ISSN:0975-9646

AuthMAN: Authentication in Multicast Mobile AdHoc Networks using Time Asymmetry

Prasad Chaudhari[1], Ms. Deepali Gothawal[2]

[1,2]*Dept of Computer Engg*
D Y Patil College of Engineering - Akurdi, University of Pune

Abstract—In recent years, mobile ad hoc networks (MANETs) have become popular, because of their ease of deployment. However, security has become a crucial issue in order to provide protected communication between mobile nodes in a hostile environment of MANET. Unlike the wired network, the characteristics of MANET such as resource constraints and dynamic network topology possess challenges to security design of the network. For example, a malicious node can inject packets into the network to consume the resources of the nodes relaying the packets. To prevent this type of attacks, it is important to design an authentication scheme that ensures that only authorized nodes can send traffic on the network. Furthermore, in MANET, multicasting is used to support group communication. A characteristics of multicast, which is a single packet can reach to many users, possesses a potential danger of malicious user, who is able to inject packet, can reach to many receivers with a malicious packet. To achieve secure multicast communications is a challenging task because of the dynamic nature of MANET, where nodes in network can join and leave the group randomly. In this paper, we present AuthMAN, a scalable and lightweight mechanism to address the problems of authentication in multicast mobile ad hoc networks. AuthMAN uses symmetric cryptography, and time-delayed key disclosure to achieve authenticated broadcast. The evaluation results show the effectiveness and efficiency of the proposed solution.

Index Terms—Authentication, multicast mobile ad hoc network (MANET) security, time asymmetry

I. INTRODUCTION

Mobile ad hoc networks (MANETs) [6] self organizing in the nature. In MANETs, nodes can cooperatively establish a network independently of any centralized management such as base stations. Mobile hosts can join the network on the fly and leave the network at any time. Furthermore, in MANET, multicasting is used to support group communication. In multicast, a single packet can reach to many users. This possesses a potential danger of malicious user, who is able to inject packet, can reach to many receivers with a malicious packet. To address this issue, it is crucial to design an authentication mechanism that ensures that only authorized nodes can send and receive traffic on the network. Authentication means verification of the identity of an entity.

Existing unicast authentication mechanisms are ineffective and inefficient in the multicast setting of a MANET. Well known unicast security mechanisms such as Transport Layer Security (TLS) [3] or IPSec [15] use a message authentication code (MAC) to achieve authentication. Even though the symmetric MAC based authentication mechanisms provide computational efficiency, but they do not provide the desired security guarantees in a multicast environment. Symmetric MAC key based authentication mechanisms are not secure in the multicast environment because every receiver knows the symmetric key. So potentially any malicious user could impersonate the sender and inject malicious packets into the network. Therefore, asymmetric approach is required to achieve authentication in the multicast environment. So that each receiver is able to verify the legitimacy of the message and the sender of the message. However, it is a challenging problem to achieve authentication in multicast mobile ad hoc network [2]. Furthermore, symmetric key based authentication mechanisms seems to be impractical in multicast mobile ad hoc network due to the dynamic nature of mobile ad hoc networks where the number of nodes in the network may increase or decrease due to mobility of nodes. Symmetric key distribution for all nodes in the network becomes impractical in MANET due to its ad hoc environment.

A. Limitation of Existing Techniques

Existing research efforts [4], [11], [12], [14] use asymmetric cryptography technique, such as digital signature, to achieve authentication in a broadcast environment of a MANET. The sender generates the signature on the message using its private key, and all the receivers in the network can verify the signature attached to the message using the sender's public key. Moreover, a receiver with the sender's public key cannot generate a digital signature for a new message. Hence it achieves authentication and non-repudiation. However, digital signatures impose a very high computational cost for both sender and receiver. In addition, use of digital signatures also increases the bandwidth requirements. This network overhead is further increased in the multicast settings where we need to attach digital signature to each message. Thus, asymmetric based authentication approach is suitable only for low-rate data streams, with sender and receivers are powerful workstations. However, in MANET, the mobile nodes need an efficient approach that saves node energy required for the authentication process.

B. Observations

The existing solutions lack to provide an approach that uses symmetric cryptography but achieves asymmetric property to perform authentication. They mainly focus on asymmetric cryptographic techniques for authentication in the MANET that increases network and computation overhead.

C. Proposed Work

This paper proposes, AuthMAN (Authentication for Multicast Mobile Network), an efficient and effective solution to achieve authentication in multicast mobile ad hoc network. The key idea of AuthMAN is to delayed key disclosure which results in an authentication delay. AuthMAN can be implemented in network, transport or application layer. AuthMAN requires receivers to buffer the received packets until the sender of the packet is authenticated. AuthMAN requires sender and receiver nodes to be loosely time-synchronized. AuthMAN achieves the following properties: 1) low computation overhead due to the use of symmetric key cryptography, 2) low communication overhead, and 3) support to multicast settings.

