International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

A Secure Intrusion Detection System for MANET using DSA and Key Exchange

Arockia Rubi.S
PG Scholar, Department of CSE,
NPR College of Engineering and Technology,
Dindigul, Tamilnadu, India.

Dhanalakshmi.N
Assistant Professor, Department of IT
NPR College of Engineering and Technology, Dindigul,
Tamilnadu, India.

Abstract- **MANETs in today`s environment is of great importance. Security is a major challenge in different types of networks such as MANETs. The dynamic features of MANETs makes vulnerable to different types of attacks. However, the communication is limited to the range of transmitters. Due to this limitation, routing protocols in MANET assumes every node in the network cooperate with each other to transmit the data. This assumption leaves the attackers with the opportunity to enter into the network. To solve this problem, an Intrusion Detection System (IDS) should be added to the network. The existing intrusion detection system to detect attacks in the network is based on the acknowledgements. But the attackers have opportunities to forge the acknowledgement packets. In this paper new intrusion detection system is proposed that uses DSA with key exchange algorithm. This proposed scheme performs better and increases the security of network when compared to contemporary approaches.**

Keywords: MANET, DSR, AODV, Attack, Security, key exchange

1. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a transmitter and a receiver; each node uses the bidirectional link to communicate with other nodes of network. MANET formation may vary depending on its application from a small, static network that is highly power constrained to a large-scale, mobile, highly dynamic network. Every node works as both a sender and a receiver.

Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they use their one hop neighbors to transmit messages. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. In MANET communication of node is limited to transmission range. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. This problem is solved by using intermediate nodes in communication. There are two types of MANETs: closed and open.

In a closed MANET, the goal is common to all nodes, such as emergency search/rescue or military and law enforcement operations. In an open MANET, individual nodes have separate goals and they share their resources in order to ensure global connectivity. Some resources are consumed quickly as the nodes participate in the functions. Battery power is more important in a mobile environment.

An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. These types of nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior. A selfish node may refuse to forward the data it received to save its own energy.

However, the open standard of MANET is vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Attackers can easily insert the malicious or incorporate nodes into the network with the help of one or two compromised nodes to achieve attacks. Such misbehaving nodes need to be detected so that these nodes can be avoided by well behaved nodes. Many schemes and intrusion detection systems proposed to detect such nodes.

In this paper, section 2 presents the related works. Section 3 explains the proposed system. Performance analysis is presented in section 4 and concluded in section 5.

2. RELATED WORKS

Security of MANET should ensure the authentication, confidentiality, availability and nonrepudiation. Nodes in MANET network have limited transmission power. So that each node assumes that every node in the network cooperates with each other to transmit the data. But this assumption leaves the attacker with the opportunity to enter into the network with just one or two compromised nodes. So the security level of MANET should be enhanced using Intrusion Detection System (IDS). This section explains the existing intrusion detection systems in MANET.

Marti *et al* [1], proposed a scheme called watchdog. This scheme improves the throughput of the network in the presence of malicious nodes. It has two parts namely, watchdog and pathrater. Watchdog is an intrusion detection system and pathrater is a response system. Watchdog detects the malicious node misbehaviors. Pathrater uses this information and works with routing protocol to avoid the

reported nodes in future transmission. This scheme fails to detect malicious nodes in the following cases: limited transmission power, receiver collision, partial dropping and false misbehavior report.

Liu *et al* [2], proposed a scheme called TWOACK, to solve the weakness of watchdog system. It is not an enhancement scheme of watchdog. This scheme solves the receiver collision and limited transmission power. It detects misbehaving links by acknowledging every data packet transmitted over three consecutive nodes along the route between source and destination. It solves the limited transmission power and receiver collision but it adds unwanted overhead to the network, because it needs to acknowledge every transmitted data packet.

The authors in [3], proposed the protocol called CONFIDANT. It consists of four important components—the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node constantly monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the event are passed to the Reputation System. This scheme also suffers from the same problems of watchdog.

Sheltami *et al* [4], proposed an acknowledgement based scheme called AACK with the ability to detect misbehaved nodes and avoid them in other transmissions. The goal of AACK scheme is to overcome watchdog weaknesses due to collisions and limited transmission power. It reduces the overhead than the TWOACK scheme and also maintains the network throughput.

