Securing Routing Protocol by Distributed Key Management and Threshold Cryptography in Mobile Ad hoc Network

Neha Gupta[1], Manish Shrivastava[2]

Abstract

Security is a major concern in mobile ad hoc network due to its various characteristics like infrastructure less nature, self configuring etc. Threshold cryptography used in key distribution of mobile ad hoc network enhances security by distributing each part of the divided secret key to each node. It is an effective technique as it refreshes the shares of each share holder periodically. It maintains the security by interchanging the shares among its share holders to prevent unauthorized access. In this paper we are using Threshold cryptography concept on ad hoc on demand distance vector routing protocol to increase the security of mobile ad hoc network. In this paper I propose a secured approach which I call secure ad hoc on demand distance vector and showing the behaviour of throughput, packet delivery ratio, average end to end delay and routing overhead of AODV and SAODV.

Keywords

Mobile Ad hoc network, Ad hoc on demand distance vector, secure ad hoc on demand distance vector, certificate Revocation list.

1. Introduction

A mobile ad hoc network is a self organized wireless network where mobile nodes can communicate with each other without reliance on a centralized authority. We cannot assume a trusted certificate authority and a centralized repository that are used in ordinary Public key infrastructure (PKI) in ad hoc network because nodes in a MANET can dynamically join and leave the network. All nodes can potentially be used as a router or servers . The characteristics of MANET pretense a number of challenges to security such as self-configuring, wireless links, infrastructure less nature. The characteristics make MANET good for military scenario, emergency situations, and rescue operations. But security in ad hoc network is difficult to achieve. A traditional key management service uses a certificate authority and trusted third party to issue public key certificates to all nodes in the network. This scheme is not appropriate in mobile ad hoc network due to its mobility characteristics. Distributive key management schemes can only be an effective approach in mobile ad hoc network.

Neha Gupta, M.Tech Scholar, Dept. of Information Technology, LNCT, Bhopal, India.
Manish Shrivastava, Head, Information Technology, LNCT, Bhopal, India.

2. Literature Review

In 2012, we have presented [1] different approaches used for key distribution and management of mobile ad hoc network. In this section I present an overview of the approaches. To overcome the limitation of distribution of public key certificates, in 2003 and 2007, S.Yi and R.Kravets and J.van der Merwe [2] [3] proposed that nodes are preloaded with public key certificates before the network formed. This approach is not effective because it is not scalable when the network size increases. As the network grows, key updation will be a problem.

In 2005, Y. Kitada, A. Watanabe, K. Takemori, and I. Sasase [4] proposed an on demand distributed public key management for wireless adhoc network. This scheme overcomes the limitation of conventional system. In conventional system a node authenticates another node’s public key and stores its certificates in a certificate repository. The node checks the authentication of a node by collecting all the certificates that make up a chain of public key certification. In addition, to verify the public key certificates making up the certificate chain, each node has to manage a CRL which is a list of invalid certificates in its repository. The disadvantage of this approach is that the amount of memory requires in storing the certificates is more. There is also need to check the validity of certificates periodically to verify the validity of certificates. When only a few certificates are stored in the repository, a failure probability of authentication increases.

To solve above problem, proposes an architecture of an on demand distributed public key management for wireless ad hoc network. In this approach, a node collects certificates of a certificate chain on demand. They propose an ASNS protocol to find a certificate chain. In the ASNS protocol, each node holds in its local repository only certificates that other node issued to it in order to reduce the memory size. A request node broadcast the search packet within its power range. If the trusted node is not the neighbor of the request node, it cannot receive the packet. In that condition ASNS broadcast the search packet to all of the trusted nodes. Search packet contains both the authentication request and the routing table information of the trusted nodes. The problem with ASNS is high communication cost because of broadcasting packets with certificates regardless of the fact that even some of the nodes do not need the certificates.

To overcome the limitations of discovering certificate chain discovery, in 2004 and 2007, H.K.R.Li and H.Mohri, I. Yasuda, Y. Takata, H. Seki [5] [6] proposed a new approach certificate chain discovery in web of trust for ad-hoc network. It divides it in two phases-Certificate searching and certificate collecting phase. It uses a distributed algorithm for constructing a spanning tree where the root node is the source node. Each node knows the number of hops to any other node by using a routing protocol.

