A Secure Data Transmission In MANETs Using Hybrid Technique

Soumya Thomas, *PG Scholar*
Department of Computer Science & Engineering, Amal Jyothi College of Engineerng, Kanjirappally

Syam Gopi ,*Faculty*
Department of Computer Science & Engineering, Amal Jyothi College of Engineering, Kanjirappally

Abstract:

Now a day networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective. Therefore an intrusion detection system (IDS) is required that monitors the network, detects misbehavior or anomalies and notifies other nodes in the network to avoid the misbehaving nodes. Numerous schemes have been proposed for Intrusion Detection systems for Mobile Ad hoc networks. MANET does not require a fixed network infrastructure; every single node works as both a transmitter and receiver. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity. The IDS (Intrusion Detection System) suitable for networks, which detects nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets. The IDS scheme is Enhanced Adaptive ACKnowledgment (EAACK).We propose a hybrid encryption technique to reduce the network overhead caused by digital signature in EAACK.

Keywords: Hybrid Encryption, Mobile Ad hoc Network, Security.

I.INTRODUCTION

In recent years mobile ad hoc networks (MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infrastructure MANETs are an attractive technology for many applications. However, this flexibility introduces new security risks. Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms.

Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDSs are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. In this paper suggest one of the issues of intrusion detection for MANETs using EAACK and reviews the main solutions proposed in the literature and also we provide the design of new protocol for better security using hybrid cryptographic technique. Cryptography which means that the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme.

II.BACKGROUND

a). Cryptographic algorithms

The cryptographic algorithms are classified into two different types such as symmetric and asymmetric method[1].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 and also described about the key distribution difficulties. Large number of protocols provides various techniques. These protocols are to provide more secure but less performance.

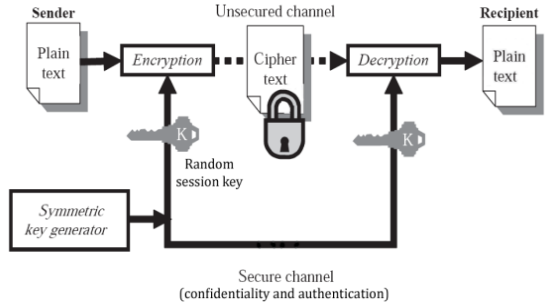

Figure1:Symmetric Encryption

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.

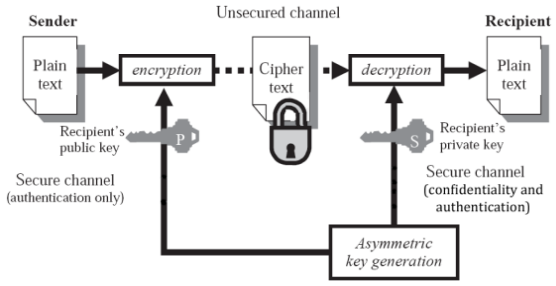

Figure2:Asymmetric Encryption

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. Everyone knows the cryptographic algorithms functionality. The sender sends his data using any one cryptographic algorithm with key value. The key value is more confidential. The key management is also more complex.

b). Overview of Hybrid Encryption Approach

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

The various cryptographic algorithms are available for network security. The symmetric cryptographic algorithms are high speed compared than asymmetric cryptographic algorithms or public key cryptographic systems like RSA, Elliptic Curve Cryptography. The public key cryptographic algorithms are more secure than symmetric algorithms. Because, it has two keys one for encryption and another one for decryption. In this hybrid encryption technique we propose symmetric encryption for encryption/decryption and using public key cryptosystems for authentication [5].

III.EXISTING SYSTEM

The existing system approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision[2].In [2], TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to

the false misbehavior attack. In [2] research work, their goal is to propose a new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, they extend their research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets. The introduction of digital signature to prevent the attacker from forging acknowledgment packets.

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, they adopt a digital signature in existing scheme named Enhanced AACK (EAACK).

EAACK is an acknowledgment-based IDS[2]. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, they incorporated digital signature in existing scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA [3] and RSA [4] digital signature schemes in existing approach.

IV.PROBLEM DEFINITION

The existing scheme implemented both DSA and RSA in EAACK scheme. The DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead [2].

Many of the existing IDSs in MANETs adopt an acknowledgment based scheme, including EAACK. The functions of such detection scheme largely depend on the acknowledgment packets. Hence, it is guarantee that the acknowledgment packets are valid and authentic by using digital signature. In this research work, our goal is to propose a IDS specially designed for MANETs, which solves routing overhead caused by digital signature but also improve the security in system.

