Scientific Journal Impact Factor (SJIF) : 1.711

IJMTER International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

MKAuth: Multikey Authentication For Multicast MANET

Ranjeet Pawar[1], Vidya Chitre[2]
[1]*Computer Engineering,BVIT,Navi Mumbai*
[2]*Information technology,Vidyalankar inst.of technology,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 adhoc 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. MKAuth use symmetric cryptography with delayed discloser of key for each time interval. The evaluation result shows the effectiveness and efficiency of propose solution.

Keywords— Authentication, Mobile adhoc Network, Multicast, time synchronization ,hash chain

I. INTRODUCTION

Due to low cost and ease of deployment associated with wireless devices wireless network become the dominant choice for connecting to internet. Ad hoc and multihop wireless networks becoming increasingly important for varieties 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.

MANETs are particularly vulnerable to malicious attacks. Thus security is a challenging problem since node exhibit low computational and energy power. An adversary can easily profit from wireless communication which is difficult to protect since it is base on a broadcast medium. An malicious user may eavesdrop, intercept, inject, eventually transmit data [2]. Thus it is important to ensure that information transmitted within MANET is valid and send by claimed source. Although Cooperative communication (CC) brings significant benefit in MANET, it presents significant challenge to security [1]. MANET faces various challenges like self organization, neighbor and topology discovery, medium access control, routing, security; our work focus is 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 applications[1]. In particular CC-MANET has more challenges for secure routing, key exchange and management because of multihop routing, packet forwarding, and lack of infrastructure, dynamic topology and node cooperation.

Source authentication means that a receiver ensures that the received data is sent by the claim source. An important amount of research effort was dedicated to the problem of source authentication. Existing unicast authentication mechanism such as transport layer security or IPSEC are not work in multicast setting of MANET. Also asymmetric cryptographic base technique such as digital signature, in which sender generate signature on message using his private key and all the receiver in the network can verify signature attached to message using senders public key. However it achieve authentication and non repudiation, digital signature impose very high computational cost for both sender and receiver. In addition digital signature consumes more the bandwidth requirement. Also symmetric MAC base authentication mechanism are not secure in multicast environment because key is known to all receiver, so potential malicious user can impersonate as sender and inject the packet in network.

In this paper, to solve the source authentication problem for multicasting in MANET, we have propose the timed, efficient, streaming, loss-tolerant authentication protocol called MKAuth (Multi Key Authentication for MANET) which use delayed 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. In MKAuth require sender and receiver to be loosely time synchronized and either sender or receiver must buffer message. As this protocol use symmetric key cryptography for authentication, but delays the authentication of receive message, it achieves the property of Asymmetric base cryptographic technique.

II. RELATED WORKS

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 use as certificate authority and contacting distributed certificate authority in MANET is difficult.

III. OVERVIEW AND BASIC CONCEPTS

3.1. Time Synchronization

The architecture of our propose system require sender and receiver to be loosely time synchronous 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. 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].

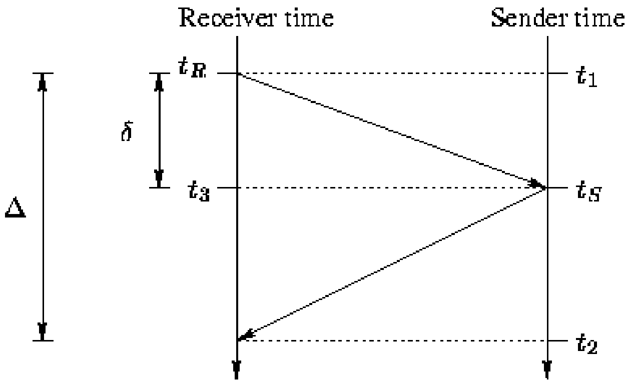


Figure 1. Time Synchronization process

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.

3.2. Hash Chain

Hash chain is successive application of cryptographic hash function [2]. It produces many onetime keys from single key and password.