When the certificate searching phase is completed, all nodes do not know about the entire path, they only have the idea about the source node. To overcome this problem [6] proposed the solution. In certificate chaining collecting phase destination node send a packet to the parent node. Each intermediate node that received the packet adds its own certificate to the packet and sends it to its parent node. When this process is completed, the source node obtains the entire certificate in a certificate chain. This scheme suffers from the delay and the traffic required is more. In 2009, H.Dahshan and J.Irvine [7] proposed a self organized, hop by hop public key management for MANET based on transitive trust between mobile nodes. Each node creates its public key and the corresponding private key locally by the node itself, issuing certificate to neighboring nodes and holding certificates in its local certificate repository. Authentication of public keys is performed by using both direct and recommendation trust. In 2002, J. B. L. Eschenauer, V.D. Gligor [8] explained transitivity of trust Establishment. If A accepts B's authentication of any entity registered by B and B accepts C's authentication of entity D registered by C, it mean that A accepts C's authentication of entity D registered by C.

In 2009, H Dahshan and James Irvine [9] proposed an on demand self organized public key management for mobile ad hoc network. It allow each user to create its public key and the corresponding private key, to issue certificate to neighboring nodes before joining the network by the node itself. Each node stores a certificate in the certificate repository which it issued or issued to it by others. Each certificate contains the node identity/network address, certificate generation and validity time. Certificate chain discovery will be performed with the help of the routing infrastructure.

Threshold scheme is a different scheme from the above approaches. In 1979, Shamir [10] proposed that secret key is divided into n shares and gives that to nodes called share holders. When a new node joins the network, minimum t nodes are needed to sign a certificate for that new node. Consider, for example, a company that digitally signs all its checks [11]. If each executive is given a copy of the company's secret signature key, the system is convenient but easy to misuse. If the cooperation of all the company's executives is necessary in order to sign each check, the system is safe but inconvenient. The standard solution requires at least three signatures per check, and it is easy to implement with a (3, n) threshold scheme.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes *k* points to define a polynomial of degree ***k-1***.

In 2004, J. H. S. Yi and R. Kravets [12] proposed composite key management for ad hoc network. To adapt PKI in ad hoc network, threshold cryptography is used to provide a virtual certificate authority comprised of multiple nodes that perform security services.. Composite key management adapts the benefit by combining virtual CA and certificate chaining approach. Composite key management uses a virtual CA and certificate chaining simultaneously in a single ad hoc network. It describes a virtual CA composed with 1 hop certificate chaining approach; only nodes that have been certified by the virtual CA are allowed to issue certificates to their nodes. Certification graph includes public/private key pair and a digital certificate. It includes the identity of the key holder and confidence value, the level of confidence the certificate issuer has.

This approach is not suitable for a fully self organized mobile ad hoc network because issuing certificates is restricted to nodes that have CA certificates. Only 1 hop certificate chaining is used.
To overcome the limitations of composite key management scheme, in 2009, H Dahshan and James Irvine [13] proposed a trust based threshold cryptography key management for mobile ad hoc network. In this scheme, a share holder node is configured with the public key of CA and a share of the Ca private key. Each user creates its own public key from the Ca private key share. When a node k is trusted by minimum n share holders, node k has n no of certificates in its repository. Node k can combine these partial signatures and obtain a certificate signed by n nodes. Every node can check the validity and authenticity of those certificates. In this scheme a node can issue certificates to directly trusted nodes and certificate chaining is used to authenticate the route from source to destination.

3. Proposed work

Public key infrastructure (PKI) enables the easy distribution of keys and is a scalable method. Each node has a public/private key pair, and a certifying authority (CA) can bind the keys to the particular node. But the CA has to be present at all times, which may not be feasible in ad hoc wireless networks. It is also not advisable to simply replicate the CA at different nodes. In this approach I am using the concept of Threshold cryptography. I applied this concept on AODV protocol which I say SAODV. AODV protocol is a flat routing protocol, it does not need any central administrative system to handle the routing process. It is a routing protocol but security is still undone. In this paper I am securing the routing cryptography concept and study the behavior of Throughput, packet delivery ratio, Average end to end delay and routing overhead.

