International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-3 Issue-5 September-2012

Survey paper on different approaches of Threshold Cryptography

Neha Gupta[1], Manish Shrivastava[2], Aditya Goel[3]
M. Tech Scholar, Department of Information Technology, LNCT, Bhopal, India[1]
Head, Information Technology, LNCT, Bhopal, India[2]
Head, Electronics and Communications, MANIT, Bhopal, India[3]

Abstract

A traditional key management service is based on a Certificate Authority or a Trusted Third party. Security solutions for traditional network are not suitable for Mobile ad hoc network. The characteristics of MANET presence a number of challenges to security such as self-configuring, wireless links, infrastructure less nature. Threshold cryptography has proved to be an effective technique for key distribution and management. In this paper we highlight the different approaches used for certificate generation, discovering and authentication of public keys.

Keywords

Mobile Ad hoc network, certificate authority, Ad hoc simultaneous search protocol, certificate revocation list

1. Introduction

A ``network'' has been defined as ``any set of interlinking lines resembling a net, a network of roads an interconnected system, *a* network of alliances." We need to protect the network because there are constant threats against the resources we share in the network. In a generic sense, security is "freedom from risk or danger." In the context of computer science, The ongoing and redundant implementation of protections for the confidentiality and integrity of information and system resources so that an unauthorized user has to spend an unacceptable amount of time or money or absorb too much risk in order to defeat it, with the ultimate goal that the system can be trusted with sensitive information.

1.1. Principles of Security

Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.

Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation: A mechanism to prove that the sender really sent this message.

One essential aspect for secure communications is that of cryptography. Cryptography is the art and science of achieving security by encoding messages to make them non-readable.

1.2. Trust models in conventional network (fixed Infrastructure)

Secure use of cryptography requires trust. There are a number of trust models employed by various cryptographic schemes.

- The web of trust employed by Pretty Good Privacy (PGP) users, who hold their own set of trusted public keys.
- Kerberos, a secret key distribution scheme using a trusted third party.
- Certificates, which allow a set of trusted third parties to authenticate each other and, by implication, each other's users.

PGP

Pretty Good Privacy is a widely used private e-mail scheme based on public key methods. A PGP user maintains a local keying of all their known and trusted public keys. The user makes their own determination about the trustworthiness of a key using what is called a "web of trust". PGP makes no statement and has no protocol about how one user determines whether they trust another user or not. In any case, encryption and signatures based on public keys can only be used when the appropriate public key is on the user's keying.

Kerberos

Kerberos is a commonly used authentication scheme on the Internet. Developed by MIT's Project Athena, Kerberos is named for the three-headed dog that, according to Greek mythology, guards the entrance of Hades (rather than the exit, for some reason!). Kerberos employs client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security

and authentication will be based on secret key technology where every host on the network has its own secret key. It would clearly be unmanageable if every host had to know the keys of all other hosts so a secure, trusted host somewhere on the network, known as a Key Distribution Centre (KDC), knows the keys for all of the hosts (or at least some of the hosts within a portion of the network, called a realm). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key; keys can be distributed physically or by some other secure means.

1.3. Digital certificates and certification authority

The ISO X.509 protocol defines a mechanism called a certificate that contains a user's public key that is signed by a trusted entity called a certificate authority (CA).Certificates contain information used to establish identities over a network in a process called authentication. Like a driver's license, a passport, or other forms of personal identification, certificates enable servers and clients to authenticate each other before establishing a secure connection. Certificates are valid only for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

Server certificate
A server certificate certifies the identity of a server. The type of digital certificate that is required by the Secure Gateway is called a server certificate.

Root certificate
A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the CA. This type of digital certificate is required by a client device to verify the server certificate.
Certificates generally have a common format, usually based on International Telecommunication Union (ITU) standards. The certificate contains information that includes the:

Issue
The organization that issues the certificates.
Subject
The party that is identified by the certificate.
Period of validity
The certificate's start date and expiration date.
Public key
The subject's public key used to encrypt data.
Issuer's signature
The CA's digital signature on the certificate used to guarantee its authenticity. Certificates and the collection of CAs will form a Public Key Infrastructure (PKI).
Certificate Chains
Some organizations delegate the responsibility for issuing certificates to resolve the issue of geographical separation between organization units, or that of applying different issuing policies to different sections of the organization.

Certificate Revocation Lists
From time to time, CAs issue certificate revocation lists (CRLs). CRLs contain information about certificates that can no longer be trusted.

1.4. Mobile ad hoc network

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.

Figure 1: Mobile Ad-hoc Network

2. Related Work

To overcome the limitation of distribution of public key certificates, in 2003 and 2007, S.Yi and R.Kravets and J.van der Merwe [1] [2] 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 updating will be a problem.

In 2005, Y. Kitada, A. Watanabe, K. Takemori, and I. Sasase [3] 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. Each node holds in its repository only the certificates that other nodes issued to it.

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.Mohri, I. Yasuda, Y. Takata, H. Seki and H.K.R.Li [4] [5] 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 [4] 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 [6] 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 [7] 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. Trust transitivity is hold only if the all evidence used to establish transitive trust satisfies the same, global, metrics of competence, permanence, and long term endurance.

In 2009, H Dahshan and James Irvine [8] proposed 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 In order for a node A to authenticate the public key of another node; it has to acquire a chain of valid certificates from node A to node D. This scheme has two phases. In route request phase source node sends the route request packet to nodes it directly trusts without adding its certificate. This certificate is stored in the repository of its trusted nodes. Similarly in route reply phase destination node does not insert its own certificate in the first hop because this certificate is stored in its

trusted nodes.