3. PROPOSED SYSTEM

In MANET security is breached by attackers by means of attack, for example packet dropping attack is a major threat to security. To enhance the security MANET needs an intrusion detection system. This proposed approach introduces the new intrusion detection system called Enhanced adaptive Acknowledgement (EAACK). This is an acknowledgement based intrusion detection system. In this approach attackers have opportunities to initiate the forged acknowledgement attacks. To prevent this attack digital signature is used with this scheme.

Digital signature is a data string; it associates a message with some entity that creates the message or an electronic form signature. It is used to ensure the integrity, authentication and nonrepudiation. Every acknowledgement packets should be digitally signed by the sender of the acknowledgement packet. The key exchange mechanism also used with this scheme to avoid the need of pre-distribution of keys to the network nodes.

A) Key Exchange Mechanism

Key exchange is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Key exchange is used whenever the node wants to communicate or wants to know the key of another node or destination node. To avoid pre distribution of keys, key exchange is used. If source needs shared key between itself and destination then it initiates KREQ/KRREQ packet. First source searches for the route between the source and destination. If it already have the route then it send KREQ packet only. Otherwise it will send KRREQ/KREQ packet. Upon receiving request packet destination reply with the key to the source. Destination may receive multiple copies of KREQ from same source. It will reply to all copies along with the key generated by it. Both source and destination stores the path and key information in the buffer. After receiving the key source starts to send data packets to the destination.

In this proposed system diffie hellman key exchange is used, which allows users to establish 'secure channels' on which to exchange keys, even if an Opponent is monitoring that communication channel. Key exchange is explained in the following figure.

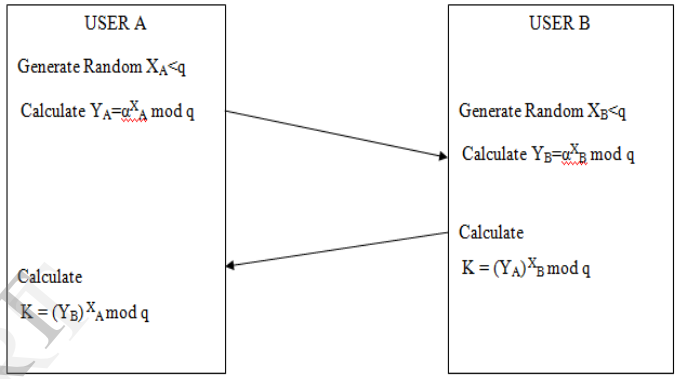

Fig 6.2 Diffie Hellman key exchange

B) Intrusion detection system

Intrusion detection system detects the malicious nodes, attackers in the network which cause the packet dropping, acknowledgement forging to breach the security of the network. In MANET nodes have limited transmission power; so that every node in the network assumes that each node will cooperate with each other to transmit the data packet. This detection system has three parts: ACK, S-ACK, and MRA. Whenever the source wants to send the data to destination, it will first find the path and key of the destination. After getting route and key it will store them on its local base. It also stores the alternate paths between the destination and itself.

ACK:

Source knows the key of receiver and route to the destination then it transmit data packet to the destination by the use of intermediate nodes. Every node in the network has the address of its one half neighbor node. Each packet has the field packet flag that indicate the type of packet.

Upon receiving the data packet, destination have to send the acknowledgement packet to the source indicating that the receiver successfully received the data packet. Source set the time interval for the acknowledgement packet. Source receives the acknowledgement within the predefined time period then the transmission is successful; otherwise source will switch to S-ACK mode.

S-ACK:

In this every three consecutive nodes in the route between the source and destination works in a group to

acknowledge the packet it received. Third node in a every group needs to send acknowledgement to the first node. In this process second node have chances to forge the acknowledgement packet from the third node or it will drop the packet it has received from first node and send a forged acknowledgement.

To avoid this intermediate nodes initiating acknowledgement forging, third node have to digitally sign the acknowledgement packet using its private key. After receiving acknowledgement from third node, first node should verify the authenticity by checking the signature of third node. If the first node doesn't receive the acknowledgement within the particular time period then the first node reports that the second and third nodes are misbehaving. Upon receiving this node misbehavior source will switch to Misbehavior Report Authentication (MRA) mode.