In Threshold cryptography approach (t, l), CA private key is divided into l shares according to a random polynomial and kept by l nodes called share holders. when a new node wants to join the network, at least t nodes need to cooperate and sign the certificate for new node. Minimum t nodes are needed to form a CA private key.

Initially CA private key is divided into share holders. Source node that wants to send data follow these steps-

1. Source node constructs the key by taking key shares from at least minimum share holders.
2. It encrypts the data with the private key of CA.
3. Send the encrypted data to destination node.

Destination node that wants to receive data follow these steps-

1. Destination node constructs the key by taking key shares from minimum share holders.
2. It decrypts the data with the private key of CA.

4. Algorithm

Given a secret value s and a set of participants $P = \{ P_{1,}\ldots\ldots P_l \}$, a (t, l) threshold scheme, where 1<=t<=l is a method of dividing s into an array s_i of shares such that-

1. When given any set t or more of $s_{i,}$ the secret value s can be reconstructed.
2. When given any set less than t of $s_{i,}$ the secret value s cannot be determined.

Distribution Phase-

Distribution algorithm takes the secret s and split s into p share according to random polynomial and distribute the shares to share holder. Each share holder P_i received a secret $s_{i.}$

```
// secret s
Step 1- A set $P = \{P_1\ldots\ldots\ldots P_t\}$
//P is the no of Participants
// A threshold value $t \leq 1$

Step2- $r_1\ldots\ldots\ldots r_{t-1} \in_R$
// select random values

Step3- $r(x) = s + r_1x + \ldots\ldots\ldots r_{t-1}x^{t-1}$
// Construct Polynomial

Step4- for each $P_i$ P
          Do send
        Share $s_{i\,=}\, r_i$ to $p_i$
// A set $\{s_1\ldots\ldots s_t\}$ of shares for each $P_i$
```

Reconstruction Phase-

The reconstruction algorithm collects each share s_i

from share holder P_i and uses that shares to construct the secret s. Minimum shares are needed to construct the secret key.
// A set $X \subset \{ P_1 \ldots\ldots\ldots P_t \}$ of size t participants
// In order to reconstruct the secret

Step1- A set of shares s_i from each $x_i \in X$
// we have taken the shares(t) value from the set to reconstruct the secret.

Step2- $s = \sum_{x_i \in X} s_i \lambda X_{, xi}$ with

$$\lambda_{X, xi} = \prod_{j \in x(i)} (j/j-1)$$

// By using LaGrange Interpolation to combine the shares and extract the secret.

5. Simulation Environment

Simulations were performed using NS-2 [14]. NS-2 is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication network. Ad hoc on demand distance vector (AODV) routing protocol was chosen for the simulation. I have simulated the approach on over environment with 100 nodes spread over area of 600*600 meters^2. The MAC layer protocol IEEE 802.11 is used in simulation. Simulation time is 100s. Propagation model is TwoRayGround and mobility model is Random Waypoint. The ns-2 constant bit rate (CBR) traffic generator is used to set up the connection pattern. For simulating data transfer maximum number of packets are 10,000. Packet size is 512 byte and routing protocol used is User datagram protocol (UDP).

6. Result

To evaluate the performance of our approach, AODV has been implemented in a network simulator NS-2 and threshold cryptography is implemented over it. The simulation result of our proposed approach (SAODV) are presented along with the simulation result of AODV protocol. AODV is the routing protocol without any modification.

I have selected the Throughput, Packet delivery ratio, Average end to end delay, Routing overhead during the simulation in order to evaluate the effectiveness of the proposed scheme.