V.PROPOSED SYSTEM

In this paper ,we propose a hybrid cryptography technique to reduce the network overhead caused by digital signature. Some times more malicious nodes are present in the network. In more malicious nodes require more acknowledgement packets. At that time the ratio of digital signature in the whole network overhead. In the presence of malicious nodes, routing overhead reduced by any hybrid techniques [6]. Our propose

a hybrid technique by using RSA and AES.

In this research work ,first we find out the secure route for data transmission. The sender send a data to the destination in securely. In our work , sender send a request message for route identification to the destination. Route identification based on AODV(Ad hoc On-demand Distance Vector routing protocol) protocol concept. The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. AODV is capable of both unicast and multicast routing. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network [7]. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicast a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.Based on this protocol , the destination is required to send a reply message to the corresponding sender. After getting a secure route ,our send a data securely to the destination by using hybrid encryption techniques. The data send from the source node will be encrypted with RSA and AES before its travelling to the destination node. Before receiving the data to the destination node will decrypted with RSA and AES. In our work with malicious and non malicious nodes in the network. The figure 3 shows in encryption process are done at sender side in the presence of non-malicious node.

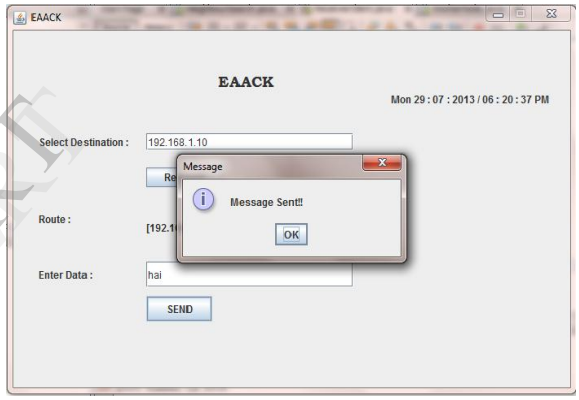

Figure3:Sender side receive an acknowledgement packet with presence of non malicious node.

At the destination node the data will be available on decryption. After receiving the data at destination , the destination node required to send an acknowledgement packet to the source.

In the presence of malicious node ,the destination node is not received the data from the source. Because the sender node cannot be identified the route to the destination.

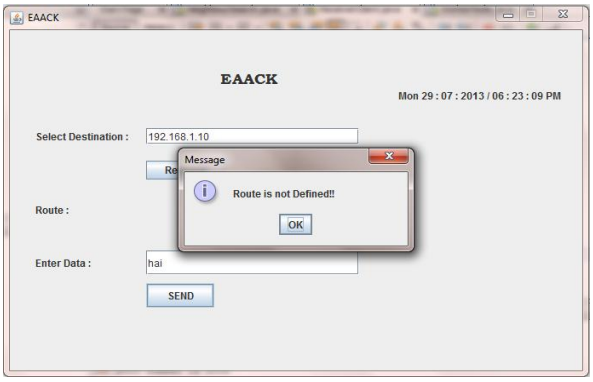

Figure 4:In the presence of malicious node ,sender node cannot be defined the route. So that routing overhead is reduced in hybrid technique compared with DSA in EAACK.

VI.CONCLUSION AND FUTURE WORKS

Packet-dropping attack has always been a major threat to the security in MANETs. Although it generates more ROs in some cases, We think that this tradeoff is worthwhile when network security is the top priority. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate hybrid technique in our proposed scheme, it can reduce the routing overhead in the network.

To increase the merits of our research work, we plan to investigate the following issues in our future research:

1) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys;

2) testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[1]. Dr. E. Ramaraj1, S. Karthikeyan2 and M. Hemalatha3;A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA); International Journal of The Computer, the Internet and Management Vol. 17.No.1 (January-April, 2009) pp 78-86.

[2]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE; EAACK—A Secure Intrusion-Detection System for MANETs; IEEE Transactions on industrial electronics, VOL. 60, NO. 3, March 2013.

[3]. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2,pp. 120–126, Feb. 1983.

[4]. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[5]. William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.

[6]. Palanisamy, V. and Jeneba Mary, Hybrid cryptography by the implementation of RSA and AES,International Journal of Current Research Vol. 33, Issue, 4, pp.241-244, April, 2011.

[7]. Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava;An Overview of AODV Routing Protocol; International Journal of Modern Engineering Research (IJMER) , Vol.2, Issue.3, May-June 2012 pp-728-732 ISSN: 2249-6645.