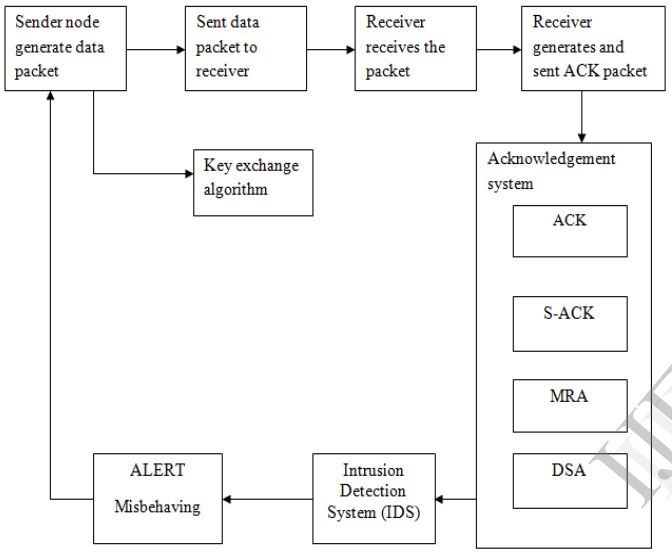

Figure 3.1 System Design

MRA:

Source will search for the alternate path to the destination in its local base. Using that alternate path it will send the MRA packet to the destination. This helps to find the false report in the secure ACK (S-ACK) mode. After receiving the MRA packet by the alternate path destination will check against with its local base. If it already received the same MRA then new report considered as false and the node which generated the report marked as malicious and in future transmission that node will be eliminated from the path.

TABLE 1
Packet Type Indicators

Packet Type	Packet Flag
General data	00
ACK	01
S-ACK	10
MRA	11

If the destination doesn't have any MRA then it accepts this report and the nodes in the packet marked as malicious; the nodes in the report will be eliminated in future transmissions.

C) Digital Signature:

Digital signature is a part of cryptography. Cryptography is a study of information security aspects such as entity authentication, confidentiality and integrity of the data using mathematical aspects. Security of MANET needs to ensure the confidentiality, integrity, availability, nonrepudiation and authentication. For this purpose in this proposed model uses digital signature. Digital signature defined as a data string, it associates the entity with messages. It has two categories. It may need original message in the verification process uses digital signature algorithm (DSA). Sometimes the signature alone is enough in the verification process, it uses RSA algorithm.

To calculate signature, first the message digest (md) in fixed length is calculated using hash function H for the message s.

$$H(s) = md \qquad \text{(i)}$$

After calculating message digest, sender applies its private key on the computed message digest (md). Finally the sender attaches the message digest (md) with message s and send to receiver.

$$S_{p_r}(md) = Sig_S \qquad \text{(ii)}$$

Upon receiving the data packet from the sender, receiver will calculate the message digest (md') again on the received message using the hash function (H).

$$H(s') = md' \qquad \text{(iii)}$$

After calculating the message digest (md'), receiver applies the sender's public key on the received signature to get the original message digest (md) which is calculated by the sender.

$$S_{p_k}(Sig_S) = md \qquad \text{(iv)}$$

If the calculated and received message digest (md == md') were same means the received message is secure and it ensures no one is altered in transit.

4. PERFORMANCE EVALUATION

This section describes the simulation methodologies and also compares the performances of watchdog scheme and proposed intrusion detection scheme through simulation result. To measure and compare the performances of proposed system, two performance metrics are adopted.

1) Packet Delivery Ratio: It defines the ratio of the number of packets received by the destination node to the number of packets sent by the source.
2) Routing Overhead: It defines the ratio of the amount of routing related transmissions [RREQ, RREP, ACK, S-ACK and MRA].

Simulation Results

This simulation is designed to test our proposed intrusion detection system performance based on packet dropping attack and false misbehavior attack.

