IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 49-54
www.iosrjournals.org

Enhancement of Security Levels Using a Secure Intrusion Detection System in Manets

[1]Lakshmi. S. M, [2]Bhavana. S, [3]Sujata.Terdal
[1]M.Tech 4th SEM, Department of CSE, VTU Regional PG Center Gulbarga.
[2]Assistant Professor, Dept of CSE, VTU Regional Center, Gulbarga.
[3]Associate Professor, Dept of CSE, PDA Engineering College, Gulbarga.

Abstract: *A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies .A Security is an important issue for ad hoc networks, especially for those security-sensitive applications .Since there is no centralized infrastructure, MANET's are vulnerable to attackers .Prevention and detection mechanisms should be focused before an attacker can damage the structure of the system..First this paper gives an overview of IDS architecture for enhancing security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. Then a hybrid cryptography IDS to reduce the network overhead caused by digital signature is indicated.*

***General Terms*:** *SIDS architecture, DSA and RSA algorithm, Hybrid cryptography IDS.*
Keywords: *Mobile Ad hoc Networks (MANETs), Secure Intrusion- Detection Systems (SIDS), Malicious Nodes.*

I. Introduction

Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes that are free to move randomly and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably. Nodes involved in network are equipped with transmitter and a receiver that communicate directly with each other if nodes are in communication range or forward message through intermediate nodes if nodes are out of communication range.

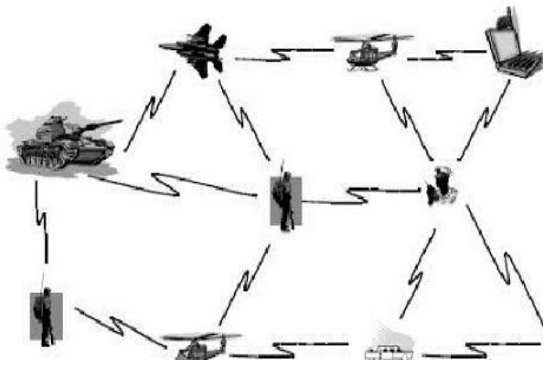

Fig. 1 Mobile Adhoc Network

Major advantage of mobile networks is to allow different nodes for data communication and still maintain their mobility. However, this communication is limited to the range of transmitters. It means two nodes cannot communicate with each other when the distance between the two nodes is out of communication range. MANET solves this problem by allowing intermediate nodes to relay data transmission .There are two types of network single-hop and multi-hop network. In a single-hop network, all nodes communicate directly with each other within the same radio range but in a multi-hop network, nodes depend on intermediate nodes to transmit if nodes are out of their radio communication range [1]. MANET is capable of operating a self-maintaining and self-organizing network. MANET does not require expensive base stations of infrastructure dependent network (single-hop wireless networks).As MANETs have different characteristics from wired networks there are number of challenges interrelated to security issues that need to be addressed .Recently MANET'S are designed for search and rescue mission, data collection, virtual classes and conferences where laptops, PDA or other mobile devices are in wireless communication. Since MANET is being used wide spread, security has become a very important issue [2]. In general, MANETs are more vulnerable to attackers based on some basic

characteristics such as open medium, changing topology, absence of infrastructure, restricted power supply, and scalability. In such case, Intrusion Detection System can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called as Intrusion Detection System (IDS) [3] [4].

The rest of the article is organized as Section 2 presents the review of about SIDS in MANETs. Section 3 presents the IDS architecture for enhancing security level of MANETs based on various algorithms, namely RSA and DSA. Finally, conclusion and discussion are p r e s e n t e d in Section 4

II. Sids In Manets

Intrusion detection is a technique to identify "any set of actions that compromise the integrity, confidentiality, availability, non-repudiation of a resource". For MANETs, the main function of IDS is to detect misbehaviors by observing the networks traffic. There are two important models of Intrusion detection systems namely: signature based and anomaly based approaches [5] . A signature-based IDS monitors activities on the networks and compares them with known attacks. However, a drawback of this approach is new unknown threats cannot be detected. In anomaly-based detection, profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, usually statistically and significantly different from determined, is flagged as suspicious. Anomaly detection can detect unknown attacks, But the issue is that anomaly based approaches yield high false positives for a wired network. If these statistical approaches are applied to MANET, the false positive problem will be worse because of the unpredictable topology changes due to node mobility in MANETs. The specification based approach is ideal for new environments, such as MANETs. In specification-based detection, the correct behaviors of critical objects are abstracted and crafted as security specifications, which are compared to the actual behavior of the objects. Intrusions, which usually cause an object to behave in an incorrect manner, can be detected without exact knowledge about the nature of the Intrusions. Most of recent researches focused on providing preventive schemes to secure routing in MANETs.

2.1 Security attributes

Security has become a most important service in Mobile Ad hoc Network (MANETs). To secure an ad hoc network, the following attributes are to be considered: availability, authentication and key management, confidentiality, integrity, non-repudiation, and scalability. In order to achieve this goal, the security solutions for each layer which are providing complete protection for MANETs are to be described.

