A Survey of Secure Intrusion Detection Systems for MANET

Priyanka Bhavsar\(^1\), Bhushan Thakare\(^2\), Hemant Deshmukh\(^3\)

priyanka.bhavsar85@gmail.com\(^1\), bhushan.thakare86@gmail.com\(^2\), hrdphdl@rediffmail.com\(^3\)

Department of Computer Engineering\(^1, 2, 3\)
Sinhgad Academy of Engineering, Pune\(^1, 2\)
Dr. Rajendra Gode Institute Of Tech & Research, Amravati\(^3\), India\(^1, 2\)

Abstract—Migrating from wired network to wireless network has been a global trend. Mobile Ad hoc NETwork (MANET) is one of the most unique and vital applications. MANET does not require a fixed network infrastructure; every node behaves as both transmitter and receiver. Nodes can communicate directly if they are in the same communication range. Otherwise, they rely on neighbours to communicate the messages. MANET is popular in military applications because of its self configuring ability. However, because of the open medium and the wide distribution of nodes, the MANET is vulnerable to malicious attacks. So it is very important to develop an efficient intrusion-detection system to protect MANET from attacks.

In this paper, there is a survey of IDS specially designed for MANETs. EAACK is capable of detecting malicious nodes despite the existence of false misbehavior reports. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performance.

Keywords—Digital Signature, Enhanced Adaptive Acknowledgment (EAACK), (AACK), Mobile AdHoc Network (MANET).

I. INTRODUCTION

MANET consists of wireless mobile nodes that form a temporary network without the aid of fixed infrastructure or central administration. Nodes can communicate directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, noncooperation may occur which can severely degrades the performance of network. MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defense line of network becomes ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect. Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols have been proposed in literature and can be classified into proactive, reactive and hybrids protocols.

MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations. Securing wireless adhoc network is highly challenging issue. The attacks can be classified as Denial of Service Attack, Jamming, Replay Attack and Wormhole attack.
(a) Denial of Service Attack: In this attack, the attacker attacks the availability of a node or the entire network. Radio signal jamming and battery exhaustion methods are used by the attacker.

(b) Impersonation: A malicious node acts as a genuine node and monitors the network traffic. It can also send fake routing packets and gain access to confidential information.

(c) Eavesdropping: Malicious node observes the confidential information and the information can be later used by the node. The secret information like public-key, password, location, private-key etc. can be fetched by eavesdropper.

(d) Routing Attacks: The malicious node attacks the routing services. The attack can be on routing protocol and another is on packet forwarding or delivery mechanism.

(e) Black-hole Attack: Black hole attack refers to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.

(f) Gray-hole Attack: This attack drops packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This attack is also known as routing misbehavior attack which leads to dropping of messages.

(g) Man-in-the-middle Attack: Attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, the attacker may impersonate the sender to communicate with receiver or impersonate the receiver.

(h) Jamming: In jamming, the attacker initially monitors the wireless medium in order to determine a frequency at which the destination node is receiving signal from the sender. It then transmits signal on that particular frequency so that the error free receptor is hindered.

(i) Replay Attack: An attacker that performs a replay attack. Packets with the valid data are repeatedly retransmitted to shoot the network routing traffic that has been captured earlier. This attack targets the freshness of the routes, but can also be used to weaken the poorly designed security solutions.

(j) Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network and "tunnels" them into another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attacks is known as a wormhole.

II. HISTORY & BACKGROUND

A. Intrusion Detection in MANET

In the Intrusion Detection Systems that are used for traditional wired networks, all the traffic must go through switches, gateways, or routers. Hence, Intrusion Detection Systems can be appended to and implemented in these wired devices easily. On the other hand, Mobile Adhoc NETworks do not have these devices. Also, the medium is wide open, so both the legitimate and the malicious users can access it. And also, there isn’t clear separation between normal and unusual activities in a mobile ie wireless environment. Since nodes can move randomly, false routing information could be from an updated node or a node that has outdated information. Hence, the current Intrusion Detection Detection Systems techniques on wired ie connected networks cannot be applied directly to Mobile Adhoc NETworks. Many Intrusion Detection Systems are proposed to accommodate the characteristics of MANETs.