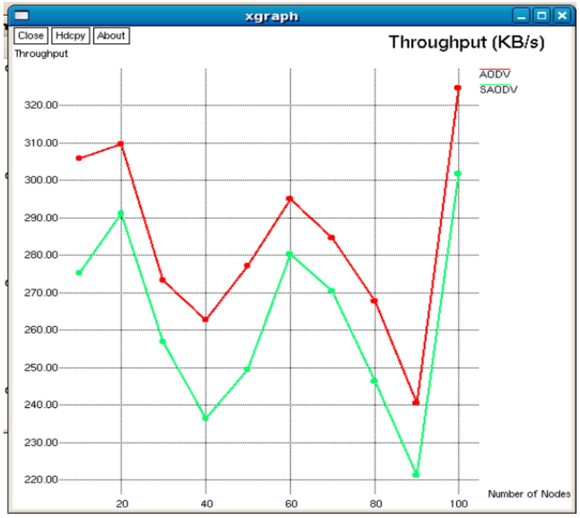

Figure: 1 Throughput in terms of kBps

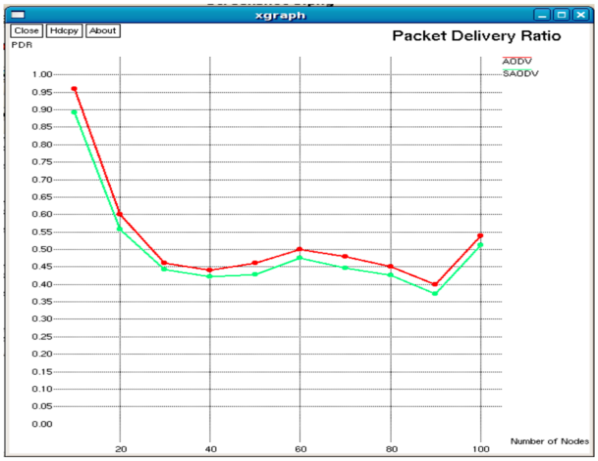

Figure: 2 Packet delivery ratio

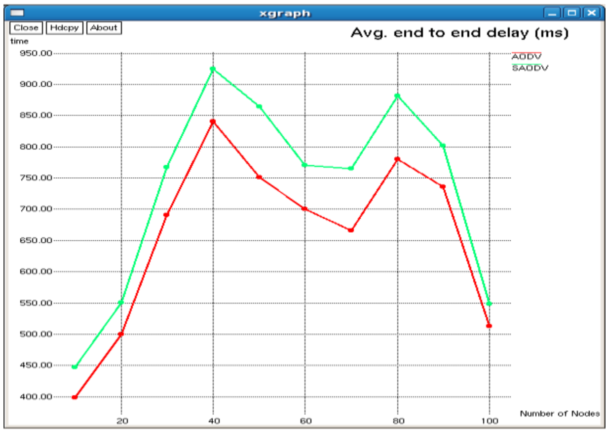

Figure: 3 Average end to end delay

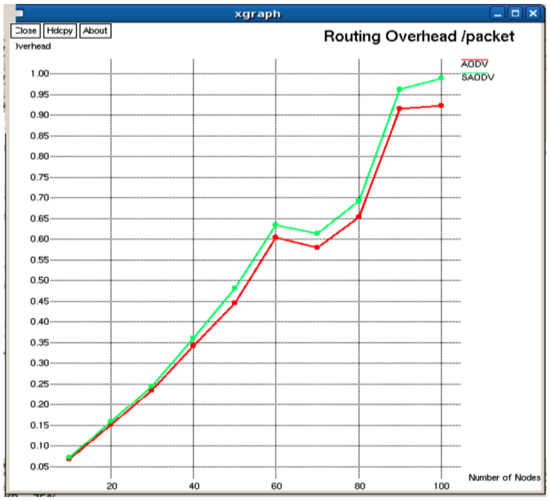

Figure: 4 Routing overhead

Figure 1 shows the Throughput of our proposed scheme SAODV and the AODV protocol. Throughput is the average rate of successful message delivery over a communication channel. It shows that throughput decreases when we are providing security in SAODV as compared to AODV. Figure 2 shows the Packet delivery ratio of our proposed scheme SAODV and the AODV. Packet Delivery ratio is the ratio of data packets delivered to destination to those generated by sources. It shows that increasing security decreases the packet delivery ratio. Figure 3 shows the average end to end delay. This includes all possible delays caused due to queuing, retransmission delay and route discovery. Delay also increases in SAODV as compared to AODV. Figure 4 shows the routing overhead. Overhead is the ratio of the total number of routing packets to data packets transmitted during the simulation. Overhead increases when security is provided in AODV.

I have shown the result in tabular form. I have taken key size 32, 48,64,96,128 bit, based on which I have presented the AODV and SAODV values. To show result I have considered node 40.

