ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Review of authentication and digital signature methods in Mobile ad hoc network

Amol Bhosle, Yogadhar Pandey
Department of Computer science & Engineering, SIRT Bhopal

***Abstract*- Mobile ad-hoc network is wireless network composed of different nodes communicate with each other without having to establish infrastructure. In this paper technique proposed here to provide the data security of such network using node authentication and digital signature. In this paper we discussed some previous methods for identifying malicious node, there was no such method to authenticate the new node before it joins the network. This new protocol design provides the integrity, confidentiality, non repudiation and authentication with the help of AES, and digital signature. The node authentication achieved by the IP address of the nodes. Digital signature formed with the help of RSA and hash function MD-5. This security mechanism called SMDNA (Securing MANET Data using Node Authentication) improves the performance of the routing protocol AODV.**

***Index Terms* - Mobile ad-hoc, confidentiality, authentication, nonrepudiation, Integrity, AODV, digital signature.**

I. INTRODUCTION

Ad-hoc networks are characterized by dynamic topology, self-configuration, self-organization, restricted power, temporary network and lack of infrastructure. Characteristics of these networks lead to using them in disaster recovery operation, smart buildings and military battlefields. Routing protocol in ad-hoc networks are classified into three main categories, proactive , reactive and hybrid. In proactive routing protocols, routing information of nodes is exchanged, periodically. In reactive routing protocol routing information of nodes gathered on time when needed. In hybrid the combination of the two are used.

A mobile ad hoc network has following features:

1 Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. The mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

2 Distributed Operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

3 Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly.

4 Wireless medium

In an ad hoc environment, nodes communicate wirelessly and share the same media (radio, infrared etc.). The wireless medium has neither absolute, nor readily observable boundaries outside of which the stations are unable to receive network frames. Thus the channel is unprotected from outside signals and hence it is significantly less reliable than wired media.

5 Limited availability of resources

Because batteries carried by each mobile node have limited power supply, processing power is limited, which in turn limits services and applications that can be supported by each node. This becomes a bigger issue in MANET because; since each node is acting as both an end system and a router at the same time, additional energy is required to forward packets.

6 Multihop Routing

Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

Security Goals

In providing a secure networking environment some or all of the following service may be required.

All Rights Reserved © 2013 IJARCET

1. Authentication: This service verifies the identity of node or a user, and to be able to prevent impersonation. There is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

2. Confidentially: Keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data.

3. Integrity: Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption.

4. Availability: Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

5. Non-repudiation: Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message

6. Access Control: To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes.

The cryptographic algorithms are classified into two different types such as symmetric and asymmetric.
In symmetric encryption method both sender and receiver share the common key value for encryption and decryption. It requires that the sender find some secure way to deliver the encryption/decryption key to the receiver. The effective key distribution needs to deliver key to the receiver. Large number of protocols provides various techniques. These protocols are to provide more secure but less performance. The public key cryptography or asymmetric cryptographic method solves the problems of key distribution. In this method, uses a pair of keys for encryption. The public key encrypts the data and corresponding private key for decryption. Each user has one pair of keys. The private key kept secret and public key knows by others. Any one wants to send some information to you they read your public key and encrypts the information. After you receive, the encrypted data using your private key to decrypt it. One issue with public key cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person's key. In a public key environment you are assured that the public keys to which you are encrypting data is in fact the public key of the intended receiver. The identification of correct public key of proper person is more difficult without using any third party.

II. RELATED WORK

Satoshi et al [11] proposed a method of dynamic learning to detect a blackhole attack in reactive routing protocol AODV. It identifies the malicious node by checking the abnormal data that deviates from the cluster of normal state. The problem with this method is suppose new node wants to join the network the authentication is not provided here.

Kanika Lakhani et al [5] proposed a watchdog mechanism to detect the malicious node. It works on the concept of threshold value. The lower the threshold value the misbehaving node drops the packets more. Thus identified the misbehaving node.The problem with this method is for new joining node we can not identify the trusted node.

Rajiv Nekkanti et al [9] proposed a method based on the trust of the neighbours. They proposed on the different levels of the security as well as levels of the encryption and levels of the trust factor. The problem with this method is we have to implement different levels of security lower the trust level more easy to break the code.

Shiva et al proposed [13] proposed the method that the digital signature based secure data transmission in wireless sensor networks. They used the asymmetric key crypto system (public) for the security. To generate the digital signature MD-5 hash function is used. Also RSA algorithm was used which provides digital signature as well as secrecy. The results were compared with AOMDV which is a extension of AODV protocol. This work was done for wireless sensor network.

