International Journal of Computer and Communication Technology

Volume 5 | Issue 2 Article 11

April 2014

An Efficient Authentication Protocol for Security in Mobile Ad Hoc Networks

Abdul Shabbir
Dept. of IT, CBIT, abdulshabbirs@gmail.com

Anasuri Sunil Kumar
Dept. of IT, CBIT, suneel8055@gmail.com

An Efficient Authentication Protocol for Security in Mobile Ad Hoc Networks

Abdul Shabbir & Anasuri Sunil Kumar

Dept. of IT, CBIT
E-mail : abdulshabbirs@gmail.com & suneel8055@gmail.com

Abstract **-** Mobile Adhoc Network(MANETs) is a collection of mobile nodes that communicate by forming a network dynamically that lacks fixed infrastructure and centralized control. Secure routing is of at most importance in such networks because of dynamically changing topologies, absence of centralized monitoring points and lack of clear lines of defense. This paper discusses a fool proof key exchange mechanism and a network model to protect the network containing malicious nodes. The reputation of a node increases as long as the node transfers the message properly and decreases otherwise. Moreover, it has minimum computation and communication overhead which makes it viable.

Key words **-** *AdHoc Network, Authentication, Clustering, Key Exchange, Network Model.*

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are a collection of independent mobile nodes that can dynamically self organize in temporary network topologies. The nodes in MANETs communicate with each other through radio waves. If the two nodes that wish to communicate are not in the radio range of each other, they have to depend on intermediate nodes to route their data packets.

This paper is organized as follows section 2 discusses related work. Section 3 sets out the key exchange mechanism and the network model. Section 4 presents the operations of public key certification, identification and isolation of malicious nodes and updating the reputation values of the nodes. Section 5 discusses the implementation results. Finally, our conclusions are set in Section 6.

II. RELATED WORK

The problem of security and cooperation enhancement among the nodes in a MANET has received considerable attention by the researchers over the last decade Cryptography has remained the backbone in most of the solutions to authenticate nodes. Several public key exchange management protocols have been proposed for wireless mobile ad hoc networks. Zhou and Hass proposed a partially distributed authority [1]that makes use of a (k,n) threshold scheme in distributing the services of the certificate authority to a set of special server nodes. Similar to partial distributed CA. Fully-distributed certificate authority proposed by Luo and Lu [2] extends the idea of the partially-distributed approach by distributing the certificate services to every node. Other solutions include the self-issued certificates proposed by Hubaux et. al[3]. It issues certificates by users themselves without the involvement of any certificate authority.

III. THE PROPOSED MECHANISM

The proposed mechanism discusses a key exchange mechanism and a Network model that is aimed at distinguishing the malicious nodes from the good ones.

3.1 The Key Exchange Mechanism

The aim of this mechanism is to obtain a path between source and destination nodes. To achieve this we make use of reactive routing protocols so that the route to destination is determined. The proposed mechanism uses the above approach to retrieve public keys. To find the certificate of a pubic key the source

node floods the network with intermediate node that knows the target node.

The authentication is based on certificate exchange that is, every node first generates a public/private key pair. Since the key pair is generated by node itself the node needs to authenticate with some of the members(or members in a cluster/members in the immediate hop) join them and access. Thus if some node A receives the public key of B then A issues certificate for the public key of B. Similarly B issues certificate for public key of A here due to multiple certifications of intermediate nodes the confidence assigned is higher.

Reputation of a particular node increases as more no of nodes confirm a given public key. It decreases if the certificate issued is spurious. If there is any conflict the certificate issued by more trustworthy node will be accepted as genuine.

3.2 Network Model

In general each node is capable of monitoring its neighbors. The cluster based approach improves the security. The monitoring will be more efficient in this approach. We divide the nodes into clusters having almost same number of Nodes, as show in Figure 1.

Nodes in a cluster will have same cluster ID. The cluster member that has the highest reputation value will become cluster head. Cluster ID will have no special meaning in the protection of network security.

