INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Improving Security in MANET Using Digital Signature Standard Scheme

Aditi Sharma [1], Maninder Kaur [2]

[1] Shaheed Udham Singh Engineering College, Department of Computer Science,
Tangori, Punjab, India
aditisharma0808@gmail.com

[2] Doaba Institute of Engg. & Tech, ECE Department,
Kharar, Punjab, India
maninderecediet@gmail.com

Abstract: *The wireless and dynamic nature of mobile ad hoc networks (MANETs) leaves them more vulnerable to security attacks than their wired counterparts. The nodes act both as routers and as communication end points. This makes the network layer more prone to security attacks. A main challenge is to judge whether or not a routing message originates from a trustworthy node. The solution thus far is cryptographically signed messages. The general assumption is that nodes in possession of a valid secret key can be trusted. Consequently, a secure and efficient key-management scheme is crucial. Keys are also required for protection of application data. However, the focus here is on network-layer management information. Whereas key management schemes for the upper layers can assume an already running network service, schemes for the protection of the network layer cannot. Keys are a prerequisite to bootstrap a protected network service. In our proposed work we are Implementing Digital Signature Standard Scheme and then we will apply this algorithm in Mobile Ad-hoc Networks. We are also Comparing the performance of modified Digital Signature Standard with Station to Station key agreement when used in Mobile ad-hoc Networks. The Performance of the algorithms will be compared on the basis of Throughput and Delay.*

Keywords: *MANET (mobile ad hoc network), RSA, DSS, security algorithm, attacks.*

1. INTRODUCTION

Mobile Ad Hoc Network (also called MANET) is a collection of portable devices that establish communication without the help of any infrastructure or established communication backbone. Furthermore, Mobile Ad hoc networks are easy to deploy and does not require any back bone support. MANET is Useful in the absence of infra-structure. MANET is used many applications, such as, Military environments, Soldiers, tanks, planes, taxi cab network, Emergency operations, search, rescue, policing etc. Each de-vice in a MANET is free to move independently in any direction, therefore change its links to other devices over and over again. Mobile Ad Hoc network are self-organizing, multi-hopping, mobile and scalable. Each node in MANET is equipped to continuously maintain the information regarding route. Topology of the ad-hoc network depends on the trans-mission power of the nodes and the location of the portable nodes, which may change from time to time [1].

The main goal of Ad Hoc routing is to send data packets among nodes distributed randomly in the network. Since mo-bile ad hoc networks have random topology, routing in such networks is a tough task. There is so much work has been done on routing in ad hoc networks. Routing is the process of finding a path from a source to destination [2]. The broadcasting is usual and a common operation in ad-hoc network. It consists of diffusing a message from a source node to all the nodes in the network. Broadcast can be used to diffuse information to the whole network. It is also used for route discovery protocols in ad-hoc networks. The routing protocols are classified as follows:-

1) Proactive (Table-Driven) Routing Protocol
2) Reactive (On-Demand) Routing Protocol
3) Hierarchical Routing Protocol
4) Hybrid Routing Protocol

Proactive (or Table-driven) routing protocols maintain routing information about each node in the network. The information is updated throughout the network periodically or when topology changes. Each node requires storing their routing in-formation. For example: Destination sequenced Distance vector routing (DSDV).

Reactive or On-demand routing protocols look for the routes and are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. For example: Ad-Hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR).

In Hierarchical routing protocol Nodes are organized in clusters, Cluster head “controls” cluster, one or multiple levels of hierarchy.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

In Hybrid routing protocol, Proactive for neighborhood, Reactive for far away (Zone Routing Protocol), for Proactive for long distance, reactive neighborhood.[3]

2. EXISTING ENCRPTION ALGORITHM

Data Encryption Standard (DES)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and de- crypt blocks of data consisting of 64 bits by using a 64-bit key.[3]

Advanced Encryption Standard (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256.

Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without de- signing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits.[4][5].