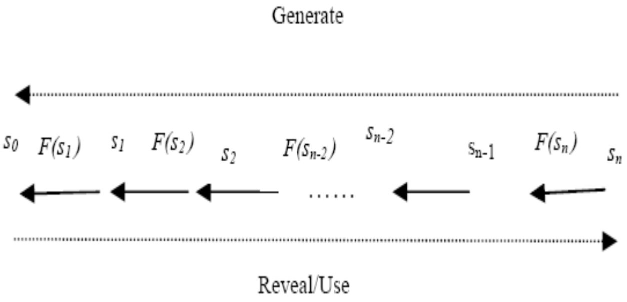


Figure 2. Hash Chain

Figure. 2 illustrate the mechanism of one way chain. In fact given a random key, use can repeatedly apply one hash function in order to generate chain of keys. The generated keys are use in reverse order So whenever receiver receives a key *K*i or *Si,*_it can verify that using last stored key *K*j. If (*K*i=F$^{|i-j|}$ (*Kj*)) then *Ki* is successfully verified, otherwise verification failed.

IV. PROPOSED SOURCE AUTHENTICATION SCHEME

The goal of the MKAuth is to provide source authentication in MANET especially for multicast communication in multihop cooperative communication. To achieves the authentication MKAuth use delayed per packet authentication technique that delays the discloser of symmetric key for that time interval. MKAuth assumes that receivers are loosely time synchronous with sender upto some synchronization error Δ, all parties are agree on current time.

To achieve source authentication in MANET, sender slit up time into intervals of uniform duration. The sender of packet forms the one way chain of key values. The sender node in MANET defines the discloser time for one way chain values, usually on order of few time intervals. A time slot n is assigned the key tK_n and packet generated during this time interval are signed using this key. At the same time in the future, the node will disclose the seed value use to generate this key, S_n, of that particular duration and all nodes in MANET can verify signature and key disclose for that time interval.

Algorithm: MKAuth_Source

```
INPUT: Random seed value s$_l$
List seeds=hashchain( s$_l$ );
divide_timeinteval ();
synchronize_nodes();
Integer i=0; // starting of time interval.
While (1)
{
  Massage: = generate_massage ();
  Key$_i$: = generate_key (seed$_i$ );
  Singner (Massage, Key$_{i)}$;
  Send (Massage + Sign);
  If (predefine time)
  {
      Disclose(seed$_i$);
  }
}
```

So whenever sender want send packet, will sign that packet using key for that duration and disclose seed value to generate key tK_n, for that particular duration. 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 S_n, 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.

The protocol uses two publically known hash functions, F$_1$ and F$_2$. F$_2$(sn) = sn -1 is use to generate the seed value chain. F1 is use to compute the keys given the seed value, via Equation 1.

$$F_1(S_n)=tK_n \qquad (1)$$

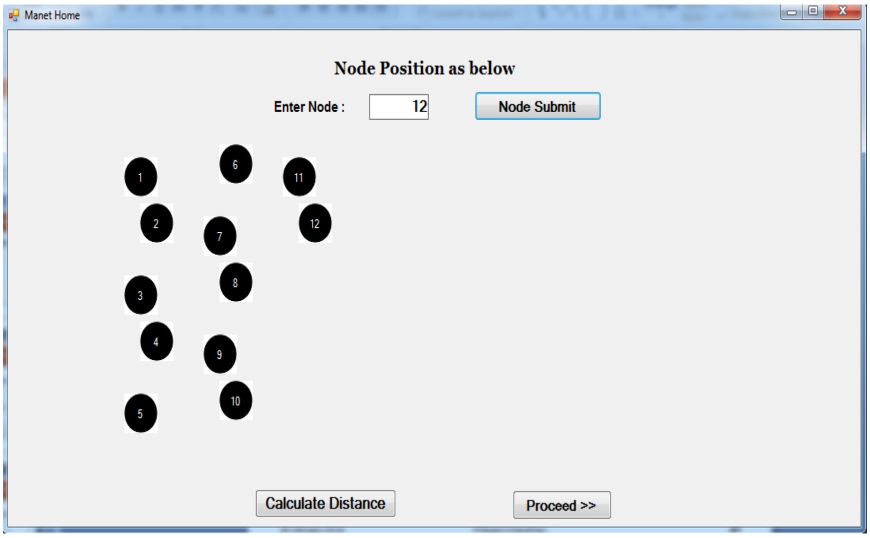
Whenever receiver nodes in MANET receive the packet, node will check whether key use to sign the MAC is still a secrete by determining node could not have reached the time interval of disclosing it. If key is still secrete, the receiver nodes in MANET will buffer the packet and then after sender disclose the key, each receiver will check correctness of MAC of buffered packet that have sent in time interval of the disclosed key.

```
Algorithm: MKAuth_Receiver
divide_timeinteval ();
synchronize_source();
Integer i=0; // starting of time interval.
While (1)
{
  If (seed_receive ())
  {
      seed$_i$ = seed_receiver();
      Boolean b= verifier (seed$_i$);
      If(b)
      {
        Key$_i$: = generate_key (seed$_i$ );
      }
  }
  If (MSG_receive (buffer))
  {
      msg$_i$ = MSG_receiver ();
```

```
        Integer interval=get_interval(msg_i );
        if(seed_available(interval))
       {
           Boolean b=verifier (Massage + Sign, Key_i);
           If (b)
          {
            Massage: = get_massage ();
          }
        }
        else
       {
         buffer_msg(msg_i);
       }
     }
   }
```

