A Case Study on Intrusion Detection Technique in MANET

Midhila Muraleedharan
Computer Science, School of Technology and Applied Sciences

Abstract: Wireless networks are becoming popular because of their ease of access and connectivity, especially the Ad hoc network which can be setup in a minute and supports mobility. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. The routing in MANET provides shorter path to reach destination, but that may not be the reliable one. So to make it reliable researchers have proposed various security mechanisms like Intrusion Detection Systems (IDS), Secure routing protocols, firewalls etc. The Enhanced Adaptive Acknowledgement (EAACK) is one of the security schemes. In EAACK, the S-ACK mode successfully detects the malicious link in the network. But it declares both the nodes connecting or forming this link as malicious or misbehaving nodes. So to detect exact intruder I here proposes an Improved EAACK Scheme.

Keywords: Ad hoc network, EAACK, IDS, Improved EAACK, Mobile Ad Hoc Network.

I. INTRODUCTION

Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances.

II. BACKGROUND

MANETs are an appealing technology for many applications such as rescue and tactical operations due to the flexibility provided by their infrastructure. However, this flexibility comes at a price and introduces new security threats. In MANET, routing protocol assumes that every node in network cooperates with each other and there is no malicious node present in the network. Attackers can easily attack the network and can easily insert malicious nodes or non-co-operative nodes into the network. Due to distributed architecture of MANET, it is difficult to centralize a monitoring technique for MANET. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper I aim to present a new efficient intrusion detection technique for MANET. The present IDS are:

1. Watchdog
2. TWOACK Scheme
3. AACK Scheme
4. EAACK Scheme
A. Watchdog

The watchdog’s work is to detect misbehaving nodes by listening to nodes in promiscuous mode. When a node forwards a packet, the watchdog mechanism of that node monitors the next node to confirm that it also forwards the packet properly. It keeps sent packets in a buffer. When the packets are actually forwarded by next nodes, they are removed from the buffer. If the packets remain in the buffer longer than some timeout period, the watchdog increments the failure count of the node implicated. When the failure count of a node exceeds a threshold, the node is identified as a misbehaving node and a notification is sent to the source node.[1]

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

1. Ambiguous collision:
This prevents one node from overhearing packet transfer from other nodes.

2. Receiver collision:
In the receiver collision problem, a node can only tell whether neighboring node sends the packet to its neighbour which is 2 hop away from the initial node, but it cannot tell if node which is 2 hop away receives it.

3. Limited transmission power:
A node could limit its transmission power, such that the signal can be overheard by the previous node and not by the true recipient. For this purpose the misbehaving node keeps track of the transmission power required to reach each of its neighboring nodes.

4. False misbehaviour report:
In this case, a malicious node falsely claims that some nodes in the path are acting maliciously.

5. Collusion:
Multiple nodes in collusion can mount a more sophisticated attack.

6. Partial dropping:
Here a misbehaving node may drop packet at very lower rate.

B. TWOACK Scheme

It is an improvement in End-to-End acknowledgement scheme called TWOACK. The TWOACK scheme detects malicious links not nodes. Such a proactive detection approach results in quicker detection and identification of misbehaving links. TWOACK uses acknowledgement technique. In this method, group of three consecutive nodes are formed such that every third node acknowledges to first node once it has received packet.

Although TWOACK solves receiver collision and limited transmission power problems posed by Watchdog, it has a lot of network overhead due to Acknowledgement process for every packet in transmission.[2],[3]

C. AACK scheme

Acknowledgement (AACK) uses both traditional acknowledgement scheme and the TWOACK scheme. Like traditional ACK scheme once destination successfully receives packet, it sends back an ACK packet to source. But if source does not get any ACK within predefined time, it
switches to TACK mode (same as TWOACK). This combination highly reduces the network overhead. And if one of first node does not receive TACK from third node, it will report source about this node as misbehaving node. But it still has a problem of false misbehavior report and forged ACK packets.[4] But it still has a problem of false misbehavior report and forged ACK packets.

D. EAACK

EAACK is designed to overcome three of the six weaknesses of Watchdog approach, as, receiver collision, limited transmission power (which are already resolved in the above schemes), and false misbehavior report. **EAACK consists of three major parts**, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

a.) ACK: ACK is basically an end-to-end acknowledgment scheme. In this, first node has to send Packet to second node, and that second node has to give back acknowledgment to the first node. If within time period the second node doesn’t send back acknowledgment then again that Packet is being send.

b.) Secure ACK (S-ACK): In S-ACK 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. In EAACK there is a mode named MRA, which first confirm whether the node is misbehaving or not, and then takes the decision of declaring it malicious.

c.) MRA: When the source node gets the report of false misbehavior, at that time the source node sends the report to MRA mode. Then in the MRA mode, another route is assigned through its local base knowledge and the same packet is sent again to the destination, but through different route. When the packet reaches destination, MRA checks whether the packet is reached its destination or not through its local knowledge base. If destination has already received the same packet before, then MRA concludes that it is a false report and whichever node generated this report is marked malicious. But if, the packet has reached its destination for the first time then the misbehavior report is trusted and accepted. Due to this scheme that EAACK has designed, it is capable of detecting malicious node.[5]

III. PROPOSED SCHEME

EAACK scheme successfully detects malicious link in the network. But it may possible that non-malicious nodes are also marked as malicious nodes. Those falsely declared malicious nodes might help in making further routing decisions. So the appropriate malicious node needs to be detected and isolated from the network.

