (2006) have proposed a novel Secure Multipath Routing Protocol (SMRP) that applies a new heuristic algorithm increasing the number of disjoint paths and a smart authentication mechanism to enhance the security against the attacks in MANETs. Zhao and Aggarwal (2010) propose a design approach and a framework named PAPA-UIC (Pre-planned Ad-hoc Proactive Approach Using Identitybased Cryptography) for securing practical type of MANETs. Wang *et al.* (2009) have troduced a Social Network Analysis (SNA) Method as a new approach to build an intrusion detection system (SNIDS) in mobile ad hoc networks.

Add-ons to existing protocols: Add-ons do not constitute complete protocols but secure versions of existing protocols are built using add-ons. Add-on mechanisms address specific security problems in mobile ad hoc routing and extensions to existing techniques.

Liu *et al.* (2007) have proposed a secure routing protocol based on trust mechanism on top of AODV. SDAR (Secure Distributed Anonymous Routing protocol) proposed by Boukerche *et al.* (2004) guarantees security, anonymity and reliability of the established route by encrypting routing packet header and abstaining from using unreliable intermediate node. Kim *et al.* (2007) have employed route investigate on to prevent security threats in MANETs by confirming the receipt of control messages using Route Investigation Request (IREQ) and Route Investigation Reply (IREP). SRPTES (Secure Routing Protocol based on Token Escrow Set for Ad hoc Networks) proposed by Huang *et al.* (2008) employs token with limited lifetime to control trust relationships between neighboring nodes and provides secure routing and packet forwarding services through valid token.

LOCALIZED ARCHITECTURE FOR ROUTING PROTOCOLS

The principal idea to design secured routing protocols is to have a secure path with minimum cost to group members. Secure routing ensures successful routing among legitimate nodes in the existence of adversary nodes around the network. The node mobility is a highly influencing factor in addition to the multicast group size and the position of the attackers in designing the protocol (Djenouri *et al.*, 2005). Node mobility results in link failures and may form loops.

The unique characteristics of mobile ad hoc networks make them more susceptible to security attacks compared to wired networks or infrastructure-based wireless networks. The adversary is represented by malicious nodes in the network. An adversarial node can correspond to any compromised node. The impact of the adversary in attacking the routing protocol results in shortening of the network life time, degradation of the packet delivery ratio, increase in control over traffic and increase in network delay (Choi *et al.*, 2008). Some of these goals are highly correlated, e.g., increasing hostile control over traffic may also cause the network delay to be increased. In order to achieve the aforementioned goals, the adversary is able to perform simple message manipulations: fabricated message injection, message deletion, message modification and re-ordering of message sequences.

By considering the facts it is proposed to have the following system design to implement security in reactive protocols.

DESIGN FRAMEWORK

Security in a MANET is an essential component for basic network functions like packet forwarding and routing. Network operations can be easily jeopardized if counter measures are not embedded into basic network functions at the early stages of the design. Unlike dedicated nodes of wired networks, nodes of a MANET cannot be trusted for the proper functioning of critical network functions (Djenouri and Badache, 2008). To ensure proper functioning, only authenticated nodes should be allowed to take part in the routing process. This necessitates the need for a prior trust relationship among the participating nodes. This can exist only in a few special scenarios like military networks and corporate networks where a common trusted authority manages the network. But this requires a tamper proof hardware for the implementation of network functions. The design of the proposed black hole and worm hole secure architecture is shown in Fig. 1.

Black hole secure architecture: Implementation of black hole secure architecture is based on the assumption that all nodes operate in promiscuous mode. In the proposed protocol, Source Node (SN) broadcasts a route discovery message to discover a valid secure route to destination.

All intermediate nodes forward this message until the destination node or other intermediate node that has a valid route to destination finally replies with a route reply message. Upon receiving this message, the source node does not start the data transmission immediately. Instead it enters into an authentication phase wherein the nodes issue certificates to their neighboring nodes which are within the radio communication range of each other.

This certificate is issued based on the security level of the nodes. The security parameters to counter the effect of Black hole attack are the sequence number and the node's packet processing behavior. Each node obtains the security parameters of its neighboring nodes and issues certificates encrypted with its private key. The nodes that form the route between the source and destination now append their certificates to form the certified route reply. Once this certified route reply reaches the source node, the source node verifies the certificate chain, trusts the route and then starts transmitting the data packets (Anita and Vasudevan, 2009).