AuthMAN uses a time between sender and receiver nodes to achieve asymmetry property. AuthMAN associates a chain of keys which are associated with a time interval. At sender side, AuthMAN attaches a MAC to each packet which is computed on the message. Then sender discloses a key from the key chain after a constant pre-defined time delay. Receiver nodes in multicast mobile ad hoc network when receives the packets they store the received packets in the buffer. Each receiver knows the schedule of the key disclosure. After the key disclosure receivers verifies the packets in the buffer. Each receiver checks the key in the hash of key chain and then checks the correctness of MAC. If the MAC value is correct then only the receiver accepts the packet otherwise it rejects the packet.

D. Contributions

This paper proposed a mechanism that uses symmetric cryptography and time-delayed key disclosure to achieve authentication in multicast MANET. To summarize, this paper makes the following contributions:

- Proposes a novel approach for authenticating a sender in a multicast environment of mobile ad hoc network with a low computation overhead.
- Uses a time-delayed key disclosure to achieve the required asymmetry property in a multicast mobile ad hoc network.
- Implemented the proposed solution conducted extensive experiments. The evaluation results show the ffectiveness and efficiency of the proposed solution.

The rest of this paper is organized as follows: Section II describes the related work. Section III presents the design of our solution. Section V is evaluation results, and Section VI concludes the paper.

II. Related Work

In [5] authors proposed an efficient protocol for integrity verification and authentication using hash chains. The proposed approach combines Merkle Trees [9] and concepts of signatures to develop an efficient mechanism that is adaptive and flexible to the limited resources of mobile nodes. Mishra et al. [10] proposed an IDS for mobile ad hoc networks. They argue that application of IDSs to mobile ad ho networks is a recent development as compaired to the research of IDSs in wired world that has more than a decade year of tradition. The common problem in using IDSs for MANETs is the resource-constrained environment. Bhargava et al. [1] proposed an intrusion detection and response model to improve the security in the Ad Hoc On Demand Distance Vector (AODV) routing protocol. Kachirski and Guha [7] presented a mobile agent based IDS technology. Lee and Zhang [16] proposed a distributed and co-operative IDS system. In the proposed approach each node in the network participates in the detection and response, that is the IDS agent runs at each mobile node.

Zhou and Haas [17] proposed to use threshold cryptography to secure mobile ad hoc networks. They proposed a distributed certificate authority to issue certificates. However, this technique fails to address challenges in ad ho network. Because only selected nodes can be used as the certification authority, and contacting the distributed CA nodes in a MANET may be difficult. Na Ruan et.al. [13] proposed a multi-factor authentication system. The proposed system integrates multiple form of authentication techniques to verify the legitimacy of a transaction. However, authors fail to specify the underlying networking environment required for the proposed scheme. Therefore, lack of correct specification of the networking environment could mislead the performance of an authentication protocol in MANETs. Qiwei Lu et.al. [8] proposed distributed and trusted computing scheme for authentication in a MANET. However, they are introduce the computation overhead due to use of asymmetric cryptographic techniques.

a) Summary: Existing research efforts focused on asymmetric based authentication approaches. However, asymmetric cryptographic solutions introduces computational as well as network overhead. Therefore, in MANET, the mobile nodes need an efficient approach that saves node energy required for the authentication process.

III. Design Section

The goal of AuthMAN is to provide authentication in a MANET. To achieve authentication AuthMAN uses delayed per-packet data authentication technique that delays disclosure of symmetric keys. AuthMAN uses time as a asymmetry property and it requires sender and receiver need to be time-synchronized.

A. Architecture of our approach AuthMAN needs sender and receiver to time synchronized. Figure 1 illustrate the process of time synchronization between sender and receiver. AuthMAN uses a simple time synchronization method for receivers to know an upper bound on the delay of its local clock w.r.t the sender's clock. To get the upper bound (UB), receiver sends a message to the sender and receiver records the time of message (Rt). Sender after receiving message sends its local time to the receiver (St). Based on the senders local time receiver sets the upper bound (UB). In other words, upper bound is calculate by subtracting receiver's time from sender's time.