There are five main layers on the network, as follows:

1. Application layer: Detecting and preventing viruses, worms, malicious nodes, and application abuses.
2. Transport layer: Authenticating and securing end-to-end communications through data encryption.
3. Network layer: Protecting the ad hoc routing protocols.
4. Link layer: Protecting the wireless MAC protocol and providing link-layer security.
5. Physical layer: Preventing traffic jamming denial-of-service attacks.

Table 1. Security attributes in MANETs

S.No	Attributes	Goals	Method
1	Availability	Resources can be accessed by all the nodes involved in network.	Distributed Adaptive Service Replication (DAR)
2	Authentication and key management	It ensures that data transmission is authentic.	Hybrid cryptography technique.
3	Confidentiality	It protects data from unauthorized access.	Converting original data into an unintelligible format using Data Encryption Standard(DES)

4	Integrity	It ensures that data being transmitted is not corrupted.	Cryptographic hash function algorithm
5	Non-repudiation	It ensures that sender and receiver of information cannot disagree information	Digital signature
6	Scalability	It ensures that newly added nodes in the network to be managed without corruption.	Secure routing protocols used to manage the scalability.

2.2 Discovering malicious nodes

1) Watchdog**:** It is very highly efficient IDS for improving the network throughput with the presence of malicious nodes. This IDS can be classified into two methods such as Watchdog and Path rater.Watchdog detects malicious misbehaviors by listening to its next hop's transmission in the network. If a Watchdog IDS overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in further transmission.

The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; and 5) partial dropping.

2) TWOACK**:** It is another important IDS for discovering malicious nodes in MANETs [6]. The main aim of TWOACK IDS is to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving nodes or links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route.

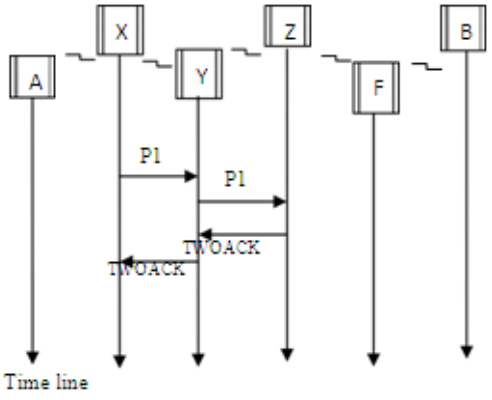

Fig. 2 TWOACK IDS for MANETs

In Fig. 2: Node X wants to transmit Packet 1 to node Y, and then, node Y transmit Packet 1 to node Z. When node Z receives Packet 1, as it is two hops away from node X, node Z generates a TWOACK packet, which contains reverse route from node X to node Z, and sends it back to node X. The retrieval of this TWOACK packet at node X indicates that the transmission of Packet 1 from node X to node Z is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes Y and Z are reported as malicious nodes. The same process applies to every three consecutive nodes along the rest of the route.

The TWOACK IDS effectively processes the receiver collision and limited transmission power problems of Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem.

3) AACK**:** It is same as TWOACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an IDS called TACK (identical to TWOACK) and an end-to-end acknowledgment IDS called Acknowledge (ACK). Compared to TWOACK IDS, AACK

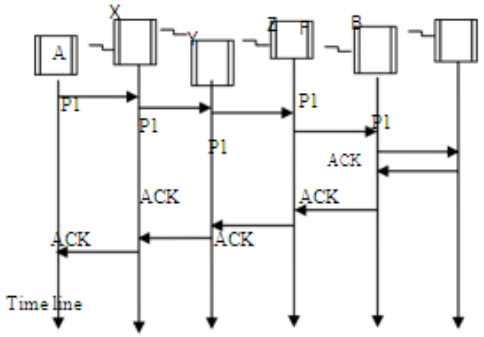

Fig. 3 End-to-End ACK IDS for MANETs

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

III. A Secure Ids Architecture

Secure IDS architecture (EAACK) introduced to improve the security level of MANETs based on security attributes and various algorithms. EAACK is designed to tackle three out of six weaknesses of Watchdog IDS, namely, 1) Receiver collision, 2) Limited transmission power, 3) False misbehavior.

1) Receiver collisions: Example of receiver collisions, shown in Fig. 4, after node X sends Packet 1 to node Y, it tries to overhear if node Y forwarded this packet to node Z; meanwhile, node F is forwarding Packet 2 to node Z. In such case, node X overhears that node Y has successfully forwarded Packet 1 to node Z but failed to detect that node Z did not receive this packet due to a collision between Packet 1 and Packet 2 at node Z. IDS reduces network overhead.

The end-to-end ACK IDS is shown in Fig. 3. The source node A sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node B receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node A along the reverse order of the same path. Within a predefined time, if the source node A receives this ACK packet, then the packet transmission from node A to node B is successful. Otherwise, the source node A will switch to TACK IDS by sending out a TACK packet. The concept of adopting a hybrid IDS in AACK reduces the network overhead greatly, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes in the presence of false misbehavior report and fake ACK packets.