If a legitimate node behaves as an adversary over a period of time, the behavior is recorded by the neighboring nodes and the corresponding certificate is revoked. The security parameters may be varied in accordance with the nature of the attacks.

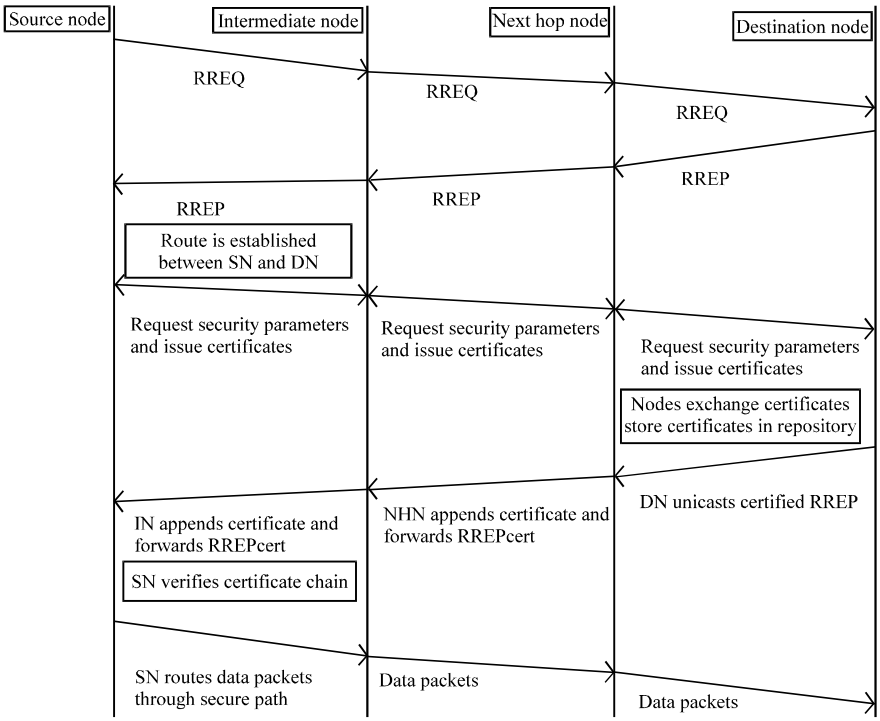

Fig. 1: Design of black hole and worm hole secure framework in MANET

Algorithm for black hole secure architecture:

Notations:
SN: Source Node
IN: Intermediate Node
DN: Destination Node
NHN: Next Hop Node
a) At source node
SN broadcasts RREQ/JREQ
IF (IN is NOT DN) THEN
Rebroadcast RREQ/JREQ
ELSE return RREP/JREP
b) At destination node
DN unicast RREP/JREP
All INs forward the RREP/JREP
RREP/JREP reaches SN
Route is established between SN and DN
c) Certification phase
Nodes forming the route certify each other:
Request id and security parameters of NHN
Generate public key of NHN based on id
Issue certificates encrypted with private key
Store certificates in repository
Exchange certificates with neighbor nodes
d) Authentication phase
DN unicast certified RREP/JREP appended with certificate from next hop node.
All INs append their certificates and forward the certified RREP/JREP
RREPcert/JREPcert reach SN
SN verifies certificate chain
Routes data packets through the secure path

Worm hole secure architecture: The architecture for worm hole security is similar to that of black hole secure architecture except that the security parameters are different. In the case of worm hole, the time difference between the sending of RREQ packet and the receipt of the same by the next hop node is used as a measure of security level. If this measured time interval is within the range of the worm hole timer, the next hop node is considered as a legitimate node and certificate is issued to this node with its security level set as 1. In case the time interval exceeds the value of the worm hole timer, the next hop node is set aside as malicious with its security level set to zero (Anita *et al*., 2010).

$$\text{Worm hole timer} = \frac{2 \times \text{Transmission range}}{\text{Speed of packet}} \quad (1)$$

Algorithm for worm hole secure architecture:

SN broadcasts RREQ
All intermediate nodes rebroadcast RREQ until DN is reached
DN sends RREP and is forwarded by all INs
Route is formed between SN and DN
Nodes forming the route, request security parameters of NHN
Check the time between sending of RREQ and its receipt by NHN
If time < = WHT, nodes issue certificate to NHNs with S = 1
If time >WHT, nodes issue certificate to NHNs with S = 0
DN sends authenticated RREP messages appended with certificates
SN verifies the certificate chain
Only S = 1 certified nodes take part in routing process
Other nodes are set aside as malicious
Worm Hole Secure route is established between SN and DN