B. Watchdog

The main objective of the watchdog mechanism is to improve the throughput of the network even in the presence of malicious nodes. The watchdog scheme is of the following two types namely watchdog and path-rater. The watchdog system serves as an intrusion detection system for Mobile Adhoc Network and is responsible for detecting malicious node misbehavior in the network. Watchdog detects misbehavior of malicious nodes by indiscriminately listening to its next hop’s transmission. When a Watchdog node overhears that its next node fails to forward a packet within a threshold period of time, it increases the node’s failure counter. Whenever the node’s failure counter exceeds the predefined threshold value, the Watchdog node reports it as misbehaving. Simultaneously, watchdog system maintains a buffer of recently sent packets and it compares each overhead packet with the packet in the buffer. Data packets are cleared from the buffer when the watchdog overhears the same packets being forwarded by the next-hop node over the same medium. If some data packet remains in the buffer for a long time, then the watchdog scheme incriminates the next-hop neighbor to be misbehaving.

![Fig. 1: Working Mechanism of Watchdog](image)

When the source node S has to forward a packet to destination node D, then uses intermediate nodes A, B and C for this purpose. Node B forwards a packet from the source S towards the destination D through the intermediate node C, as node A cannot transmit the packet all the way to node C. But node A can listen to node B’s traffic. Node A can overhear node B’s transmission and can verify whether node B has attempted to pass the packet to node C. The solid line represents the intentional direction of the packet sent by node B to node C, while the dashed line depicts that node A
is within transmission range of node B and can overhear the packet transfer. The path-rater technique is used to avoid the use of the misbehaving nodes in any of the future route selections. The information related to routing can be passed with the message itself. The watchdog scheme fails to detect malicious behavior of the nodes in the presence of the following:

- Ambiguous Collisions.
- Receiver Collisions.
- Limited Transmission Power.
- False Misbehavior Report.
- Collusion.
- Partial Dropping.

C. AACK

AACK is a new scheme called as Adaptive ACKnowledgement. It is similar to TWOACK scheme. AACK is an acknowledgment-based scheme which works on the network layer and can be considered as a combination of two schemes called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called as ACKnowledge (ACK). When compared to TWOACK, AACK significantly reduces the network overhead and it is still capable of maintaining and also excelling the network throughput.

III. PROBLEM DEFINITION

Enhanced Adaptive ACKnowledgement (EAACK) is designed to tackle two problems out of the six drawbacks of Watchdog scheme, namely, false misbehavior report and receiver collision problem.

A. Receiver Collisions

When Node A sends a data Packet 1 to node B, node A tries to overhear if node B has forwarded this packet to node C. Meanwhile, node X is forwarding data Packet 2 to node C.

B. False Misbehavior Report

Even when Node A overheard that node B successfully forwarded Packet 1 to node C, node A still reported node B as misbehaving. Due to the open medium of MANET and the remote distribution of nodes in MANETs, the attackers can easily capture and mislead one or two nodes in the network to achieve this kind of false misbehavior report attack.

IV. EXPERIMENTAL RESULTS

EAACK is consisted of two major parts. They are Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA). Digital signature is introduced in the EAACK scheme to forbid the attacker from forging the acknowledgment packets.

A. ACK

ACK is ACKnowledgement is fundamentally an end-to-end acknowledgment scheme. It aims to reduce network overhead when no network misbehavior is detected. If the ACK scheme fails, then the node switches to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.
B. S-ACK
The S-ACK scheme is the advanced and improved version of TWOACK scheme. The basic principle of S-ACK is to let each three consecutive nodes in the network work in a group to detect the misbehaving nodes. For each of the three consecutive nodes in the route, the third node has to send an S-ACK acknowledgement packet to the first node in the network. S-ACK mode was introduced with an intention to detect misbehaving nodes in the presence of receiver collision.

