Multi Key Authentication for MANET

Mr. Ranjeet Pawar[1] Prof. Vidya Chitre[2]
[2]Assistant Professor
[2]Department of Information Technology
[1]Bharati Vidyapeeth Institute of Technology, Navi Mumbai [2]Vidyalankar Institute of Technology, Wadala, Mumbai

Abstract— Security is become main concern for widely deploy wireless network due to the broadcast medium and wireless resources are stringently constraints. An adversary can easily join the network and may eavesdrop, intercept, inject, eventually transmit data. Hence it is necessary to adaptively achieve the security according to available resources. In particular Mobile Ad-hoc network (MANET) with cooperative communication present significant security challenges. To prevent the attack like injecting malicious packet, nodes in MANET should able to ensure the source of packet. So it is important to design source authentication scheme which provide low computational overhead and consume less bandwidth. Furthermore, in MANET, multicasting is use to support group communication. To achieve the secure multicast communication is also challenging due to dynamic nature of MANET. The traditional authentication algorithms using public key cryptography are not effective in MANET. To address the challenge of source authentication we have propose MKAuth source authentication technique which is scalable, lightweight, timed, efficient and require less computational overhead. MMAuth use symmetric cryptography with delayed discloser of keys for each time interval.

Key words: MANET, CC, MKAuth
General Terms: Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

I. INTRODUCTION

Due to low cost and ease of deployment associated with wireless devices wireless network become the dominant choice for connecting to internet and doing collaborative work by forming network among coworkers. Ad hoc and multihop wireless network becoming increasingly important for a variety of applications ranging from tactical military network, to metro area Wi-Fi network, to sensor application, to vehicular network. A mobile ad hoc network (MANET) is a self-configuring wireless network of mobile devices connected by wireless link. Mobile host can join the network on fly and leave the network any time. Cooperative communication (CC) has been considered as promising technique to improve transmission reliability over ever challenging wireless medium.

MANET faces various challenges like self-organization, neighbor and topology discovery, medium access control, routing, security; our work focuses on security aspect of MANET for multicast communication. Multicasting is use to support group communication in MANET. Security has become main concern and bottleneck for widely deployed wireless application [1]. In particular CC-MANET has more challenges for secure routing, key exchange and management because of multihop routing, packet forwarding, lack of infrastructure, dynamic topology and node cooperation.

Security is main challenge because of broadcast nature of mobile adhoc network. It is important to verify that data received by receiver is legitimate and coming from intended source. Our propose work is related to insuring that packet received is from authenticate source. Traditionally there are various source authentication technique like digital signature are available. Digital Signature use senders private key to sign the packet being send and receive will use source public key for verifying signature. But communication in mobile Ad-hoc network is resource constraints. The technique like digital signature requires more computational power since using asymmetric cryptography and requires more bandwidth.

If we consider authentication using symmetric cryptography, the number of key require for authentication will increase with number of host in MANET increases and also key distribution will consume more bandwidth. But computational cost of symmetric key cryptography is less that asymmetric key cryptography. Hence we are proposing source authentication using application of symmetric cryptography but rather than using different key for different pairs we will use same key for all host but key will be different for different time duration. we have propose the timed, efficient, streaming, loss-tolerant authentication protocol called MKAuth(Multi Key authentication) technique, which use delayed discloser of symmetric key cryptography base authentication technique. MKAuth provides low computational overhead for generation and verification of authentication information, low communication overhead, robustness for packet loss, scale to large number of receiver.

II. RELATED WORK

Public key cryptography such as Elliptical key cryptography has been propose for solving problem of source authentication. However, ECC base scheme and Identity based scheme [10] suffer from energy consumption as well as significant communication and computation cost.

Qiwei Lu, Yan Xiong and Huang propose a Distributed ECC-DSS Authentication Scheme Based on CRT-VSS and Trusted Computing in MANET [4]. A secret key distributed storage scheme based on CRT-VSS and trusted computing is proposed for MANET. Besides, efficiency performance of such Schemes is not good enough due to the exponential arithmetic with Shamir's scheme.

Striki and Baras [12] proposed technique for integrating key distribution with entity authentication for efficient, scalable and secure group communication in MANET. In this, key management ensures communication security among nodes and the capability of their cooperation as a secure group. It consists of key generation, user

authentication and key distribution services. In this work, addressing key distribution, group key generation, entity authentication: it is emphasized that entity authentication should be designed with key distribution algorithms in mind and vice versa. The drawback of system is that, central authorization entity is assumed at all times for all nodes makes the task of network operations more difficult and indicates the need for distributed algorithms to provide the functions of centralized entities.

Zhou and Hass [13] have proposed to use threshold cryptography to secure MANET. They proposed a distributed certificate authority to issue certificate. This technique fails to address challenges in ad hoc network because of only selected nodes can be used as certificate authority and contacting distributed certificate authority in MANET is difficult.

III. BACKGROUND DETAILS

A. Time Synchronization:

The architecture of our propose system require sender and receiver to be loosely time synchronous and that receiver knows the upper bound on sender local time. The receiver issues times synchronization request at time $t_{R,}$ at which time the sender clock is at time t_1 The sender responds to request at its local time $t_{s.}$ The receiver only interested in upper bound on sender's times.