Sybil secure architecture: As nodes enter the network they register their identity with their neighboring nodes. The IP address of the node may be taken as an identity. On registering the identity, the neighboring node applies a one way hash function H to the identity and calculates the public key. The corresponding private key is created locally. The neighboring nodes issue certificates to the incoming node by verifying the repository to check if a similar identity exists. If the verification succeeds, a certificate is issued to the incoming node. Only after this successful registration nodes are allowed to join the network. For example if node A is within the radio range of incoming node B, node A issues a certificate to B:

$$\text{Cert (A ->B)} = [ID_B, K_B, t, e, S] K_A \quad (2)$$

The certificate contains the identity of node B, the public key of B, the time of issue of the certificate, the time of its expiry and the security level of the node signed by the private key of A. This certificate is stored in the repositories of node A and node B.

If the verification fails that is, if the identity posed by the incoming node is already present in the issuing node's repository then the incoming node is prevented from joining the network. Also, the certificate issued to the already existing node is revoked. Only nodes with authenticated certificates are allowed to take part in the route discovery process.

Algorithm for sybil secure architecture:

Notations:
SN: Source Node
IN: Intermediate Node
DN: Destination Node
NHN: Next Hop Node
a) Initial certification phase
Nodes register id with neighboring nodes on joining the network,
NHN generates public key based on id
Nodes create private key locally
NHN checks repository to check for similar identity
NHN issues certificates encrypted with private key
Store certificates in repository
Exchange certificates with neighbor nodes
If verification fails:
Incoming node is prevented from joining network
Certificate issued to existing node with similar id is revoked
Route discovery process
SN broadcasts RREQ appended with certificate
IF (IN is NOT DN) THEN
Rebroadcast RREQ after inserting its certificate
All INs append their certificates and forward the RREQ
ELSE return RREP
DN unicast RREP
All INs forward the RREP
RREP reaches SN
Sybil secure route is established between SN and DN

SECURITY ANALYSIS

Researchers consider a wireless mobile ad hoc network consisting of N nodes. The average number of neighbors within a node's wireless communication range is C.

There are m malicious nodes in the network denoted by m_1, m_2 ,m_3, ..., m_m. For simplicity, researchers do not consider node arrival and departure in this analysis. The network lifetime, i.e., the duration of time that the network operates, is T.

Each node is initially assigned a certificate with lifetime $t_i << T$. When its current certificate expires, a node renews the certificate with lifetime increased by t_i. A malicious node starts to launch the attacks at time t_{mi} and its certificate is revoked at time $t_{rmi} > t_{mi}$.

Each node keeps the certificate of G legitimate neighbors. The average number of route requests sent out during one time unit, is denoted by r. The computation overhead is measured using the number of cryptographic executions. The only cryptographic executions in the proposed method are certificate renewal and revocation.

Each renewed certificate involves G+1 cryptographic computation at most one computation at the requesting node and one at each of its G neighbors. Similarly, each revoked certificate involves G+1 cryptographic computation at most.

Each legitimate node renews its certificate for $\sqrt{2t/t_i}$ times. Each malicious node is revoked of its certificate only once. Therefore, the total number of cryptographic executions in the entire network, throughout the network lifetime is:

$$E = \left(m + N\sqrt{\frac{2t}{t_i}} \right)(G+1) \quad (3)$$

In the proactive approach, the malicious attacks are prevented by applying cryptographic techniques such as digital signatures or message authentication codes on the routing messages. As a result, each time a node receives a routing update it has to perform two cryptographic computations: one to verify the received update, the other to generate its own update.

Researchers consider only the computation overhead associated with processing route request packets each of which is flooded in the network. Thus, the total number of cryptographic executions in the proactive approach is:

$$Ep = 2rt\mu N \quad (4)$$

where, μ is a constant ratio depending on the number of nodes. To compare the proposed method with the proactive approach, researchers have:

$$\frac{E}{Ep} = \frac{\left(m + N\sqrt{\frac{2t}{t_i}} \right)(G+1)}{2rt\mu N} = \frac{G+1}{\mu r\sqrt{\frac{2t}{t_i}}} \quad (5)$$

In proactive approach, each routing message is authenticated and hence the proposed method has comparatively lower computation overhead. This is because the cryptographic computations are performed only on certificate manipulation which happens much less frequently than routing message exchange.

