ISSN:0975-9646

Secure Token for Secure Routing of Packet in MANET

S.S.Zalte, Prof.(Dr.)Vijay R.Ghorpade
Computer Science Department, Vivekanand College
Kolhapur, India
D.Y.Patil College of Engineering and Technology
Kolhapur, India

***Abstract*— Routing of data in the Mobile Adhoc Network(MANET) is the most valuable task in today's world, as it is used in day to day life from a single individual to large organizations. MANET is a favorite target for attackers because of its unique characteristics dynamic topologies, mobility, limited resources, infrastructure less, no centralized management etc. pose a number of non-trivial challenges to security. These challenges and characteristics require MANETs to provide broad security to routing and desirable network performance. In this paper we propose secure token by using cryptographic algorithm AES and hashing algorithm SHA2.**

Keywords—MANET,Routing, Cryptography, Token, AES, SHA2.

I. Introduction

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies.

Mobile Ad hoc Networks are having widespread applications which are part of day to life as we can connect any mobile node to the network and can perform required tasks like accessing the Internet without having the fixed infrastructure or when the use of such infrastructure requires wireless extension.

Wireless communication network are categorized into two types:

a) Infrastructure Networks

An infrastructure network consists of wireless mobile nodes and one or more bridges, which connect the wireless network to the wired network.

b) Infrastructure-less Networks

In this networks each node acts both as a router and a host. Because of the connectivity among the nodes may vary with time due to node improvements, the network topology is dynamic. There is no base station or access point. Nodes can communicate with each other by forming a multi hop route .

Mobile Ad-Hoc Network is a type of infrastructure less network in which nodes are portable devices such as mobile phones and laptops as shown in Fig-1.

MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks.

MANET is more susceptible than wired network due to to their unique characteristics like dynamically changing topology, absence of infrastructure, open medium, resource constraint (memory, bandwidth, computation power etc.) and trust among nodes. Because of these vulnerabilities, MANETs are more prone to malicious active and passive attacks.

Nodes in MANET are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality and non-reputation should be guaranteed during the communication between source and destination[1].

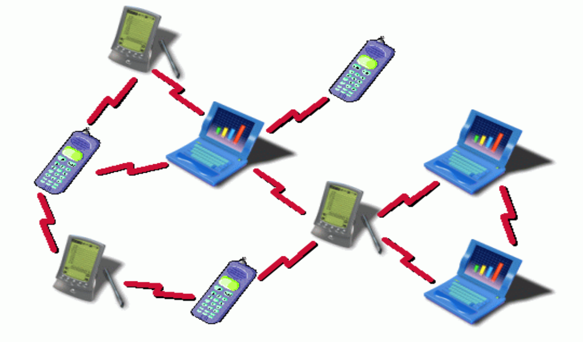

Fig-1. Mobile Adhoc Network.

A. Routing in MANET

Routing in MANET is intrinsically different from traditional routing found on infrastructure networks. Routing in MANET depends on many factors including topology, selection of routers, initiation of request and specific underlying characteristic that could serve as a heuristic in finding the path quickly and efficiently. The low resource availability in these networks demands efficient utilization and hence the motivation for optimal routing in ad hoc networks. Also, the highly dynamic nature of these networks imposes severe restrictions on routing protocols of routing control information among the nodes[2].

The routing protocols in Mobile Adhoc Network are classified into two categories.