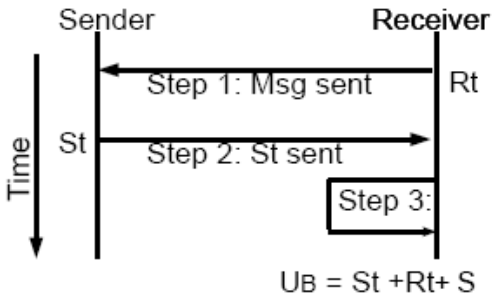

Fig. 1. Time Synchronization Process

Algorithm 1 Algorithm for time asymmetry property of AuthMAN

1: Input:
Rmsg (= synchronous message from receiver,
Smsg (= synchronous message from sender
Rt (= receiver's local time,
St (= sender's local time
2: Output:
Dt (= upper bound time
3: Step 1:
Rmsg;Rt sent by receiver to sender
Sender records its local time, St
4: Step 2:
Smsg; Rt; St sent by sender to receiver
5: Step 3:
Receiver calculates upper bound time
Dt = St - Rt + S . S is estimated bound on the clock drift

Algorithm 1 describes our proposed algorithm for time synchronization.

B. Security Considerations

To achieve delayed data authentication, AuthMAN relies on receive to buffer packets. However, this could cause Denial of Service (DoS) on receivers. Attackers could flood receivers to buffer excess packets to launch DoS. To combat DoS, AuthMAN uses safe packet test that checks each arriving packets to have a valid source IP address and port number.

IV. Implementation Of Authman

We simulated the AuthMAN algorithm using a custom JAVA based simulator. In the custom simulator software, we created different scenarios for cluster formation, routing and topology control. For topology control, we considered random deployment of nodes in the network. We used Java version 7, JUNG version 2.0 framework and JFreechart version 1.0.16 for simulation of topology control. In particular, we used java.util.* classes for managing iterators of nodes, hashmap of nodes, list of nodes and paths, and a set of nodes in the clusters. We used javax.swing.* classes for GUI. We also used org.jfree.chart.* classes to plot nodes to create a MANET network of nodes. The edu.uci.ics.jung.* classes to draw circle layouts of nodes, visualization of nodes in the GUI, draw graph of nodes to show their connectivity.

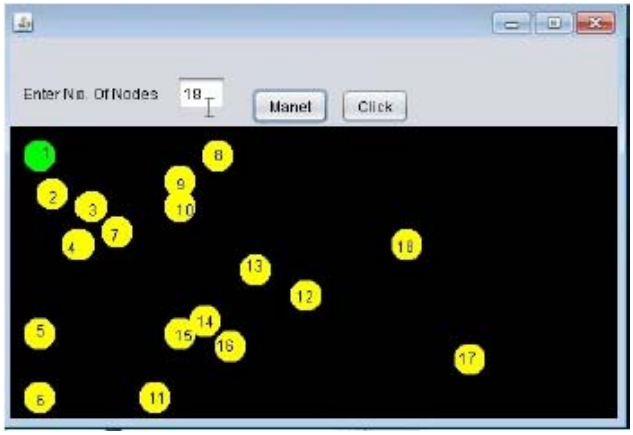

Fig. 2. An example of a MANET

Figure 2 shows an example of a MANET with various mobile ad hoc nodes.

V. Results And Discussion

We run our algorithm on several random networks created by randomly distributing nodes. We developed a custom simulator software to run simulations. Average number of neighbor node in the network is 10. At the beginning of simulation, a mobile node in the network is randomly selected to initiate the group communication, and six nodes are randomly selected to join the group. Simulation software uses 90 seconds interval to select a node randomly to join or leave the group. Nodes verses Key-size Figure 3 shows the graph of nodes versus key size of our simulated network environment. As shown in the graph, when the number of nodes increases it results into the increase in the size of key size.

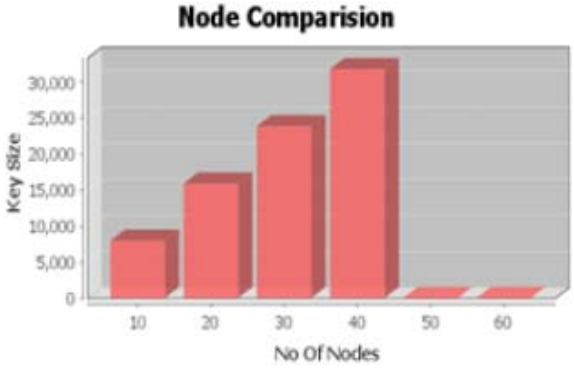

Fig. 3. Graph of No of Nodes verses Key Size

Time Ratio Figure 4 summarizes the time required to send the packets. As the number of packets to send increases the required time to send them also increases.