C. MRA
The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog scheme which is detecting the misbehaving nodes with the presence of false misbehavior report. The essence of MRA scheme is to authenticate whether the destination node has received the reported missing packet through some different alternate route in the network.

An alternate route is required to send the MRA packet to the destination node. When the MRA packet reaches the destination node, it searches its local knowledge i.e. database and compares if the packet which was reported as missing packet was received. If it is received already by the destination, then it is safe to resolve that the misbehavior report was false and the node which generated this misbehavior report is marked as malicious node. Otherwise, the misbehavior report is trusted and accepted and the packet is resent.

D. Digital Signature
EAACK is an acknowledgment-based intrusion detection system (IDS). This scheme relies on the acknowledgment packets to detect misdoing in the network. Thus, it is enormously important to ensure that all the acknowledgment packets in EAACK scheme are authentic and untarnished. In order to ensure the integrity of this IDS, EAACK requires all acknowledgment packets to be signed digitally before the packets are sent out from the node and are verified on each step until they are accepted at the destination.

V. Performance Evaluation
In order to determine and equate the performance of the EAACK system, the following performance metrics are adopted.

1) Packet Delivery Ratio:
Packet delivery ratio (PDR) is defined as, the ratio of the data packets received by the destination to the number of packets sent by the source nodes.

\[
PDR = \frac{\sum \text{Received packets at destinations}}{\sum \text{Sent packets by sources}}
\]

2) Delay:
Network delay is one of the important design and performance characteristics. The delay of a network specifies how long a bit of data takes to travel across the network from one node i.e. endpoint to another node or endpoint.

3) Routing Overhead:
Routing overhead refers to the ratio of the routing related transmissions. Overheads are the indirect elements of cost.

The following are the comparison graphs that are plotted between the malicious nodes and Packet Delivery ratio.
VI. COMPARATIVE STUDY
A summarized comparison of all the intrusion detection systems is shown in Table 1.

VII. ADVANTAGE OF EAACK
- EAACK solves the limited transmission power problem and receiver collision problem.
- It is capable of detecting misbehavior attack.
- It ensures authentication and integrity of packets.
- Digital signatures prevent the attack of forged acknowledgement packets.

VIII. FUTURE ENHANCEMENT
- Possibilities of adopting hybrid cryptography techniques to reduce the network overhead that is caused by digital signature.
- Examine the possibility of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys in RSA and DSA.
- Testing the performance of EAACK in real network environment.

IX. CONCLUSION
EAACK makes MANETs secure to a greater extent. The starring threats like false misbehavior report and the forged acknowledgement packets can be detected by using this scheme. EAACK system is specially designed for MANETs and is compared against other popular mechanisms in different scenarios through simulations.
- Results of comparison demonstrate a positive performance against existing schemes such as watchdog, TWOACK.
- Digital signatures were integrated which caused greater ROs but highly improved the PDR when attackers are smart to inscribe forged acknowledgement packets.
- In EAACK we can implement both DSA and RSA but DSA scheme is more suitable.

REFERENCES
[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
<table>
<thead>
<tr>
<th>TECHNIQUE</th>
<th>MALICIOUS ROUTING</th>
<th>ROUTING OVERHEAD</th>
<th>FALSE MISBEHAVIOUR REPORT</th>
<th>PACKET DELIVERY RATIO</th>
<th>DETECTION AND PREVENTION OF FORGED ACKNOWLEDGEMENT</th>
<th>BLACK HOLE ATTACK DETECTION AND REMOVAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>WATCHDOG</td>
<td>No</td>
<td>Large</td>
<td>No</td>
<td>Low</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TACK</td>
<td>Yes</td>
<td>Lesser than TWOACK</td>
<td>No</td>
<td>Large</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TWOACK</td>
<td>Yes</td>
<td>Large</td>
<td>No</td>
<td>Medium</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>AACK</td>
<td>Yes</td>
<td>Lesser than TWOACK</td>
<td>No</td>
<td>Large</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EAAACK</td>
<td>Yes</td>
<td>Same as AACK</td>
<td>Yes</td>
<td>Large</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>