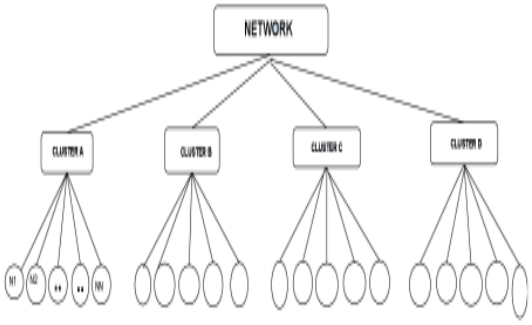

Fig. 1 : The Network Model

IV. OPERATION

Once a new node enters a network it requests certificates from other nodes in order to accomplish this it floods the network with request message(CRM) as shown in Figure 2.

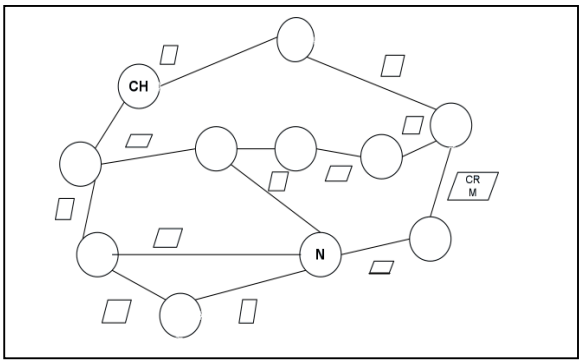

Fig. 2: New node requesting certificate

Before asking node A's certificate node B would evaluate the minimum reputation value that is necessary to consider the public key of A as safe. The minimum value of reputation depends on the node B's security requirements. Node B then sends certificate asking message(CRQ) that includes node A's address and the list of intermediary nodes as shown in Figure 3.If the intermediate node say I has no certificate for A or if its is already replied to the certificate request it simply forwards the packet.

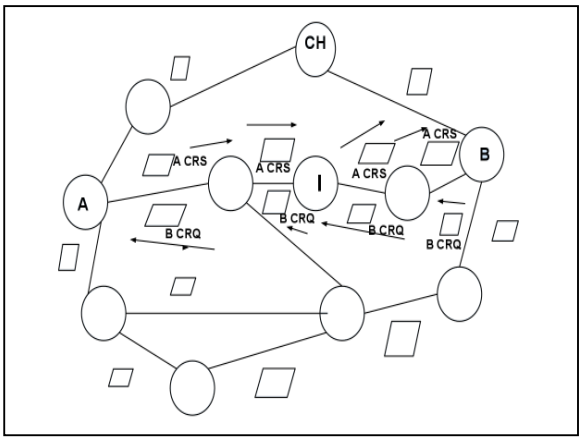

Fig. 3 : Certificate Exchange between nodes

Otherwise, the intermediate node I sends a certificate reply to B(ICRS) containing a certificate response containing A's public key as shown in Figure 4. A responds and sends a request(CRS) for B's public key .Since A and I know each other they can authenticate .The interaction between them is safe. Therefore no node can corrupt the certificate of B issued by I.

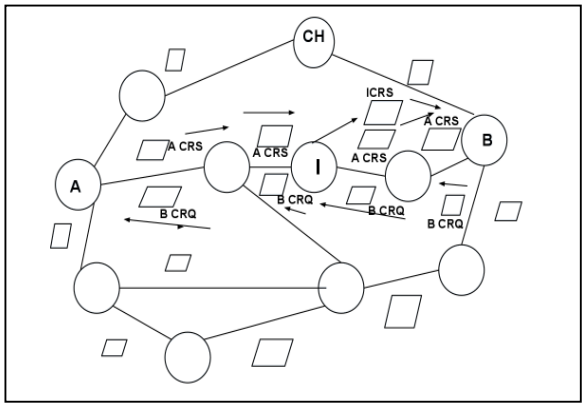

Fig. 4 : Role of intermediate node

B repeats the operation until it receives the required number of certificates after receiving them B sends the first packet to A .Which has the details of all the nodes which authenticate node A. In this way node A gets information about all the affirmers of B. Once they exchange their keys. They exchange certificates with one another.

V. SIMULATIONS

In this section we evaluate the security performance of the authentication service.

Experimental setup:

The simulations have been carried out using Berkeley (NS-2) Network simulator [7] [8]to analyze the effects of security exposures on various network functions such as routing and packet forwarding.The main objective was the evaluation of network performance in terms of total number of packets forwarded and delay when a certain percentage of nodes were found to be misbehaving.

Throughput T=(Number of packets received)/(Number of packets sent).