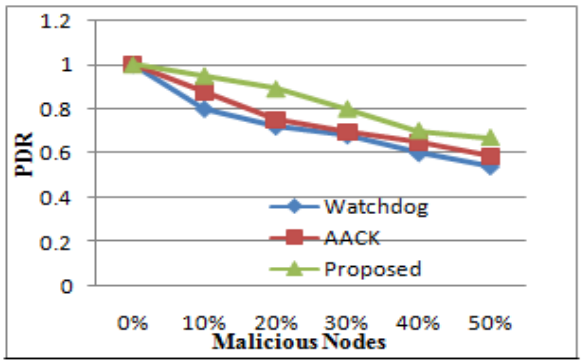

Fig.1 PDR against packet dropping attack

In Fig.1, it shows our proposed IDS perform better than the watchdog. From this result, our proposed scheme s able to detect the misbehaviors with the presence of limited transmission power.

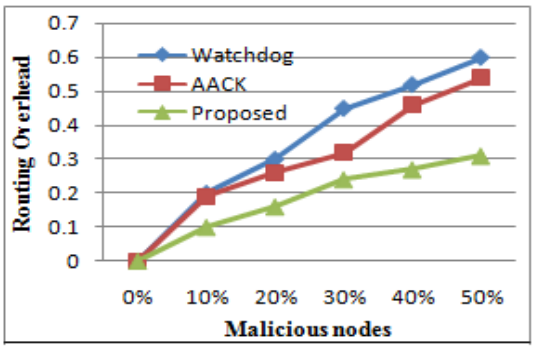

Fig.2 RO against packet dropping attack

In Fig.2, it shows result for routing overhead. Our proposed system yields better performance than other acknowledge based intrusion detection system, because this proposed system uses key exchange. It avoids the overhead caused by pre distribution.

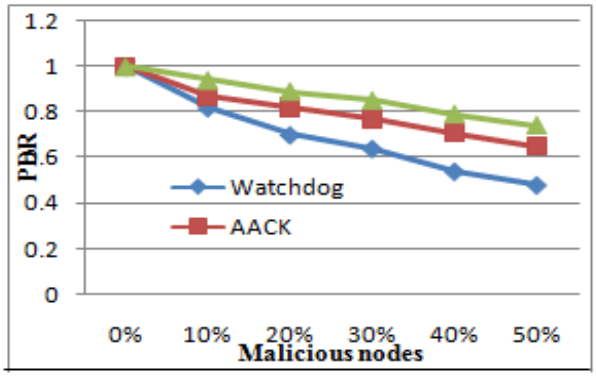

Fig.3 PDR against false misbehavior report

In Fig.3, it shows the result for packet delivery ratio in case of false misbehavior report. In this, the proposed system works better than existing intrusion systems namely, watchdog and AACK. This is achieved by the use of MRA scheme in our proposed system.

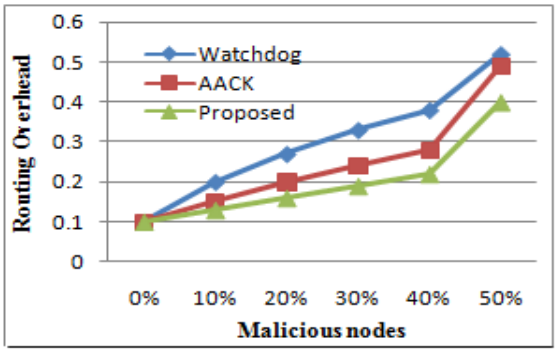

Fig.4 RO against false misbehavior report

5. CONCLUSION

In this paper, an intrusion detection system is proposed to detect the malicious nodes, attackers and false reports in the network. This system is used with key exchange and digital signature for authentication and to reduce the overhead caused by pre distribution of keys. Packet dropping attack is a major security threat to the mobile adhoc network. This proposed system greatly reduces the packet dropping and also detects the malicious misbehaviors in the cases of false misbehavior report. Digital signature is used with this system prevent the attackers from initiating forged acknowledgements. The simulation result shows the positive performances of the proposed system against packet dropping and false misbehavior report.

REFERENCES

1. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" *IEEE trans*. Vol.60, no.3, MAR, 2013.
2. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.
3. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
4. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
5. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
6. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron., vol. 55, no. 4, pp.* 1835–1841, Apr. 2008.
7. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008. [16] K. Liu, J. Deng, P. K
8. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.
9. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.