3. LITERATURE SURVEY

Interest in the area of Mobile Ad-hoc Network (MANET) is growing since last few years because of its practical applications and requirement of communication in mobile devices. However, in comparison to wired network or infrastructure-based wireless network, MANET is particularly vulnerable to security attacks due to its fundamental characteristics, e.g., the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring and management. The black hole attack is one of such security risks. In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. In this paper, we propose a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs.

The proposed method uses promiscuous mode to detect malicious node (black hole) and propagates the information of malicious node to all the other nodes in the network. The simulation results show the efficacy of the proposed method as throughput of the network does not deteriorate in presence of the back holes.[6]

The possible contributions through the project in the Intrusion detection/Security in WSN as compared to previous approaches are as follow: The proposed system will decrease the consumption of energy. The proposed work will efficiently reduce the amount of information in the entire network. The lifetime of network can be prolonged by the proposed Hybrid Intrusion Detection System (HIDS). The system will enhance security level & can detect more attacks.[7]

Cryptography can be used to implement viruses that are able to mount extortion-based attacks on their hosts. Public-key cryptography is essential in enabling the writer to get an advantage over the victim. We also presented an experimental crypto virus that accomplishes this (it demonstrates cryptographic implementations requiring small space). A model based on a distributed network was then formulated and an algorithm was provided for how to write a virus that is able to gain discretionary access control over its host. We also suggested a set of measures that can be taken to minimize the risks posed by the cryptovirological attacks

the Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. They have proposed a protocol to secure on demand source routing in MANETs that fulfills the security requirements. Our protocol uses one way hash function to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route control packet can be detected. Using Public Key Cryptography (PKC), nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality [9]. Source, destination and intermediate nodes in route list authenticate others nodes by verifying signature. Security analysis results shows, protocol provides the security against many attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack. Our protocol is based on Public Key Cryptography. Asymmetrical algorithms require more calculation than the sym. algorithms. So, it consumes much battery power than protocols based on symmetric algorithms.

4. PROBLEM STATEMENT

4.1 PREVIOUS WORK

Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view.

4.1.1 Related Work

The conventional routing algorithms do not provide security and are prone to attacks caused by malicious nodes moving in the network. Since security is one of the major concerns of ad hoc networks there is a need for secure routing schemes in ad hoc networks. This can be achieved by using either of the following security based routing methods: payment-based systems, reputation-based systems and cryptography-based systems. All these systems have their own features. Of these, the reputation-based systems and the cryptography-based systems are the ones that are most widely used in ad hoc networks. It has also been observed that most of the secure routing algorithms use cryptography as the central mechanism to implement security. Two of the most widely used algorithms for public key cryptography are RSA and Station-to-Station key agreement.

4.1.2 Station-to-Station key agreement in MANETs for generating session key:-Before the protocol, the two parties Alice and Bob each possess a public/private key pair and a certificate for the public key. During the protocol, Alice computes a signature on certain messages and sends Bob the public value ga mod p together with her signature and her public-key certificate. Bob also proceeds a in a similar way. Even though Carol is still able to intercept messages between Alice and Bob, she cannot forge signatures without Alice's private key and Bob's private key. Hence, the enhanced protocol defeats the middleperson attack.

4.1.3. ATTACKS ON STATION TO STATION KEY AGREEMENT

No honest entity X (A or B) can be coerced into sharing a key with another entity without X's knowledge

- Unknown key share attack against B

When A (correctly) believes the key is shared with B, but B believes the same key is shared with some entity C ≠ A

- Unknown key share attack against A

When B (correctly) believes the key is shared with A, but A believes the same key is shared with
Some entity C ≠ B

5. OUR PROPOSED WORK

Step-1:- Defining topology and parameters of the network.

Step-2:- Creating Connection between mobile nodes.

Step-3:- Route Computation from source to destination.

Step-4:- Applying Digital Signature Standard (DSS) in Mobile ad-hoc networks for data encryption and decryption.