Table 1: Simulation Parameters

Parameters	Values
Area	1000X1000 m
Radio Range	250m
Link Cap	2 mbps
Pause Time	5sec
Simulation Time	200sec
Buffer Size	50Packets
Packet Size	512 bytes

Table 1 shows the parameter settings for our experiment

The variable parameters are

Network Density: high(60 nodes),Low(20 nodes)

Mobility: high(15m/sec),Low(2m/sec)

Routing Protocol : DSR

The results obtained from the simulations carried out show that throughput goes on reducing as the number of malicious nodes increases. This simulation result is shown in Fig 5. But the rate at which the packets are lost is better when compared with other mechanisms.

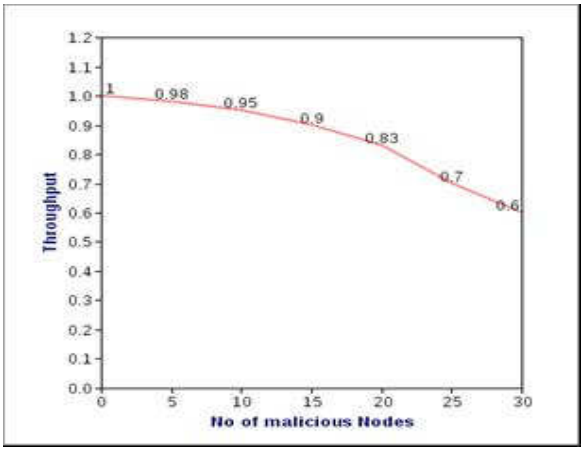

Fig. 5 : Throughput Vs No. of Malicious Nodes

Delay increases as the number of malicious nodes increases. This simulation result is shown in Fig 6. Again the delay due to malicious nodes is little when compared with other approaches.

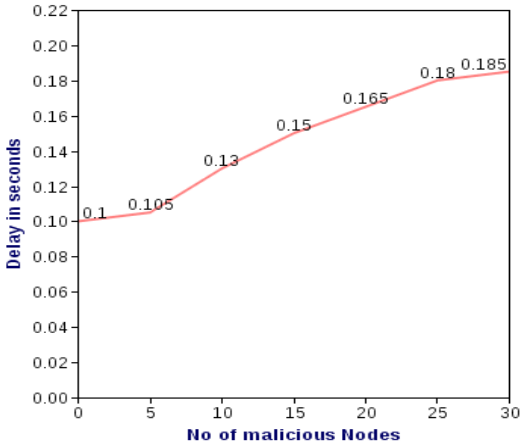

Fig. 6 : Delay VS No. of Malicious nodes

VI. CONCLUSION

In conclusion, a secure, scalable and distributed authentication mechanism that improves the genunity of public key certification in Mobile Adhoc networks. The network model is cluster based this helpd in behaviour monitoring and provides high availability for public key certification. The protocol is robust against isolated attacks launched by malicious nodes it works equally well against cooperative attacks in a network. The solution provides wider applicability in many areas of network security.

REFERENCES

[1] L. Zhou and Z. J. Hass,"Securing Ad Hoc Networks," IEEE Networks Special Issue on Network Security,November/December, 1999.

[2] H. Luo and S. Lu, "Ubiquitous and robust authentication services for ad hoc wireless networks," Tech. Rep. TR-200030, Department of Computer Science, University of California, Los Angeles, Los Angeles, Calif, USA, 2000.

[3] J-P. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," Proc. 2001 ACM International Symposium on Mobile ad hoc networking & computing, pp. 146–155, Long Beach, CA, USA, 4-5 October 2001.

[4] ZhengYan, PengZhang, Teemupekka Virateen, "Trust Evaluation Based Security Solution in Ad Hoc Networks".

[5] A. Abdul-Rahman, "The PGP trust model," EDI-Forum: the Journal of Electronic Commerce, April 1997, Available at http:// www.cs.ucl.ac.uk/ staff/F.AbdulRahman/docs/.

[6] William S., Cryptography and network security (2nd ed.): principles and practice: Prentice-Hall, Inc., 1999.

[7] Z:\cs757_2004fall\cs757-ns2-tutorial1.prn.pdf "Ns2 tutorial"

[8] http://netlab.caltech.edu/projects/ns2tcplinux "Ns2 Tutorial"

❑❑❑