Changhui et al [2] proposed method that provide a scheme that with hash based message authentication code to overcome the shortcomings. Hash based message authentication code using cryptographic hash functionsuch as SHA-1 in combination with secret key.It provides the integrity of information transmitted over a unreliable mediun based on secret key. In this method HMAC checking and symmetric ecryption used to replace complicated ECC to achieve secure communication.

M.A.Matin et al proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. The increase in key size as well as block size, the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here.

Hongbo Zhou et al [6] proposed a method of autoconfiguration which is a method to achieve uniqueness of address allocation with the help of IP address for each node. In this authors used the method of SA-PKD which includes broadcasting of DAD (Duplicate address

All Rights Reserved © 2013 IJARCET

Detection) message. In DAD message it contains the Hash value of IP address of node and IP address signed with its private key. If a node receives a DAD message it calculates hash value of its own IP address. If it is same them generates NACK message and sends back to node N.

S.Thadvai et al. [10] proposed a method based on message recovery which includes message and the signature hence the communication cost is lower for the message recovery method. In this method they used the Authentication Encryption Scheme (AES) for message recovery.

Nikos Komnios et al [8] proposed a two phase detection procedures of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. This method works in two phases, in phase one detecting unauthorized nodes with the help of its neighbouring nodes. In second phase the compromised nodes are detected by a local agent that collects and analyses data. The problem with this approach is we have to rely on the neighbouring node for authentication.

Seungjin Park et al [12] preposed a method of one hop broadcaste in MANET which uses the EROB algorithm that uses data packets as well as control packet broadcast in progress(BIP) to prevent the collisions. Sometimes it may cause a broadcast propogation problem i.e. for every collision the BIPs are generated and so the network is filled by the BIPs.

Bing Wu et al [1] proposed a method using key management in MANET. The third party certification authority is responsible for handling the certificates such as new issue or expiration and revocation of certificates. Problem with this method is that implementation of third party CA is complex.

Uttam Ghosh et al [14] proposed a ID based distributed dynamic IP configuration scheme for address allocation. They discussed the three categories namely best effort allocation, Leader based allocation and Decentralized allocation. And gave solution to overcome the problems arised by these three categories. For address detection they denied the concept of DAD scheme.

Wang Feng et al [15] proposed scheme on public key management chain mobile network. This algorithm make full use of temporary, protect terminal in public key use efficiency high hash survival chains of time.

Luis et al.[7] proposed the method a pair-wise key based scheme for forming secured private clusters in mobile adhoc networks.The solution tackles the problem of node authentication combined with traffic encryption in relatively small adhoc networks using proactive neighbour discovery and authentication.

Table1: Observation table

Sr. No.	Title	Method used	Observations / Problem
1	Trust based adaptive on demand ad hoc routing protocol	Trust based	At lower level of trust more chances of attack
2	Secure and efficient key mngt in MANET	Key MNGT (SEKM)	Uses third party Certificate authority, handling and maintaining certificates is complex
3	Detecting blackhole attack on AODV based MANET by dynamic learning method	Dynamic learning	Calculation of mean vector is complex and lengthy process. Also for joining of new node authentication not provided here.
4	A simulation model to secure routing protocol AODV against Blackhole attack inMANET	Wathdog mechanism	For joining of new node authentication not provided here.
5	Detecing unauthorized and compromised nodes in MANET	Two phase detection	Have to rely on neighbouring nodes.
6	Secure autoconfiguration and public key distribution for MANET	Address autoconfiguration	Works on DAD (Duplicate address Detection) which creats flooding in network

All Rights Reserved © 2013 IJARCET

III. PROBLEM STATEMENT

The observations made from some previous techniques as shown in table1. The security to data was not provided while in communication. Also the node authentication of trusted nodes was not provided sufficiently. Whenever a new node wants to join the network there was no provision present to authenticate it and join it in network.

To achieve secure communication in MANET some requirements must be satisfied:
(a) A security association must exist between network members, these security associations ensure authentication and non repudiation for trusted nodes.
(b) Sensitive information must be exchanged confidentially between the nodes in the network.
(c) Integrity of the information exchanged within the network has to be maintained so that corrupted messages are detected and blocked.