Step: - 5 Connection Termination.

6. OBJECTIVES

Our main objectives are listed below:

- To achieve security
- To achieve Authentication
- To achieve Integrity
- To achieve Confidentiality

7. RESULTS AND CONCLUSION

We have Implemented Digital Signature Standard (DSS) algorithm in Mobile ad-hoc Network using Network Simulator 2(NS-2.35). Results have been analyzed in the form of graphs. Parameters considered for graphs are:-

7.1 Throughput:- Throughput is the ratio of number of packets received successfully by a node within a given period of time. Throughput of the network fluctuates with respect to time depends upon the size of the interface queue.

7.2 Delay:- Delay time is another important factor for optimizing a system. If delay time increases of a system that system should not be declared as optimized one in terms of delay. The delay time of the simulation fluctuates because of random positioning and movement of the nodes. The average delay time should provide a profound knowledge of time optimization of a system.

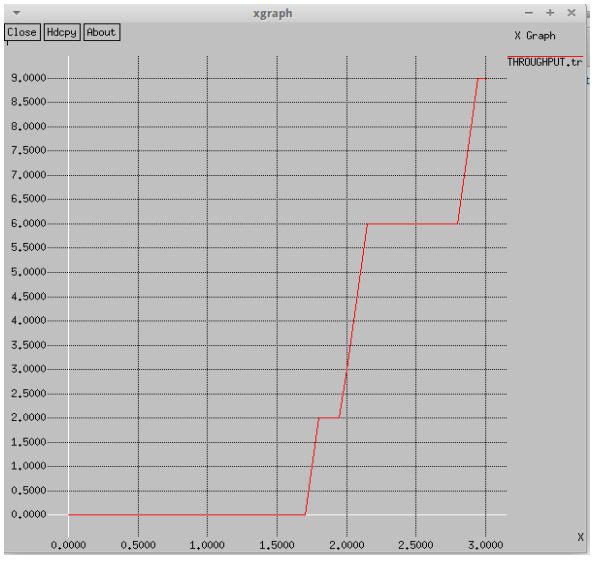

Figure 2: Average Throughput Analyses

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

M: Message **r: Random Secret** **h(M): message digest** **S_1 S_2: Signatures**
d:Alice private key **V:Verification** **(e_1,e_2,p,q): Alice's Public Key**