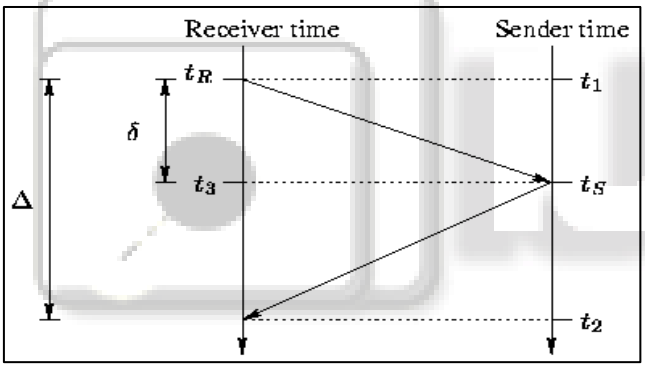

Fig. 1: Time Synchronization process

When receiver has its time tr, it compute the upper bound on current sender time as $t_s \leq t_r - t_R + t_S$[9]. Public key cryptography such as Elliptical key cryptography has been propose for solving problem of source authentication. However, ECC base scheme and Identity based scheme [10] suffer from energy consumption as well as significant communication and computation cost.

IV. PROPOSE SYSTEM

Our propose system is application of symmetric key cryptography for source authentication. By considering nature of communication in mobile adhoc network, rather than using unique key between each pair as in symmetric cryptography, we will use same key between all hosts for signing the message. We will use different key for different time duration and receiver of packet able to verify whether key use to sign the message is authenticate using key of previous time duration. MKAuth assumes that receivers are loosely time synchronous with sender up to some synchronization error Δ, all parties are agree on current time. To achieve source authentication in MANET, sender slit up time into interval of uniform duration. Sender will generate chain of seed value by repeatedly applying same hash function and sender will use those seed values in reverse order to generate the keys.

So whenever sender want send packet, will sign that packet using key for that duration and disclose that key in the network. So receiver can check whether packet has come from authenticate source by verifying sign using key of that duration and also verify whether key is authenticate by applying hash function on disclose seed value, will generate seed of previous duration as they are generated by repeatedly applying hash function . If Key for that duration is not disclosed yet it will buffer that packet until discloser of key.

V. CONCLUSION

With proliferation of mobile adhoc network, security becomes main concern due to resource constraint and dynamic nature of MANET. The traditional techniques do not work for MANET. So any malicious user can join the network and can inject the packet with malicious intends. Our propose system can solve the problem source authentication with less computational overhead.

VI. ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1] Quansheng Guan, Richard Yu, "Joint Topology Control and Authentication Design in Mobile Ad Hoc NetworksWith Cooperative Communications", IEEE Transactions on Vehicular Technology, VOL. 61, NO. 6, JULY 2012.
[2] Na Ruan, Yoshiaki Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things", 2012 International Conference on Selected Topics in Mobile and Wireless Networking, pp 60 65, Apr. 2012.
[3] yadev Maity and R. C. Hansdah, "Membership Models and the Design of Authentication Protocols For MANETs", 26th International Conference on Advanced information Networking and Applications Workshops, pp 544-551, July 2012.
[4] Qiwei Lu; Yan Xiong; Wenchao Huang; Xudong Gong; Fuyou Miao, "A Distributed ECC-DSS Authentication Scheme based on CRT-VSS and Trusted Computing in MANET", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 656 665, 2012.
[5] Maity, S.; Hansdah, R.C., "A Secure and Ecient Authentication Protocol (SEAP) for MANETs with Membership Revocation", 27th International Conference on Advanced Information Networking and Applications workshops, pp 363 370, 2012
[6] S.Neelavathy Pari, Sabarish Jayapal, "A Trust System in MANET with Secure Key Authentication Mechanism", Department of Computer Technology, Anna University, India, pp 261 265, August 2012.
[7] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of security in large-scale wireless ad hoc

networks", IEEE/ACM Trans. Netw., vol. 19, no. 2, pp. 319332, Apr. 2011.

[8] Zhang Tao; Yue Kang; Yao Jinkui, "A distributed anonymous authentication scheme for Mobile Ad hoc network from bilinear maps", International Conference on Mechatronic Science, Electric Engineering and Computer, pp 314 318, 2011

[9] Jason L. Wright; Miloc Manic," Time synchronization in Hierarchical Tesla Wireless Sensor Network" IEEE., 2009

[10] F. Hess, "Efficient identity based signature Schemes base on pairing" in Proc. SAC, St. John's Newfound and, Canada, August2002.

[11] Tang, H.; Salmanian, M., "Lightweight Integrated Authentication for Tactical MANETs", The 9th International Conference for Young Computer Scientists.

[12] Striki, M.; Baras, J.S., "Towards integrating key distribution with entity authentication for efficient, scalable and secure group communication in MANETs"

[13] L. Zhou and Z. Haas," Securing ad hoc netwok. In preceeding IEEE network volumn 13, pages 24-30, 1999.