V. SIMULATION

We simulate MKAuth using custom C# base simulator. In custom simulator software, we have created different scenarios for cluster formation, routing, topology control and we consider random deployment of nodes in the network.



Enter Node : 12

Figure 3. An example of MANET

We use C#.NET 4.0 framework for simulation of topology control. In particular we use Collection classes for managing Iterators of node and hash map of nodes and path and set of nodes in cluster. We use system.form.* classes for GUI. We also use chart classes to plot the node to create MANET network of nodes.

VI. SIMULATION

We run our algorithm on several random network created by randomly distributing nodes. We developed custom simulation software to run simulation. Average number of neighbor node in network is 10. At the begging of simulation mobile node in network is randomly selected to initiate the group communication and six nodes are randomly selected to join the group. Simulation software set 90 sec interval to select a nodes to join and leave the network. The following table shows when number of nodes increase size of key produced by hash chain algorithm for authentication of source using different key for different time interval.

Table 1. Number of nodes Vs Key chain size

Sr No	No of nodes	Key Size
1	10	7961
2	20	15922
3	30	23890
4	40	31332

The following graph shows length of hash chain value generated by algorithm when number of nodes increases.

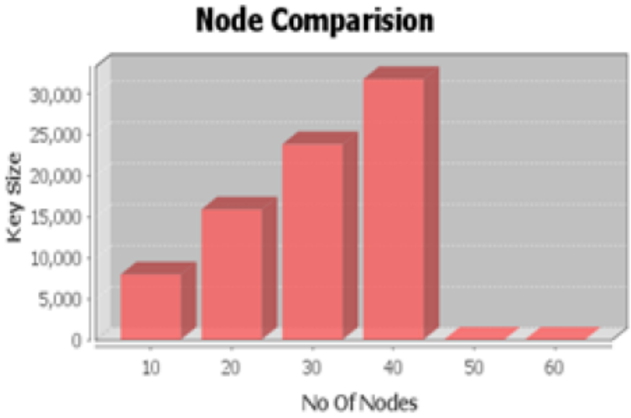


Figure 4. Graph of no of nodes verses key size

The following times ratio table summarize the time require to send the packet

Table 2. Number of packet Vs time

Sr No	No of packet	Time in second
1	10	2
2	20	3
3	30	4
4	40	5

Group establishment success ratio Vs Max speed figure shows max speed of nodes on group establishment success ratio. During experiments max speed of node in network varies from 0m/s to 60m/s to change the mobility. When nodes mobile speed keeps at 60m/s success ratio of MKAuth in key establishment is more than 85%.

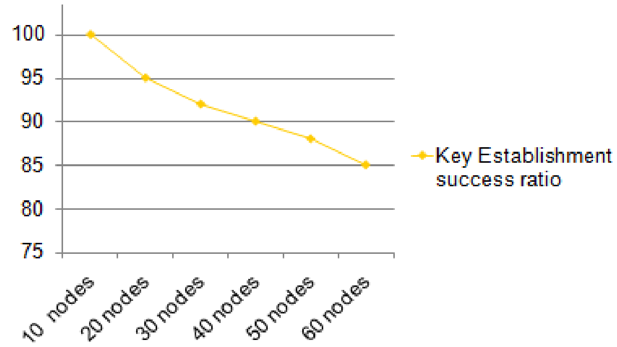


Figure 5. Key generation ratio

VII. 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 hence source authentication is real challenge for MANET due to dynamic topology control. To solve the source authentication problem we have proposed the delayed key discloser base on symmetric key cryptographic technique for source authentication which requires loose time synchronization. It scales well for multicasting in MANET. MKAuth provides low computational overhead for generation and verification of authentication information, low communication overhead, robustness for packet loss and scale to large number of receiver.

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] Soumyadev 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.