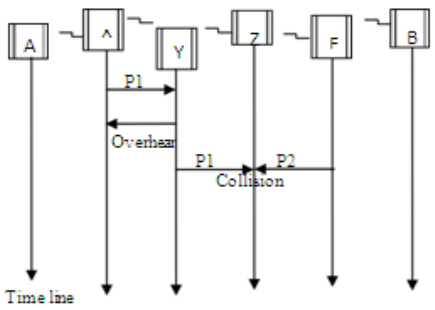

Fig. 4 Receiver collisions in MANETs

2) Limited transmission power: Example of Limited power, shown in Fig. 5, in order to manage the battery power in MANETs, node Y limits its transmission power so that it is very strong to be overheard by node X after transmitting the packet (P1) to node Z , but too weak to reach node Z.

3)

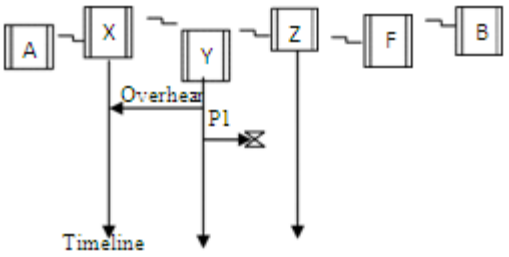

Fig. 5 Limited transmission power in MANETs

4) False misbehavior**:** Example of false misbehavior in MANETs, shown in Fig. 6, Even though node X and Y forwarded Packet 1 to node Z successfully, node X still inform node Y as misbehaving, as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve false misbehavior report attack. TWOACK and AACK IDS are vulnerable to the false misbehavior attack. In order to solves not only receiver collision and limited transmission power but also the false misbehavior problem to launch Secure IDS architecture (EAACK) .

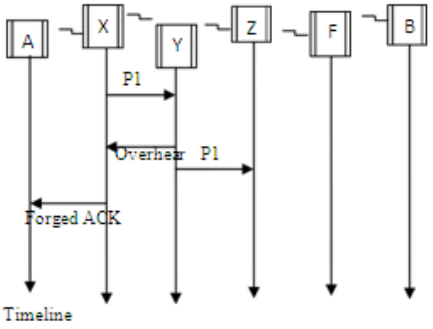

Fig. 6 False misbehavior in MANETs

4.1 Secure IDS description

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA). In order to distinguish different packet types in different schemes 2-b packet header is involved in EAACK. According to the Internet draft of DSR [7], there is 6 b reserved in the DSR header. In EAACK, 2 b of the 6 b is used to distinguish different types of packets.

Data	ACK	S-ACK	MRA

Fig. 7 EAACK protocol in MANETs

In this secure IDS, It is assumed that the link between each node in the network is bidirectional. Furthermore, for each communication process, both source node and destination node are not malicious node. All acknowledgment packets are to be digitally signed by its sender and verified by its receiver.

1) ACK: ACK is basically an end-to-end ACK IDS.It is a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time slot, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes along the route in the network.

2) S-ACK: It is an improved version of the TWOACK IDS [6]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The main advantage of introducing S-ACK mode is that it detects misbehaving nodes in the presence of receiver

collision or limited transmission power.

3) MRA : Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA field is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes[8]. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

4) Digital Signature: EAACK is an acknowledgment-based IDS.They all rely on ACK 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 forge acknowledgment packets, all of the three schemes will be vulnerable to attacks. To overcome this problem digital signature is adopted in secure IDS. To ensure the integrity of the IDS, EAACK requires all ACK packets to be digitally signed before they are sent out and verified until they are accepted [9].

4.2 Secure IDS in DSA and RSA

The signature size of DSA is much smaller than the signature size of RSA. So the DSA scheme produces slightly less network overhead compared to RSA . However the Routing Overhead differs between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes, the more Routing Overhead's the RSA scheme produces.This can be assumed due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network. With respect to this result,DSA is found as a more desirable digital signature scheme in MANETs [10]. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

IV. Conclusion And Futurework

In this paper, a comparative study of Secure Intrusion- Detection Systems (SIDS) for discovering malicious nodes and attacks on MANETs is presented. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure levels of network. In this case detection should be focused as another part before an attacker can damage the structure of the system. Secure IDS named EAACK protocol specially designed for MANETs. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. As security is very important in MANETS, hybrid cryptography architecture will tackle the issue in an efficient manner.

References

[1]. EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE

[2]. Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[3]. Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad,2003."Chapter 30:Security in wireless ad- hoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publisher

[4]. 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.

[5]. "A study of different types of attacks on multicast in mobile ad hoc networks" Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier AdHoc Networks(2008) 32-46. [7] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6]. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[7]. A. Tabesh and L. G. Frechette, "A low-power stand- alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[8]. "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol"Ahmed M. Abdulla, Imane A. Saroitb, Amira Kotbb, Ali H. Afsaric a* 2010 Published by Elsevier Lt.

[9]. H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks:Challenges and solutions" (2004). IEEE Wireless Communications. 11(1), pp. 38-47.

[10]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.