ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

The Extended Security in Mobile Ad-hoc Network with Modified PKI

Er.Harjivan Singh Brar*
Lect CSE, G.T.B.Khalsa Institute of Engg,
Malout.India
harryzbrar@gmail.com

Er. Mandeep Singh Sandhu
Assistant Professor.
Bhai Maha Singh College of Engg,
Muktsar.,India

Abstract: Mobile ad hoc network (MANET) technology spreads widely in these days. It is suitable for environments that need on fly setup. A lot challenges come with implementing these networks. The most sensitive challenge that MANET faces is the security issue. Traditional Public Key cryptography (PKC) and Identity based Cryptography (IBE) are slow and not suitable for these environments because of the nodes resources limitations. This paper is going to discuss the security of MANET using the PKI schemes in an efficient way. In this paper we have presented a new algorithm that will extend the drawbacks of PKI technique and make the network much secure and reliable for small and larger scale networks. Keys and certificates have to be issued to each node (trusted), neglecting malicious nodes on the track and finding the valid route to transfer the data.

Keywords: Mobile Ad hoc Networks, Security, Public Key Cryptography, Trusted authority, Central Authority.

I. INTRODUCTION

Today Mobile Ad hoc network (MANET) is being used in very sensitive missions such as military operations for achieving connectivity between soldiers. It is also being used to help in avoiding accidents and traffic jams in the road transportation system. Because of its mobility features, it is very challenging to keep such a network secure. There are three main mechanisms being used to secure MANET and they are prevention, detection and response mechanisms. Prevention mechanism is used to secure network against external attacks, where it can be achieved by authenticating users and nodes and by securing routing protocols used to create routes between nodes. Detection and Response mechanisms are used to secure network against internal attacks. This can be achieved using intrusion detection systems. This paper focuses on the authentication mechanism to secure MANET against malicious external attackers.

This paper is organized as follows. Section II presents an overview of recent work on ad hoc network security. Section III describes the problems with PKI in ad hoc routing protocols. Section IV presents our approach using modified PKI to secure ad hoc routing Algorithm. Finally, section V offers concluding remarks.

II. BACKGROUND

This section presents some of the previous researches done in the authentication field for MANET. Several proposed ad hoc routing algorithms, for example [1], [2], [3], [4], [5], have security vulnerabilities and exposures that easily allow for routing attacks. Numerous solutions have been proposed for providing a secure and reliable certification authority in ad hoc networks [6], [7], [8], [9]. We divide the authentication schemes into two types: PKI-based and Identity-based authentication schemes.

A. *PKI-based authentication schemes*

Many researchers have been done in order to find a reasonable solution for authenticating MANET nodes using the PKC system. MANET does not have infrastructure. Any node may fail or go out of range at any time. Therefore

MANET cannot depend on any central entity. Each node has a part of the responsibility in the authentication process. It is suggested to distribute the CA to a set of n nodes [10].

These nodes share the keys management responsibility. They are called "servers", and they work together to do the cryptography operations. Researchers in [10] also specified a threshold for the number of servers that should be available to do the cryptography operation successfully. This concept is called "Threshold Cryptography. Researchers [11] proposed that any node joining the network can act as a server node to reduce the load on the existing servers. According to [12], using a large number of nodes as servers makes the system vulnerable to Sybil attack. Researchers [13] proposed using a partial revocation certificates. That network Revocation certificate is build by gathering the partial revocation certificates built by the network nodes.

Researchers in [14] proposed using clusters where in each cluster there is a Cluster Head that controls the authentication process. Researchers in [15] proposed using some nodes as Temporary Certificate Authority to increase the availability of the authentication service. These nodes are called TCA (Temporary Certificate Authority). This scheme causes overhead because of the large number of authentication messages transferred between nodes.