In EAACK the Misbehaving Report Authentication (MRA) mode is to verify the authenticity of the report generated by any node. But it is not useful to isolate the exact intruder. It can only detect whether the misbehavior report generator is a trusted node or not. The S-ACK mode in EAACK detects the malicious link in the network not the malicious node. The MRA does not overcome this limitation successfully.

To detect the exact intruder the **Improved EAACK Scheme** is developed. In the improved EAACK scheme in addition to ACK and TWO-ACK(S-ACK) modes we have an additional mode named Special mode. In this mode, as source has received NACK from a trusted node, so up to that node the path is safe. And now we know that the misbehaving node is one of the nodes who are within two hop range of last trusted node. So to identify that, Source asks the neighboring nodes of
these two nodes to send a message to those two particular nodes. The node who responds to all of these messages is considered as the trusted one. And the other is considered as the intruder and is added to the blacklist. Then we generate another route for the packet excluding this intruder node.

IV. COMPARISON

Table 1: Comparison of techniques

<table>
<thead>
<tr>
<th>Watchdog</th>
<th>TWOACK</th>
<th>AACK</th>
<th>EAACK</th>
<th>Improved EAACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issues:</td>
<td>• Receiver collision. • Limited transmission power. • False misbehaviour report.</td>
<td>• Receiver collision and Limited transmission power are solved. • False misbehaviour report problem still exist.</td>
<td>• Reduce the overhead of TWOACK Scheme. • False misbehaviour report problem solved using MRA mode.</td>
<td>• Enhancement of EAACK. • Detect the exact intruder.</td>
</tr>
</tbody>
</table>

V. DIGITAL SIGNATURE

The security in MANETs is defined as combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation VI. Digital signature is a widely adopted approach to ensure the authentication, integrity and non-repudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analogue of a written signature VII.

Digital signature schemes can be mainly divided into the following two categories:

• Digital Signature with Appendix: The original message is required in the signature verification algorithm. Examples include Digital Signature Algorithm (DSA) VII.
• Digital Signature with Message Recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA VIII.

![Communication with Digital Signature](image)

**Fig 1: Communication with Digital Signature**

The EAACK uses DSA and RSA Algorithm to digitally sign the data and acknowledgement packets in order to make it secure and reliable. In digital signatures the Elliptic Curve Cryptography (ECC) based algorithms are more effective algorithm than DSA and RSA algorithms. So In
Improved EAACK, we are suggesting ECDSA. In cryptography, the Elliptic Curve Digital Signature Algorithm offers a variant of Digital Signature Algorithm (DSA) which uses elliptic curve cryptography (ecc). As with elliptic curve cryptography in general, the bit size of public key believed to be needed for ECDSA is about twice the size of the security level, in bits. The size of an ECDSA public key would be 160 bits, whereas the size of a DSA public key is at least 1024 bits. On the other hand, the signature size is the same for both DSA and ECDSA.[9]

Both ECDSA signatures and public keys are much smaller than RSA signatures and public keys of similar security level. But the signature verification process of ECDSA is slightly slower than RSA (for reasonable security levels). That is the one place that RSA shines. But ECDSA is excelled with its running time in both key generation and signing. [10].

Table 2: Performance comparison

<table>
<thead>
<tr>
<th></th>
<th>DSA</th>
<th>RSA</th>
<th>ECDSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key length is small.</td>
<td>Key length is large.</td>
<td>Key length is smaller than DSA and RSA.</td>
<td></td>
</tr>
<tr>
<td>Less secure.</td>
<td>More secure</td>
<td>Secure than DSA and same as RSA.</td>
<td></td>
</tr>
<tr>
<td>Execution time is less.</td>
<td>Execution time is large.</td>
<td>Execution time is lesser than RSA and DSA.</td>
<td></td>
</tr>
</tbody>
</table>

![Node Overhead of MANET](image)

Fig 2: performance of DSA, RSA, ECDSA

VI. CONCLUSION

MANETs are a new technology increasingly used in many applications. These networks are more vulnerable to attacks than wired networks. Since they have different characteristics, conventional security techniques are not directly applicable to them. Many MANET IDSs have been proposed, with different intrusion detection techniques, architectures, and response mechanisms.
Proposed systems generally emphasize few MANET issues. MANETs have most of the problems of wired networks and many more besides. As a consequence intrusion detection for MANETs remains a complex and challenging topic for security researchers.

REFERENCES


IX. en.m.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

X. crypto.stackexchange.com/questions/3216/signatures-rsa-compared-to-ecdsa.

XI. Ashish Patil, Nilesh Marathe, Puja Padiya. “Improved EAACK scheme for detection and isolation of a malicious node in MANET”.

@IJRTER-2017, All Rights Reserved 84