For example, consider an ad hoc network that has N = 100 nodes and operates for 2 h (T = 120 min). Each node initially has a certificate with lifetime (t_i = 10 min). On an average, each node has G = 10 neighbors in its transmission range and initiates one data transmission every 10 min.

Thus, r = N/10 = 10 routing requests per minute. Let us assume for simplicity μ = 1. Based on Eq. 5, researchers can see that:

$$\frac{E}{Ep} = 0.02$$

This shows that the computation overhead of the proposed method is significantly lower than the proactive approach in this network setup.

CONCLUSION

Researchers have proposed solutions for black hole, worm hole and Sybil attack by authenticating nodes using localized certificate chains. This study proposes to combine the certificate chaining techniques with the existing route discovery scheme of on-demand multicast routing protocols. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the overhead incurred in this process is reasonable with a good network performance in terms of security. Researchers believe that this is an acceptable performance, given that the attacks prevented have a much larger impact on the performance of the protocol. As the schemes use the underlying protocol as a support for certificate publishing, the performance of the network is not much affected and does not add much delay.

REFERENCES

Akbani, R., T. Korkmaz and G.V.S. Raju, 2008. HEAP: A packet authentication scheme for mobile ad hoc networks. Ad hoc networks, 6: 1134-1150.

Alampalayam, S. and A. Kumar, 2004. An adaptive and predictive security model for mobile ad hoc networks. J. Wireless Personal Commun., 29: 263-281.

Anita, E.A.M. and V. Vasudevan, 2009. Prevention of Black hole attack in multicast routing protocols for mobile ad-hoc networks using a self-organized public key infrastructure. Inform. Secur. J.: Global Perspect., 18: 248-256.

Anita, E.A.M., V. Vasudevan and A. Ashwini, 2010. A certificate-based scheme to defend against worm hole attacks in multicast routing protocols for MANETs. Proceedings of the IEEE International Conference on Communication Control and Computing Technologies, October 7-9, 2010, Ramanathapuram, India, pp: 407-412.

Argyroudis, P.G. and D. O'Mahony, 2005. Secure routing for Mobile Ad hoc Networks. IEEE Commun. Surv. Tutorials, 7: 2-21.

Balakrishnan, K., J. Deng and P.K. Varhney, 2005. TWOACK: Preventing selfishness in Mobile Ad Hoc Networks. Proceedings of the IEEE Wireless Communications and Networking Conference, Volume 4, March 13-17, 2005, New Orleans, LA., USA., pp: 2137-2142.

Boukerche, A., K. El-Khatib, L. Xu and L. Korba, 2004. SDAR: A secure distributed anonymous routing protocol for wireless and Mobile Ad Hoc Networks. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, November 16-18, 2004, Tampa, FL., USA., pp: 618-624.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Carter, S. and A. Yasinsac, 2002. Secure position aided ad hoc routing. Proceedings of the IASTED International Conference on Communications and Computer Networks, November 4-6, 2002, Cambridge, MA., USA., pp: 329-334.

Choi, S., D.Y. Kim, D.H. Lee and J.I. Jung, 2008. WAP: Wormhole attack prevention algorithm in Mobile Ad Hoc Networks. Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, June 11-13, 2008, Taichung, Taiwan, pp: 343-348.

Deng, H., W. Li and D.P. Agrawal, 2002. Routing security in wireless ad hoc networks. IEEE Commun. Mag., 40: 70-75.

Dhillon, D., J. Zhu, J. Richards and T. Randhawa, 2006. Implementation and evaluation of an IDS to safeguard OLSR integrity in MANETs. Proceedings of the International Conference on Communications and Mobile Computing, July 3-6, 2006, Vancouver, Canada, pp: 45-50.

Dinger, J. and H. Hartenstein, 2006. Defending the Sybil attack in P2P networks: Taxonomy, challenges and a proposal for self-registration. Proceedings of the 1st International Conference on Availability, Reliability and Security, April 20-22, 2006, Vienna, Austria, pp: 756-763.

Djenouri, D. and N. Badache, 2008. Struggling against selfishness and Black hole attacks in MANETs. Wireless Commun. Mobile Comput., 8: 689-704.