B. *Identity-Based Public Key Cryptography (ID-PKC) Authentication scheme*

[a] *Introduction about ID-PKC:* According to [16], keys and certificates management is one of the difficulties faced when using the Public Key Cryptography. One of the solutions to that is by using the Identity-Based Public Key Cryptography. The main idea is to use identity information (such as email address) as a public key. According to [17] Private Key is generated by the

TA (Trust Authority) using the node public key and a master secret and system parameters. The master secret is hold by the TA. This private key is used for decrypting and signing messages.

[b] *PKC versus ID-PKC:* Researchers compared the PKC system and the ID-PKC system. They focused on the following points in their comparison:

[i] Easiness of implementation: ID-PKC is more suitable for the sender to implement. It is enough for him to know the identity of the receiver to generate his public key information. While in PKC, the sender needs to authenticate the receiver's public key by a third party.

[II] Risks of compromising: The results of compromising CA or TA give PKC an advantage over IDPKC. If CA is compromised, the past encrypted traffic is still secure. In the other hand, if TA is compromised and the master secret key is stolen, then the attacker knows how keys were generated, thus the attacker can decrypt all the past encrypted transferred information.

[iii] Keys generation In PKC: Public Key is generated at the same time as the private key by the owner or the CA, and the private key is generated by the client or the CA. On the other hand, in ID-PKC, public key can be generated any time by any client, and then the receiver should get the corresponding private key by the TA, when the private key is generated by the TA using a master key. This makes the system vulnerable to the key escrow attack. To defend against this attack, It has been suggested [18] that using the (k, n) threshold cryptography technique to distribute the master key shares among n nodes that represent the TA service. Each node of the distributed TA service computes the partial private key of any node based on its identity.

[c] *Threshold in Identity-based key management system:* A mechanism that has been proposed [19] depended on the threshold cryptography concept. They suggested a distributed key generation component which produces the network master keys pair shares to each node in a distributed way. There is one public/private key pair for the entire network called Master Key (PK, SK), where PK is known to all nodes. On the other hand, SK (Master Private Key) is shared by n nodes. In <k, n> system, any k nodes can generate SK jointly. However any (k-1) nodes are not capable to do so. Each node uses its identity information as a public key. It sends a request to the distributed key generator component to obtain the corresponding private key. To compute the master key, it is separated into multiple shares and distributed into n nodes, thus there is no need for a trusted third party [1]. When two nodes need to communicate, the source node generates a secret sharing (session key) using its private key and destination node's public key. The destination node computes the secret key, using its private key and the source node's public key. This session key is used as a symmetric key for encryption and authentication.

III. PROBLEMS WITH PKI

A. *Limited assurance provided in reality*

[a] CA's generally protected in case of failure

[b] What certificate assures (usually)

B. *Private-key insecurity*

C. *Technical and Implementation difficulties*

[a] Assumption of global namespace

[b] Difficulty in detecting key compromise

D. *Particular message was generated by an entity that had available to it a particular private key.*

E. *CA that provided the certificate, at some time in the past, had grounds for believing that that Private Key was associated with a particular entity.*

F. *Private Key is now available to other entities as well as the entity to which it purports to be 'bound';*

G. *Private Key invocation that gave rise to a particular message was performed with the entity's free and informed consent.*

IV. APPROACH USING MODIFIED PKI

An extended security in Mobile Ad hoc Network with modified PKI consists of a preliminary certification process followed by a route instantiation process that guarantees end-to end validation. The protocol is simple compared to most non-secured ad-hoc routing protocols. Route discovery in an extended security in Mobile Ad hoc Network with modified PKI is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are validated at each hop from source to destination, as well as on the reverse path from the destination to the source. Thus it enhances the functionality of the PKI.

Step 1: Creation of a random Ad hoc network: A random Ad-hoc network at a given instant of time is created depending on.

[a] The total no of nodes in the Ad-hoc network.

[b] The communication range of each node.