Table: 1 Throughput

Key size	AODV(KBps)	SAODV(KBps)
32 bit	253	249
48 bit	253	245
64 bit	253	240
96 bit	253	238
128 bit	253	232

Table: 2 Packet Delivery Ratio

Key size	AODV	SAODV
32 bit	44%	43%
48 bit	44%	42%
64 bit	44%	40%
96 bit	44%	39%
128 bit	44%	36%

Table: 3 Average End to End Delay

Key size	AODV (ms)	SAODV(ms)
32 bit	740	790
48 bit	740	820
64 bit	740	860
96 bit	740	900
128 bit	740	920

Table: 4 Routing Overhead

Key size	AODV	SAODV
32 bit	0.38	0.38
48 bit	0.38	0.39
64 bit	0.38	0.40
96 bit	0.38	0.42
128 bit	0.38	0.45

7. Conclusion and future work

Threshold cryptography used in key distribution of mobile ad hoc network enhances security by distributing each part of the divided secret key to each node. It is an effective technique as it refreshes the shares of each share holder periodically. It maintains the security by interchanging the shares among its share holders to prevent unauthorized access. In this paper I used threshold cryptography concept on AODV protocol. Results in tabular form depicts the behavior of Throughput, Packet delivery ratio, Average end to end delay and routing overhead. In case of AODV, when there is no encryption and key distribution concept AODV values remain constant. With secret key concept on SADV, there is gradual decrease in throughput and Packet delivery ratio and increase in average end to end delay and routing overhead. The purpose of this approach is to show the network performance that is not degraded too much when security is achieved. In future work I will increases scalability and security by incorporating more distributed CA to enhance the performance.

References

[1] Neha Gupta, Manish Shrivastava, ”Survey paper on different approaches of threshold cryptography,” International Journal of Advanced Computer Research (IJACR) volume 2, Number 3, Issue5, September 2012.

[2] S.Yi and R.Kravets,”Moca: Mobile certificate authority for wireless ad hoc network”, in proceedings of the 2nd Annual PKI Research Workshop (PKI 2003), 2003.

[3] J.VanderMerwe, D.Dawoud and S.McDonald, ”Key distribution in mobile adhoc networks based on message relaying, “in fourth European workshop on security and Privacy in Adhoc and Sensor Networks,july2-3,2007.

[4] Y. Kitada, A. Watanabe, K. Takemori, and I. Sasase, “On demand distributed public key management for wireless ad hoc network”’ in IEEE Pacific Rim Conference on Communication, Computers and Signal Processing, 2005.

[5] H.K.R.Li, J.Li and P.Liu, “Localized Public key management for mobile adhoc network”, in IEEE Global Telecommunications Conference, 2004, pp, 1284-1289.

[6] H.Mohri, I. Yasuda, Y. Takata, and H. Seki, “Certificate chain discovery in web of trust for ad hoc networks,” in proceeding of the 21st International Conference on Advanced Information Networking and Applications workshop, IEEE Computer Society, vol.2,pp,2007.

[7] H.Dahshan and J.Irvine, “Key management in web of trust for mobile adhoc networks,” in IEEE 23rd International Conference on Advanced Information Networking and Applications, 2009.

[8] J. B. L. Eschenauer, V.D. Gligor, “On trust establishment in mobile ad-hoc networks,” in Proceedings of the Security Protocols Workshop, Cambridge, 2002.

[9] H Dahshan and James Irvine, "On demand self organized public key management for mobile ad hoc network," in IEEE 69th Vehicular Technology Conference: VTC2009-Spring, 2009.

[10] Shamir, "How to share a secret," Communication of the ACM, vol.22, pp. 612–613, 1979.

[11] Rivest, R., Shamir, A., and Adelman, L. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM 21, 2(Feb. 1978), 120-126.

[12] J. H. S. Yi and R. Kravets, "Composite key management for ad hoc networks," in First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous’04), pp.52–61, 2004.

[13] H Dahshan and James Irvine, “Trust Based Threshold cryptography key management for mobile ad hoc network”, Department of Electronics and Electrical engineering, 2009.

[14] K. Fall and K. Vardhan, "The network simulator (ns-2)",Available at:http://www.isi.edu/nsnam/ns.

I did B.E (IT) from Institute of Technology and management, Gwalior in 2007. Currently I am Pursuing M.tech from Laxmi Narayan college of Technology Bhopal.