Sr no.	No of Packet sent	Time (sec)
1	10	2
2	20	3
3	30	4
4	40	5

Fig. 4. Time required to send number of packets

Group Establishment Success Ratio Vs Max Speed Figure 5 shows an effect of max speed of nodes on the group establishment success ratio. During experiments, max speed of the mobile nodes in the network was varied from 0 m/s to 50 m/s to change the mobility. Static network can be created using max speed of 0 m/s. When the nodes mobile speed keeps at 50m/s, the success ratio of the AuthMAN in the key establishment is more than 85%

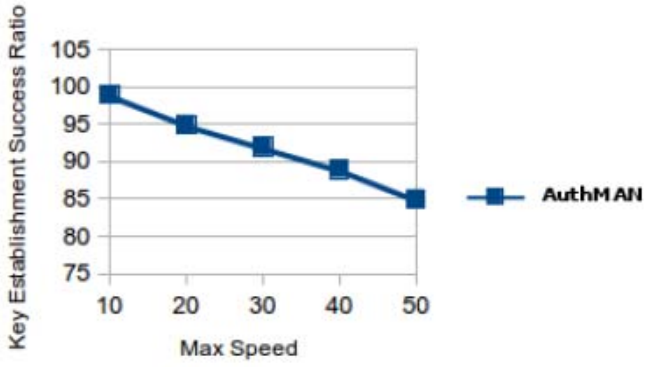

Fig. 5. Group Establishment Success Ratio Vs Max Speed

VI. CONCLUSION

In recent years, mobile ad hoc networks (MANETs) have become popular, because of their easy of deployment. Unlike the wired network, the characteristics of MANET such as resource constraints and dynamic network topology pose challenges to security design of the network. In MANET, multicasting is used to support group communication. In multicast, a single packet can reach to many users. This possesses a potential danger of malicious user, who is able to inject packet, can reach to many receivers with a malicious packet. To achieve secure multicast communications is a challenging task because of the dynamic nature of MANET, where nodes in network can join and leave the group randomly. In this research work, we presented AuthMAN, a scalable and light-weight mechanism to address the problems of authentication in multicast mobile ad hoc networks. AuthMAN uses symmetric cryptography, and time-delayed key disclosure to achieve authenticated broadcast. We showed the feasibility of the proposed approach with the help of our prototype implementation. The evaluation results showed the efficiency of the proposed solution.

REFERENCES

[1] S. Bhargava and D.P. Agrawal. Security enhancements in aodv protocol for wireless ad hoc networks. In Proceedings of theIEEE Vehicular Technology Conference (VTC 2001), pages 2143–2147, 2001.

[2] D. Boneh, G. Durfee, and M. Franklin. Lower bounds for multicast message authentication. In Proceedings of the Advances in Cryptology (EUROCRYPT), pages 434–450, 2001.

[3] Dierks and Allen. The tls protocol version 1.0. RFC 2246,1999.

[4] R. Gennaro and P. Rohatgi. How to sign digital streams. IBM T.J.Watson Research Center Technical Report, 1997.

[5] T. Heer, S. Gtz, O. G. Morchon, and K. Wehrle. Alpha: An adaptive and lightweight protocol for hop-by-hop authentication. In Proceedings of the ACM CoNEXT, pages 1–12, 2008.

[6] Internet Engineering Task Force (IETF). Manet working group. www.ietf.org/html.charters/manet-charter.html.

[7] O. Kachirski and R. Guha. Intrusion detection using mobile agents in wireless ad hoc networks. In Proceedings of the IEEE Workshop on Knowledge Media Networks, pages 153– 158, 2002.

[8] Qiwei Lu, Yan Xiong, Wenchao Huang, Xudong Gong, and Fuyou Miao. A distributed ecc-dss authentication scheme based on crt-vss and trusted computing in manet. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and ommunications, pages 656–665, 2012.

[9] R Merkle. A certified digital signature. In Proceedings of the CRYPTO, 1989.

[10] Mishra. Software engineering - rroduct quality - part 4: Quality in use metrics. ISO/IEC 9126-4, 2000.

[11] A. Perrig, R. Canetti, J. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of the IEEE Symposium on Security and Privacy, 2000.

[12] P. Rohatgi. A compact and fast hybrid signature scheme for multicast packet authentication. In Proceedings of the 6th ACM Conference on Computer and Communications Security, 1999.

[13] Na Ruan and Yoshiaki Hori. Dos attack-tolerant tesla-based broadcast authentication protocol in internet of things. In Proceedings of the International Conference on Selected Topics in Mobile and Wireless Networking, pages 60–65, 2012.

[14] C. K. Wong and S. S. Lam. Digital signatures for flows and multicasts. In Proceedings of the IEEE ICNP, 1998.

[15] IETF working group. Ip security protocol. http://www.ietf.org/html.charters/OLD/ipsec-charter.html.

[16] Y. Zhang and W. Lee. Intrusion detection in wireless ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pages 275–283, 2000.

[17] L. Zhou and Z. Haas. Securing ad-hoc networks. In Proceedings of the IEEE Network, volume 13, pages 24–30, 1999.