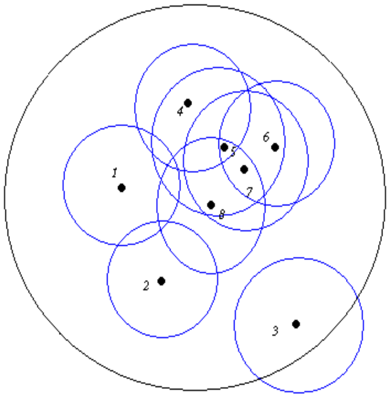

Figure 1: Node Distribution in Network

Step 2: Finding the neighbors of each node: Each node in the ad-hoc network has some neighbors with which it can communicate directly. Each of these neighbors lies within the transmission range of the node. If the distance between two nodes is greater than the transmission range of the nodes then the two nodes cannot communicate directly and are not neighbors. On the other hand, if the distance between two nodes is lesser than the transmission range of the nodes then they are neighbors.

Table I: Neighbor nodes

NODE	NEIGHBOR
1	No neighbor
2	No neighbor
3	No neighbor
4	5
5	4, 6, 7, 8
6	5, 7
7	5,6,8
8	5,7

For example, for the network shown in above figure: 1 and the neighboring nodes of each node are given in above table: 1.

Step 3: Certification: Assigning certificates to the nodes by an extended security in Mobile Ad hoc Network with modified PKI requires the use of a trusted certificate server T, whose public key is known

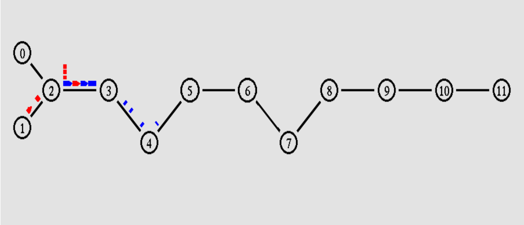

Figure 2:

Assigning certificates to nodes to all valid nodes. Before entering the ad hoc network, each node must request a certificate from T. Each node receives exactly one certificate after securely validating their identity to T. In the program it is assumed that all the nodes have validated their identity to the trusted server T. Thus all nodes receive a certificate from T.

Step 4: Discovery of all routes to the destination: Once certificates have been assigned to the nodes, the valid route from the source node to the destination node is found out. The source node begins route instantiation to destination by broadcasting to its neighbors a *route discovery packet* (RDP). The RDP includes a packet type identifier (RDP), the IP address of the destination (IPX), source node's certificate (cert A), a nonce NA, and the current time t, all signed with source node's private key. When a node receives an RDP message, it sets up a reverse path back to the source by recording the neighbor from which it received the RDP. The receiving node uses source node's public key, which it extracts from source node's certificate, to validate the signature and verify that source node's certificate has not expired. The node signs the contents of the message, appends its own certificate, and forward broadcasts the message to each of its neighbors. Upon receiving the RDP, the neighbor's of the transmitting node validate the signature with the given certificate. They remove the transmitting node's certificate and signature, records the transmitting node as their predecessor, signs the contents of the message originally broadcast by the source, appends their own certificate, and forward broadcasts the message. This process continues until the RDP reaches the destination node.

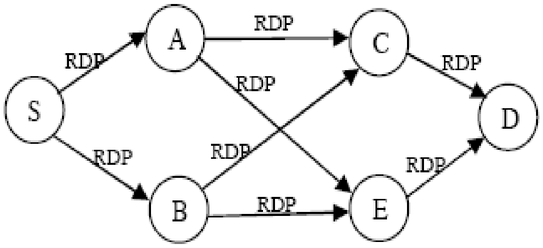

Figure 3: Broadcasting RDP

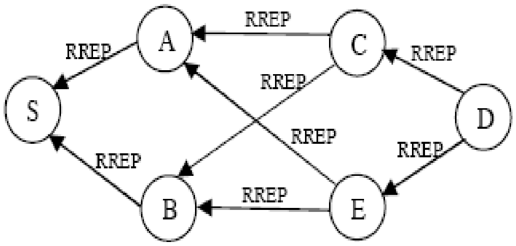

Figure 4: Replying to each RDP

Step 5: Finding the valid route between the source and the destination nodes: The valid route in an extended security in Mobile Ad-hoc Network with modified PKI is the route from which the first RDP packet is received by the destination. The destination, replies to the first RDP that it receives at a source and a given nonce. There is no guarantee that the first RDP received traveled along the shortest path from the source. An RDP that travels along the shortest path may be prevented from reaching the destination first if it encounters congestion or network delay, either legitimately or maliciously manifested. In this case, however, a non-congested, non-shortest path is likely to be preferred to a congested shortest path because of the reduction in delay.