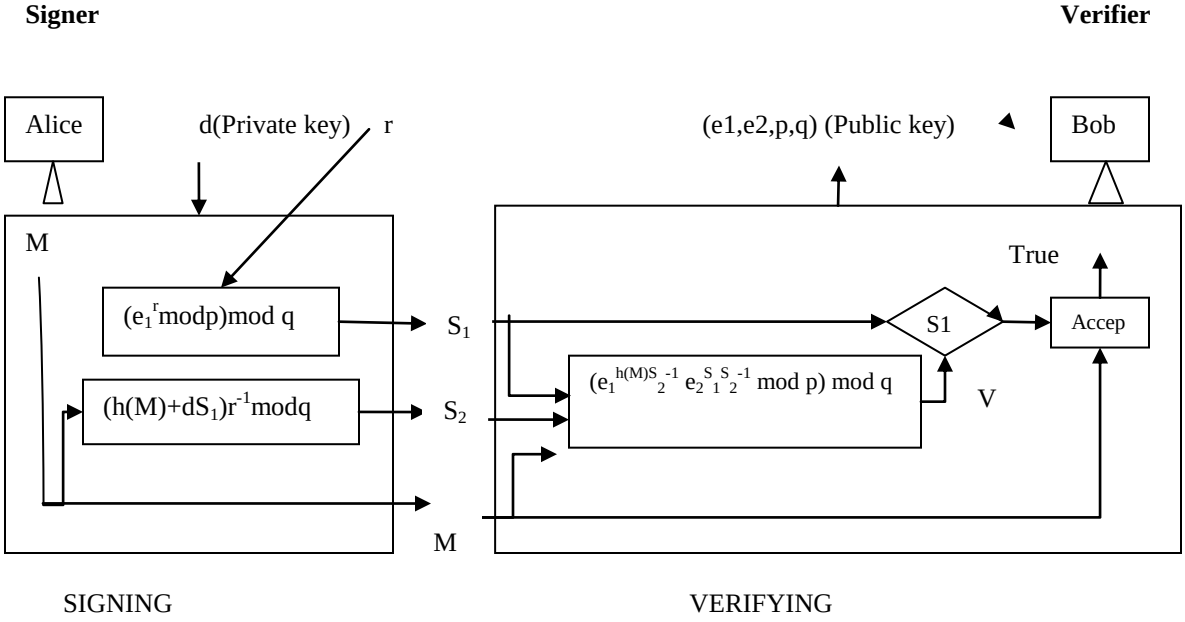

Figure 1: Digital Signature Standard Scheme

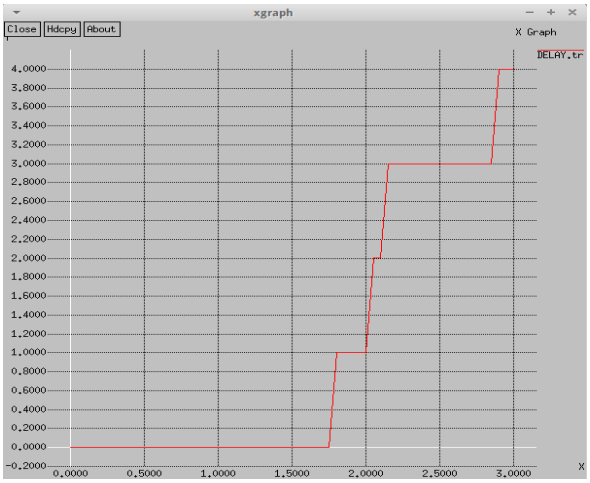

Figure 3: Average Delay Analysis

REFERENCES

[1] **Ms. Sonal Belani, Prof. Parmalik kumar, Prof. Hitesh Gupta (2013)** ***"A Survey on Reliable Routing Protocols using Received Signal Strength in MANET"*** **International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 3067 ISSN 2229-5518.**

[2] **Vishal Garg, Rishu (2012) "*Enhanced Public Key Encryption Algorithm for Security of Network*" International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 ISSN 2229-5518.**

[3] **Gaurav Sharma, Ajay Kakkar (2012) "*Cryptography Algorithms and approaches used for data security*" International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 ISSN 2229-5518.**

[4] **Gurpreet Singh, Supriya Kinger (2013) "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 2058 ISSN 2229-5518.**

[5] **Shafiqul Abidin, Dr. Kumar Balwant Singh (2012) "Authentication of DSS and Secrecy" International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 1 ISSN 2229-5518.**

[6] **Pramod Kumar Singh, Govind Sharma(2012) *"An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET"* 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 978-0-7695-4745-9/12 $26.00 © 2012 IEEE DOI 10.1109/TrustCom.2012.78**

[7] **Mr. Tekchand H. Lonkar Mr. Rajesh Tiwari (2013) "Enhancing the Security of a Cluster-based Wireless Sensor Network Using Hybrid**

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Intrusion Detection System" International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 370 ISSN 2229-5518

[8] Shafiqul Abidin, Rajeev Kumar, Varun Tiwari (2013) "A Review Report on Cryptovirology and Cryptography" International Journal of Scientific & Engineering Research, Volume 3, Issue 11, November-2012 1 ISSN 2229-5518.

[9] Mr. Vivek, R. Shelk, Mr. Sumit Sharma, Prof. Rahul Deshmukh (2013) The Secure Dynamic Source Routing Protocol in MANET to authenticate the node International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 ISSN 2229-5518.