Threshold scheme is a different scheme from the above approaches. In 1979, Shamir [9] proposed that secret key is divided into n shares and gives that to nodes called shareholders. 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 [10]. 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. Each executive is given a small magnetic card with one Di piece, and the company's signature generating device accepts any three of them in order to generate (and later destroy) a temporary copy of the actual signature key D.

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***. Suppose we want to use a (***k, n***) threshold scheme to share our secret ***S,*** without loss of generality assumed to be an element in a finite field ***F.*** Choose at random ***K-1*** coefficients in ***F*** and let $a_o = S$. Build the polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \text{-- - - - - -} + a_{k-1}x^{k-1}$.

Let us construct any n points out of it, for instance set ***i =1***, - - -, ***n*** to retrieve (***i***, ***f*** (***i***)). Every participant is given a point (a pair of input to the polynomial and output). Given any subset of ***k*** of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term a_0.
In 2004, J. H. S. Yi and R. Kravets [11] 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. Virtual CA plays a important role of trusted node. They must be trustworthy and protected but it imposes higher maintenance. Certificate chaining fits well with ad hoc network, relying on each mobile node to issue certificates to other nodes but the validity of a certificate chain depends on all mobile nodes in the chain which may not be easy to obtain. Both approaches have advantages and disadvantages. Composite key management adapts the benefit of both the technique by combining virtual CA and certificate chaining. It follows two fundamental principles node participation and trusted third party. Node participation states that key management framework for ad hoc networks should rely on a large number of nodes for availability, but a smaller group of nodes for security. The use a trusted third party principle states that a key management should use a TTP because authentication provided by the TTP is trusted with high level of confidence. 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. Confidence value is calculated for the whole route and the user can decide whether it granted permission for authentication request. Firstly raw confidence value is calculated by multiplying confidence value of all edges. Attenuation factor can be calculated with the probability that a chain of length d is intact can be denoted as $(1-p)^{(d-1)}$ .The final confidence value can be calculated by multiplying raw confidence value and attenuation factor.

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 [12] proposed a trust based threshold cryptography key management for mobile ad hoc network. In this scheme, a shareholder 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 shareholders, 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.

Public key certificate generation includes two types of certificates. First certificate is issued by the nodes that trust the nodes. This certificate is verified by the private key of the issuer node. The second certificate

called the CA certificate is signed by the CA private key. Any node can verify the certificate that has the public key.

Public key authentication is performed when a source node sends a route request to nodes it directly trusts and nodes that have CA certificates through its one hop neighbors. When a node that gets the route request is the destination node, it sends a route reply. If the destination node is one hop trusted node, it adds the certificate of the destination node before it sends it to source node. If the node is neither the destination node nor the one hop trusted nodes, it adds its certificate to the route request and passes the route request to one hop trusted nodes. When the destination node receives a route request, it verifies every certificate and sends a route reply packet. All intermediate nodes that receive a route reply add its own certificate before passing the route reply to source nod. When a source node receives a route reply, it verifies every certificate in the certificate chain before it sends data to the destination node.

3. Comparison of Different Approaches

1. On Demand Distributed Public Key Management for Wireless Ad hoc network- It uses Ad hoc Simultaneous Nodes search protocol (ASNS) protocol.

Advantages-

a) Reduce Memory size.
b) Certificate Revocation list is not required.
Applications-
It is applicable to the network in which
Density of the node is low.

2. Certificate Chain Discovery in Mobile Ad hoc Network-

It uses Distributed algorithm.

Advantages –
a) It addresses node mobility by reducing time and communication complexity.
b) It proposes a new method with lower communication.

3. Key management in web of trust for mobile adhoc networks-

It uses Ad hoc on demand Distance vector Protocol.

Advantages-

a) Low Communication cost
Applications: It is highly robust in mobility environment of MANET.

4. On Demand Self-Organized Public Key Management for Mobile Ad hoc Network-
It uses On Demand Distance Vector routing protocol.
Advantages-
b) Low Communication Cost.
Applications-
It is suitable for stationery networks and with low to high mobility.
5. Composite Key Management for Mobile Ad hoc Network- It uses On Demand Distance Vector routing protocol.

Advantages-

c) This scheme increases the availability and maintains strong security.
d) Communication overhead is localized to one hop neighbor and each certificate request consists of a single broadcast request packet and one or more reply packet. Applications- It is useful in flexible, modular and adaptive key management services.

6. Trust Based Threshold cryptography Key Management for Mobile Ad hoc Network.It uses Ad hoc on demand Distance vector Protocol.

Advantages-

a) This scheme provides redundancy since it is operable with and without the existence of the certificate authority.
b) It dynamically switches from a cent realized scheme of trust to a distributed one.
Applications-
This scheme is robust in the mobility environment of MANET.

4. Conclusion

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 shareholder periodically. It maintains the security by interchanging the shares among its shareholders to prevent unauthorized access. In this paper I presented the different schemes used for key distribution and key management in mobile ad hoc. Each scheme applies its own methods and approaches to provide security measures in mobile ad hoc network. Each paper I discussed in this paper has its own advantages and disadvantages. Comparison between different approaches has also been presented in the paper.

References

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

[2] 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.

[3] 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.

[4] 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.

[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.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.

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

[8] 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.

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

[10] 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.

[11] 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.

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

I did B.E (IT) from Institute of Technology and management, Gwalior in 2007.Currently I am Pursuing M.Tech from LNCT Bhopal.