Step 6: Evaluatin the effect of the malicious node presence on the Ad hoc network route discovery: It is supposed that a given node in the network is a malicious node's or can introduce an additional node in the network which is malicious. Then on route discovery using an extended security in Mobile Ad hoc Network with modified PKI this malicious node would not be a part of the valid route.

V. CONCLUSION

This research presented a new authentication solution for MANET. This scheme gathers the robust security features of PKI with techniques to enhance the speed of the network achieving an extended security with modified PKI algorithm. Traditional routing algorithms fail to provide security, and rely on an implicit trust between communicating nodes. The technique will be very beneficial in PKI framework, not only secure but also when network get scaled .The server will track all nodes and their position. If malicious node is entered, the Path is changed by tracking neighbor nodes & finds the valid path that will be secure.

VI. REFERENCES

[1] C. E. Perkins and E. M. Royer, “Ad hoc On-Demand Distance Vector Routing,” in Proc. WMCSA, Feb. 1999.

[2] D. Johnson, D. Maltz, and Y.-C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),” IEEE Internet Draft, Apr. 2003.

[3] S. Murthy and J. Garcia-Lunca-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and Applications Journal, Oct. 1996.

[4] V. Park and M. Corson, “A HighlyAdaptive Distributed Routing Algorithm for Mobile Wireless Networks,” in Proc. Infocom, Apr. 1997.

[5] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Computer Communications Review, Oct. 1994.

[6] J.-P. HuBaux, L. Buttyan, and S. Capkun, “The Quest for Security in Mobile Ad Hoc Networks,” in Proc. MobiCom, Oct. 2001.

[7] S. Capkun, L. Buttyan, and J.-P. Hubaux, “Self-Organized Public-Key Management for Mobile Ad hoc Networks,” IEEE Transactions on Mobile Computing, vol. 2, no. 1, Jan.-Mar. 2003.

[8] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks,” in Proc. ICNP, Nov. 2001.

[9] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network, vol. 13, no. 6, pp. 24–30, 1999.

[10] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network, 13(6), pages 24–30 (1999).

[11] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks,” in Proceedings of Ninth International Conference on Network Protocols (ICNP),pages 3-7 November (2001).

[12] S. Capkun, L. Buttyan, and J.-P. Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks,” IEEE Transactions on Mobile Computing, 2(1), pages 52–64 (2003).

[13] Yi,S and Kravets,R.“MOCA: Mobile certificate authority for wireless ad hoc networks,” 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland, pages 3-8, April (2003).

[14] Bechler, M., Hof, H. J., Kraft, D., Pählke, F. e Wolf, L, “A cluster-based security architecture for ad hoc networks,” IEEE INFOCOM, pages 3-5 (2004).

[15] George,C.,William, J., Nathaniel, J.” A Framework for Key Management in Mobile Ad Hoc Networks,” International Journal of Information Technology Vol. 11 No. 2, pages 4-8,(2005).

[16] Paterson, K.G., Price, G., “A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography”, Information Security Technical Report, 8(3):57-72, Elsevier Ltd, 2003.

[17] A.Shamir, "Identity-based cryptosystems and signature schemes," In Advances in Cryptology – CRYPTO ’84, volume 196 of LNCS, pages 47-53. Springer-Verlag, 1984.

[18] Bohio M., and Miri, A., "Efficient identity based security schemes for ad hoc network routing protocols," Journal of Ad Hoc Networks, pages 3-8, July(2004).

[19] Deng, H., Mukherjee, A., Agrawal, D.P., "Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks," in Proceedings of ITCC, Las Vegas,pages 2-5, 2004.