Djenouri, D., L. Khelladi and N. Badache, 2005. A survey of security issues in mobile ad hoc and sensor networks. IEEE Commun. Surv. Tutorials, 7: 2-28.

Douceur, J.R., 2002. The Sybil attack. Proceedings of the 1st International Workshop on Peer-to-Peer Systems, March 7-8, 2002, Cambridge, MA., USA., pp: 251-260.

Fu, P., D. Zhang, L. Wang and Z. Duan, 2005. Intelligent hierarchical intrusion detection system for secure wireless ad hoc network. Proceedings of the 2nd International Symposium on Neural Networks, May 30-June 1, 2005, Chongqing, China, pp: 482-487.

Hashmi, S. and J. Brooke, 2008. Authentication mechanisms for mobile ad-hoc networks and resistance to Sybil attack. Proceedings of the 2nd International Conference on Emerging Security Information, Systems and Technologies, August 25-31, 2008, Cap Esterel, France, pp: 120-126.

Hu, Y.C., D.B. Johnson and A. Perrig, 2002a. SEAD: Secure efficient distance vector routing for Mobile Wireless Ad hoc Networks. Proceedings of the 4th Workshop on Mobile Computing Systems and Applications, June 20-21, 2002, Calicoon, NY., USA., pp: 3-13.

Hu, Y.C., A. Perrig and D.B. Johnson, 2002b. Ariadne: A secure on-demand routing protocol for ad hoc networks. Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, September 23-28, 2002, Atlanta, GA., USA., pp: 12-23.

Hu, Y.C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Selected Areas Commun., 24: 370-380.

Huang, C., B. Huang, Y. Mo and J. Ma, 2008. SRPTES: A secure routing protocol based on token escrow set for ad hoc networks. Proceedings of the 22nd IEEE International Conference on Advanced Information Networking and Applications, March 25-28, 2008, Okinawa, Japan, pp: 583-589.

Jeong, J.M., G.Y. Lee and Z.J. Haas, 2008. Prevention of Black hole attack using one-way hash chain scheme in ad hoc networks. Proceedings of the International Conference on Information Networking: Towards Ubiquitous Networking and Services, January 23-25, 2007, Estoril, Portugal, pp: 564-573.

Kadri, B., M. Feham and A. M'hamed, 2009. Securing reactive routing protocols in MANETs using PKI. Secur. Commun. Networks, 2: 341-350.

Kim, H.S., B.S. Kang, S.H. Pack and C.H. Kang, 2007. Route investigation for secure routing in Mobile Ad hoc Networks. Proceedings of the IEEE International Conference on Emerging Security Information, Systems and Technologies, October 14-20, 2007, Valencia, Spain, pp: 163-168.

Levine, B.N., C. Shields and N.B. Margolin, 2006. A survey of solutions to the Sybil attack. Technical Report 2006-052, University of Massachusetts Amherst, Amherst, MA., USA., p: 1-11.

Liu, Z., S. Lu and J. Yan, 2007. Secure routing protocol based trust for ad hoc networks. Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Volume 1, July 30-August 1, 2007, Qingdao, China, pp: 279-283.

Lu, B. and U.W. Pooch, 2005. A lightweight authentication protocol for Mobile Ad hoc Networks. Int. J. Inform. Technol., 11: 119-135.

Lundberg, J., 2000. Routing Security in Ad Hoc Networks. In: Mobile Security, Fall 2000: Proceedings of the Helsinki University of Technology Seminar on Network Security, Lipmaa, H. and H. Pehu-Lehtonen (Eds.). Telecommunications Software and Multimedia Laboratory, Helsinki, Finland, pp: 1-12.

Manickam, J.M.L., R. Bhuvaneswari, M.A. Bhagyaveni and S. Shanmugavel, 2007. Secure routing protocol for mobile ad-hoc networks. Proceedings of the Summer Computer Simulation Conference, July 15-18, 2007, San Diego, CA., USA., pp: 725-731.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in Mobile Ad hoc Networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking August 6-11, 2000, Boston, MA., USA., pp: 255-265.

Mehfuz, S. and M.N. Doja, 2008. Swarm intelligent power-aware detection of unauthorized and compromised nodes in MANETs. J. Artif. Evol. Appl. 10.1155/2008/236803.

Michiardi, P. and R. Molva, 2002. CORE: A collaborative reputation mechanism to enforce node cooperation in Mobile Ad hoc Networks. Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security, September 26-27, 2002, Portoroz, Slovenia, pp: 107-121.