1) Routing Protocols Based on Topology 2) Routing Protocols Based on Position

1) Routing Protocols Based on Topology

These routing protocols use links information that exists in the network to perform packet forwarding. They are further divided into Proactive, Reactive and Hybrid Protocols.

i) Proactive Routing Protocols

Irrespective of repeated communication requests. This routing protocols maintain the next forwarding hop in the background. Since the destination route is stored in the background, there is no route discovery and that is the advantage of proactive routing protocol. But the disadvantage of this protocol is that it provides low latency for real time application. The various types of proactive routing are FSR, DSDV, OLSR, CGSR,WRP, TBRPF.

ii) Reactive/Ad hoc Based Routing protocols

Reactive routing protocols floods the network with query packets for path search i.e. route discovery and process is said to be complete when route is found. When it is necessary for a node to communicate with each other then and then only route discovery starts. The various types of reactive routing protocols are AODV, PGB, DSR, TORA, JARR.

iii) Hybrid Protocols

The hybrid protocols are used to overcome the drawbacks of proactive routing protocols by reducing the control overhead of proactive routing protocols and at the same time initial route discovery delay decreased in reactive routing protocols. ZRP ,HARP.

2) Routing Protocols Based on Position

These routing protocols are used the information of geographic position of nodes in order to select the next forwarding hops. There are various types of position based routing protocols such as GPSR , GSR, GPCR etc.

B. Security Goals

For security sensitive applications like adhoc networks, we consider the following attributes.

1) Availability- Only authorized entities should be allowed to access the information created and stored by an organization.

2)Confidentiality-Ensures that unauthorized entities never access the certain information.

3)Integrity-To ensure that transmitted message is never altered.

4)Authentication-When two parties are communicating with each other they must be identify each other. This will prevent gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5)Non-repudiation-Ensures that the sender cannot deny the message is sent by him.

Cryptography can be used to provide security in routing protocol by achieving confidentiality, integrity, authentication, and non-repudiation for communications in public networks, storage, and more. Cryptographic algorithms, in general, are divided into the following:

i) Symmetric key algorithms: These algorithms share the same key for encryption and decryption. Examples include Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).

ii) Public key algorithms: These algorithms use pair of keys for encryption and decryption. Examples include Digital Signature Algorithm (DSA) and the Rivest-Shamir-Adleman (RSA) algorithm.

iii) Elliptic curve algorithms: The difficulty of elliptic curves is based on computing discrete logarithms in the group of points on an elliptic curve defined over finite field. Examples include Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Nyberg Rueppe (ECNR).

iv) Hash: These algorithms transform original string into shorter fixed length value or key and their most important property is irreversibility. Irreversibility and collision resistance are necessary attributes for successful hash functions. Examples of hash functions are SHA-1, SHA-256, SHA-384, MD5, HMAC[3].

As we known, asymmetric cryptography approach such as public-key cryptography (PKC) can achieve authentication, integrity and confidentiality in wired networks. But it is too complicated and expensive for wireless networks. Asymmetric key cryptography algorithm is slow and requires more CPU processing power and battery power which is not feasible in MANET as nodes have limited memory, battery power and CPU computation power[9].

Because of its low computational and communication overhead symmetric-key approach is preferred in wireless network. In symmetric-key approach, two communicating parties need to share a secret key before they communicate with each other. Due to the unpredictable network topology, it is big challenge to distribute the secret keys into the wireless nodes securely and efficiently.

II. Related Work

Kamal Kumar Chauhan et al.[1] used Public Key Cryptography (PKC), nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Source, destination and intermediate nodes in route list authenticate others nodes by verifying signature.

K.Sangeetha et al.[2] proposed use of Elliptic curve cryptosystems instead of DSA/RSA. Time taken for transmitting via AODV is less than the DSR. The throughput is also AODV outperforms than the DSR Routing protocol. ECC is used because of high security level with smaller key size.

Kimaya Sanzgiri et al.[4] proposed Authenticated Routing for Ad hoc Networks (ARAN), uses public-key cryptographic mechanisms to defeat all identified attacks. Author describes the threats, specifically showing their effects on AODV and DSR.

Stephan Eichler et al.[5] proposed a novel secure routing protocol based on AODV for infrastructure-based MANETs. In this paper author gives extension to AODV protocol by using digital signature which is a combination of RSA and SHA-1.

Zahra Moradlu et al.[6] proposed scheme distributes the role of the key generation center (KGC) among all nodes, therefore the private key is issued by distributed

KGCs (DKGCs) and the node itself. Each pair of nodes can share a symmetric key in a non-interactive way .