As symmetric cipher algorithm allows us to store the data in a compressed encryption form which results in a small size database. Also it performs faster encryption/decryption. Due to these advantages we are using symmetric cipher algorithm to perform data encryption and decryption. This will also serve confidentiality. Moreover we combine the MD-5 and RSA public key algorithm to generate the digital signature.
The main advantage of using digital signature is it provides user authentication and data integrity and non-repudiation. As digital signature is akin to signing the document physically, it is the acknowledgement of the message so sender can not deny the message.

The proposed method is as follows:

Step 1. Initially establish the route to receiving node by the control message of AODV i.e. RREQ
Step 2.Receiver then sends back RREP message to the sender along with its hash value of IP address.
Step 3.This hash value of IP address is compared with the hash value at sender side, if same then that node is trusted node.
Step 4. Issue trusted node a digital signature using MD-5 and RSA
Step 5. Using Symmetric key encryption algorithm AES encrypt the data and send it to receiver. Along with digital signature
Step 6. Intermediate node checks for digital signature and if valid then forwards data.
Step 7. If digital signature is invalid that means malicious node, find another route.
Step 8. At receiver side decrypts data using AES

IV. CONCLUSION

The work proposed here is Securing data in mobile ad hoc network using the digital signature scheme applied on AODV routing protocol. Also symmetric key cryptography for the fast encryption/ decryption process. The authentication of node done through the IP address of destination this ensures the reliability of node.

V. REFERENCES

[1] Bing Wu, Jie Wu, Eduardo Fernandez, Mohammad Ilyas, Spyros Magliveras " Secure and efficient key management in mobile ad hoc networks", Computer Applications 30(2007) 937-954 Elsevier.

[2] Changhui Hu,Tat Wing Chim,S.M. Yiu,Lucas C.K. Hui, Victor O.K.Li "Efficient HMAC-based secure communication for VANETs" Computer Networks 56, Elsevier 2012.

[3] Fan-Hsun Tseng, Li-Der Chou and Han-Cheih Chao "A survey of Black hole attacks in wireless mobile ad hoc networks" , Human centric computing and Information sciences, Springer (2011)

[4] Hongbo Zhou, Matt Mutak, Lionel Ni "Secure autoconfiguration and Public key Distribution for Mobile Ad-hoc Networks" (978-1-4244) IEEE 2009

[5] Kanika Lakhani, Himani bathla, Rajesh Yadav "A simulation model to secure the routing Protocol AODV against Black hole attack in MANET", vol.10(5) 40-45 May 2010.

[6] Loay Abusalah, Ashfaq Khokhar , and Mohsen Guizani "A survey of Secure Mobile Ad hoc Routing Protocols", IEEE communications surveys and Tutorials, vol 10 (4) 78-93, 2008

[7] Luis Sanchez, Jorge Lanza, Luis Munoz,Kimmo Ahola,alution "Securing the communication in Private Heterogeneous Mobile Adhoc Networks", Springer (2008)

[8] Nikos Komnios , Dimitris Vergados, Christos Douligeris "Detecting unauthorized and compromised nodes in mobile ad hoc networks" ad hoc Networks. 5(Elsevier 2007) 289-298.

[9] Rajiv K. Nekkanti, Ching-wei Lee "Trust based adaptive on demand ad hoc routing protocol" ACM 2004

[10] Sandeep Thadvai et al "A Novel authenticated encryption scheme with convertability" , Mathematical and Computational Modelling, Elsevier 2012.

[11] Satoshi Kurosawa,Hidehisa Nakayama ,Nei Kato, Abbas et al, "Detecting blackhole attack on AODV bades mobile ad hoc Networks by dynamic learning Method ", Intenational Journal of Network Security, vol.5(3). 338-346 (2007).

All Rights Reserved © 2013 IJARCET

[12] Seungjin Park , Seong-Moo Yoo "An efficient reliable one-hop broadcast in Mobile Adhoc networks" Ad hoc Networks 11(2013) 19-28. Elsevier (2012)

[13] Shiva Murthy G.Robert John D'Souza, Golla Varaprasad "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks" IEEE sensors Journal vol.12.No.10, October 2012.

[14] Uttam Ghosh,Raja Datta "A secure dynamic IP Configuration scheme for mobile ad hoc networks" Ad hoc Networks 9(2011) 19-28. Elsevier(2011)

[15] Wang Feng et al "A Mobile adhoc network public key encryption algorithm based on hash-chain" , SciVerse ScienceDirect ,Procedia Engineering 23(659-664), Elsevier 2011

All Rights Reserved © 2013 IJARCET