Murthy, C.S.R. and B.S. Manoj, 2004. Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education India, New Delhi, India, ISBN-13: 9788131706886, Pages: 878.

Neumann, W.D., 2004. HORSE: An extension of an r-time signature scheme with fast signing and verification. Proceedings of the International Conference on Information Technology: Coding and Computing, Volume 1, April 5-7, 2004, Las Vegas, NV., USA., pp: 129-134.

Nguyen, H.L. and U.T. Nguyen, 2006. Study of different types of attacks on multicast in Mobile Ad hoc Networks. Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 23-29, 2006, Washington, DC., USA., pp: 149.

Oh, S., C. Lee and H. Choo, 2006. Collaborative trust-based shortest secure path discovery in Mobile Ad hoc Networks. Proceedings of the 6th International Conference on Computational Science, May 28-31, 2006, Reading, UK., pp: 1089-1096.

Papadimitratos, P. and Z.J. Haas, 2002. Secure routing for Mobile Ad hoc Networks. Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference, January 27-31, 2002, San Antonio, USA., pp: 193-204.

Papadimitratos, P. and Z.J. Haas, 2003. Secure link state routing for Mobile Ad hoc Networks. Proceedings of the Symposium on Applications and the Internet Workshops, January 27-31, 2003, Orlando, FL., USA., pp: 379-383.

Park, B.N. and W. Lee, 2005. ISMANET: A secure routing protocol using identity-based signcryption scheme for mobile ad-hoc networks. IEICE Trans. Commun., E88-B: 2548-2556.

Perrig, A., R. Canetti, J.D. Tygar and D. Song, 2000. Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy, May 14-17, 2000, Berkeley, CA., USA., pp: 56-73.

Pirzada, A.A. and C. McDonald, 2004. Kerberos assisted authentication in mobile ad-hoc networks. Proceedings of the 27th Australasian Computer Science Conference, Volume 26, January 18-22, 2004, Dunedin, New Zealand, pp: 41-46.

Sanzgiri, K., D. LaFlamme, B. Dahill, B. Levine, C. Shields and E.M. Belding-Royer, 2005. Authenticated routing for ad hoc networks. IEEE J. Sel. Areas Commun., 23: 598-610.

Tang, L., X. Hong and P.G. Bradford, 2006. Privacy preserving secure relative localization in vehicular networks. Proceedings of the 2nd International Conference on Mobile Ad-hoc and Sensor Networks, December 13-15, 2006, Hong Kong, China, pp: 543-554.

Vigna, G., S. Gwalani, K. Srinivasan and E. Belding-Royer and Kemmerer, 2004. An intrusion detection tool for AODV-based ad hoc wireless networks. Proceedings of the 20th Annual Computer Security Applications Conference, December 6-10, 2004, Santa Barbara, CA., USA., pp: 16-27.

Wang, W., H. Man and Y. Liu, 2009. A framework for intrusion detection systems by social network analysis methods in ad hoc networks. Secur. Commun. Networks, 2: 669-685.

Yin, J. and S.K. Madria, 2006. SecRout: A secure routing protocol for sensor networks. Proceedings of the IEEE 20th International Conference on Advanced Information Networking and Applications, Volume 1, April 18-20, 2006, Vienna, Austria, pp: 393-398.

Zapata, M.G. and N. Asokan,. 2002. Securing ad hoc routing protocols. Proceedings of the 1st ACM Workshop on Wireless Security, September 28, 2002, Atlanta, GA., USA., pp: 1-10.

Zhang, X.Y., Y. Sekiya and Y. Wakahara, 2009. Proposal of a method to detect Black hole attack in MANET. Proceedings of the International Symposium on Autonomous Decentralized Systems, March 23-25, 2009, Athens, Greece, pp: 1-6.

Zhang, Y., L. Xu and X. Wang, 2008. A cooperative secure routing protocol based on reputation system for ad hoc networks. J. Commun., 3: 43-50.

Zhang, Y., W. Lee and Y.A. Huang, 2003. Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9: 545-556.

Zhao, S. and A. Aggarwal, 2010. PAPA-UIC: A design approach and a framework for secure Mobile Ad hoc Networks. Secur. Commun. Networks, 3: 371-383.

Zhu, S., S. Xu, S. Setia and S. Jajodia, 2003. LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, May 19-22, 2003, Providence, RI., USA., pp: 749-755.