Tameem Eissa et al.[7] proposed new Key Management System which consists of four keys: identity key , public key, private key, symmetric key. This research proposed to use this idea in MANET system by hiding the public keys and making them visible only to the trusted nodes. This research also proposed using RSA since it is one of the most secure schemes.

Soma Saha et al.[8] proposed extension to ORRP-1 i.e. SORRP protocol . The HELLO message is used for finding the cost vector as well as neighbor sensing. Symmetric key cryptography or shared secret key cryptography both the sender and receiver use the same secret key for encryption and decryption. Thus confidentiality is maintained using symmetric key cryptography. to protect the secret key from eavesdropping or any other security threats public cryptography is used.

A.Rajaram et al.[10] proposed high certificate authentication scheme having three components Monitoring Routing cum forwarding (RCF) behavior, Certificate revival and Certificate revocation. Author also used Shamir's secret sharing scheme which provides extendable as well as flexible security.

Ramya K et al.[11] proposed hybrid security protocol which is a combination of Elliptic Curve Cryptography MD5 and RSA used to achieve both the Confidentiality , Integrity and Authentication. Author also used digital signature in EAACK to ensure the integrity of the intrusion detection system**.**

Gandhi Krunal et al.[12] proposed double digest symmetric key distribution based algorithm for detecting and defending against malicious nodes in MANET. Author used SHA (Secure Hash Algorithm) for creating digest.

R. Rajamohamed et al.[13] Author proposed security to the Variable bit rate source routing protocol (VBSR)i.e. hashed VBSR. Which gives a better security to key management as well as to data transmission.

III. Proposed Method

Basic idea behind the secure token is to, use digital signature by using Advanced Encryption Standard (AES) and Secure hash (SHA2) algorithms to secure the data and maintain privacy between the sender and receiver, which will improve the services provided by the MANET.

Some of the security features we will be incorporating in our proposal are:

i) Diffie–Hellman key exchange (D–H) -In Diffie-Hellman secrete key can be exchanged without secure communication channel between two users without prior knowledge of each other. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

ii)SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). SHA stands for Secure Hash Algorithm.
SHA-2 is a hashing algorithm used to compute fixed length digest of original message or a test or a data file. The receiver also compute message digest through the SHA-2 algorithm and compares it with the message digest it has received. SHA-2 is called secure because it is difficult to find a original message that corresponds to a particular message digest or two messages with the same message digest. If message change during transmission the message digest also change and the signature would fail to verify indicating the message has been modified. SHA-2 is also irreversible i.e. given a message digest it is computationally difficult to find the original message. SHA-2 is widely used in a number of security applications electronic fund transfer, electronic mail, software distribution, data storage and other application which require data integrity assurance and data origin authentication. SHA-256 is not much more complex to code, and has not yet been compromised in any way. The SHA-256-bit key makes it a good partner function for AES.

iii)Advance Encryption Standard(AES) is a symmetric block cipher, published by the National Institute of Standards and technology(NIST) in December 2001. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys -128,192,256 bits. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. The algorithm was designed to have the following characteristics:

i) Resistance against all known attacks
ii) Speed and code compactness
iii) Design simplicity

IV. Proposed Architecture

In the proposed method, we use secure token to provide the security to the non-mutable fields in the RREQ and RREP messages. Secure token is used to authenticate between each two neighbor nodes by agreeing on a secret key: Fig-2 shows a method of Diffie- Hellman, AES can be used to sign the hash SHA-2 of the package, and then put it in the field authentication. The proposed method is as follows:

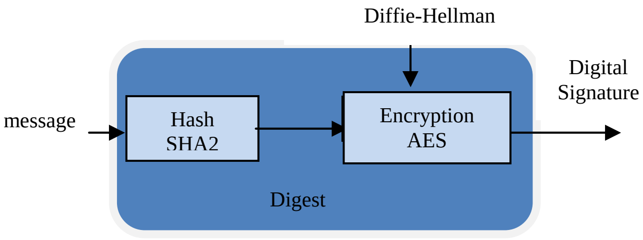

Fig.-2 Secure Token

i) Along with digital signature signed message with all fields except hop count is sent to intermediate nodes.
ii) Whenever an intermediate node receives an RREQ or RREP, it first verifies the signature. If the signature is verified then only the node updates its routing table and forwards the data .
iii) If digital signature is invalid that means node is malicious. Signing the messages makes sure that the message was coming from a particular node and that node cannot deny on sending that message.
iv) At receiver side decrypts data using AES. Calculate hash of received message and compare it with the original.
v) If there is a match, it means the signature has been verified, and the recipient can accept the message is coming unaltered from the sender. If there is mismatch, it means the message has not been signed by the sender or the message has been altered. In both cases, the message should be rejected. Find another route.

V. CONCLUSION

Though ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. We propose a solution to secure data packet, by adding a digital signature, based on symmetric cryptography generated using the AES algorithm and the SHA2 hash function. It is more suited to a mobile environment. Data confidentiality and integrity can be achieved by data encryption using strong symmetric key algorithm such as AES. Without having digital certificate node's can't participate in network communication. Here we can achieve access control, non-repudiation, prevents spoofing and unauthorized participation in routing.

During the survey, we also realized that some aspects such as the intrusion detection techniques can be further improved. We hope to explore deeper in this research area .

REFERENCES

[1] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, "Securing On-Demand Source Routing in MANETs ", IEEE Explore Digital library, 2010, pp:294-297.

[2] K.Sangeetha, "Secure Data Transmission in MANETS Using Eliptic Curve Cryptography", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014, pp:2557-2562.

[3] A article on "Next Generation Encryption" , Cisco security intelligence operations, April 2014

[4] Kimaya Sanzgiri, Daniel LaFlamme,Bridget Dahill, "Authenticated Routing for AdHoc Networks", IEEE Xplore Digital Library,VOL. 23, NO. 3, MARCH 2005, pp:1-13.

[5] Stephan Eichler, Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", München, Germany, IEEE *Xplore* Digital Library, 8-2006.

[6] Zahra Moradlu, Mohammad Ali Doostari, Mohammed Gharib, " Fully Distributed Self Certified Key Management for Large-Scale MANETs", 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing on Autonomic & Trusted Computing,pp:96-102.

[7] Tameem Eissa, Shukor Abdrazak, Md Asri Ngadi, " Enhancing MANET Security using Secret Public Keys "2009 International Conference on Future Networks , IEEE, pp:130-134.

[8] Soma Saha , Rituparna Chaki , Nabendu Chaki , " A New Reactive Secure Routing Protocol for Mobile Ad-Hoc Networks", IEEE computer society(2008), pp:103-108

[9] Thandu Naga Srinu Padma, Tandu Ramarao, Nischala Simhadri , "AODV Routing Protocol in MANET based on Cryptographic Authentication Method ",Vol 2, Issue10, IJCSET |October 2012,ISSN-2231-0711,pp:1459-1464.

[10] A.Rajaram and Dr.S.Palaniswami , "A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks",IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5, July 2010 , ISSN-1694-0814, pp:37-45.

[11] Ramya K, Beaulah David, Shaheen H, "Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET", www.iosrjournals.org, eISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 1, Ver.VIII (Feb. 2014), pp:32-36.

[12] Gandhi Krunal A, Patel Tejal K., "Dual Digest Symmetric Key Security Scheme for AODV in MANET",(IJCSIT), Vol. 5(4),2014, ISSN:0975- 9646, pp:5548-5552 .

[13] R.Rajamohamed, Dr. V. Rajamani, "Hashed Symmetric Key Encryption Based VBSR", JATIT & LLS. 10thApril 2014. Vol. 62, ISSN: 1992- 86 445, pp:161-165 .