Secure Intrusion Detection Techniques for MANET using Improved EAACK

Pooja P. Mokadam¹
M. Tech Student, CSE
VIT College of Engineering, Nagpur, India

Pravin G. Kulurkar²
Professor & Head, CSE,
VIT College of Engineering, Nagpur, India

Abstract: The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they depend on their neighbours to relay messages. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. From the invention of wireless networks, it is preferred due to their natural mobility and scalability. Major advantages of wireless networks are its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. 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. Minimal configuration and quick deployment make MANET ready to be used in unexpected situations where an infrastructure is unavailable or impossible to initiate in scenarios like natural or human-induced disasters, military conflicts. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network.

II. BACKGROUND

IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. So it is vital to address its security issues. Such existing IDSs in MANETs are 1) Watchdog 2) TWOACK and 3) AACK.

1. Watchdog

Watchdog enhances the rate of production of the network even in the presence of attackers. It has two parts namely Watchdog and Pathrater. It detects malicious nodes by overhearing next hop’s transmission. A failure counter is initiated if the
next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehaviour report 5) partial dropping 6) collusion.

2. **TWOACK**

TWOACK checks the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. It is required to works on routing protocols such as Dynamic Source Routing (DSR). The major drawbacks are 1) Increased overhead 2) Limited battery power 3) Degrades the life span of entire network.

3. **AACK**

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks is that it suffers from 1) False misbehaviour report 2) Forged acknowledgment packets.

III. LITERATURE REVIEW

N. Kang, E. Shakshuki and T. Sheltami offered a scheme called Enhanced Adaptive ACKnowledgement (EAACK). This scheme aims to conquer four of the weaknesses in traditional Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and false misbehaviour. But there is no authentication for acknowledgements. The functions of detection scheme largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. So this scheme is not much efficient. Although the simulation result showed that the proposed scheme outputs higher packet delivery ratio, it also has a higher overhead ratio with the increase of malicious nodes in the network. This is due to the introduction of MRA scheme. Elhadi M. Shakshuki proposed EAACK which was designed with the implementation of RSA and DSA digital signatures using DSR routing protocol. Performance evaluation was done and results were obtained. But this EAACK has no provision for handling link breakage and malicious source node scenario. Later the introduction of digital signature to prevent the attacker from forging acknowledgment packets was proposed. It used a new protocol for better security using hybrid cryptographic technique to reduce the overhead caused by digital signature.

IV. **EAACK**

In the existing approach, EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehaviour, limited transmission power and Receiver collision. EAACK consists of three major parts, ACK, Secure ACK (SACK) and misbehaviour report authentication (MRA).

1. **ACK**

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected.

2. **S-ACK**

The S-ACK scheme is an improved version of the TWOACK scheme. 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 intention of inaugurating S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

3. **MRA**
The MRA scheme is outlined to rectify the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The significance of MRA scheme is to confirm whether the destination node has received the reported missing packet through a different route.

4. **Digital Signature**

EAACK is an acknowledgment-based IDs. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviours in the network. Thus, it is extremely crucial 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, digital signature scheme has been incorporated into EAACK. We, analyzed the performance of existing EAACK in various scenarios and found that it gave poor performance during

A: **Link breakage, occurs due to**
- Continuously changing, network topology
- High mobility of nodes, Factors like traffic and delay
- Nodes move beyond transmission range
- Insufficient energy levels

B: **Malicious source node, resulting in**
- Packet drop, Drained battery
- Buffer overflow, Message tampering
- Fake routing, Stealing information.

C. **Partial packet dropping**

D. **Resulting in Increased routing overhead, delay**

E. **Reduced packet delivery ratio.**

V. **SIMULATION WORK**

A. **Simulation Configuration**

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250CPU and 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS-2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670×670 m. The language we are using are TCL and AWK script. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B.

In order to measure and compare the performance of our proposed scheme, we adopt the following performance metrics:

1) **Packet Delivery Ratio:** Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.
2) Delay: Network delay is an important design and performance characteristic. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another.

3) Routing Overhead: Routing overhead refers to the ratio of routing related transmissions.

VI. PROBLEM IDENTIFICATION

A. Simulation Environment

Based on the simulation parameters defined, the mobile ad hoc network is designed as in fig. The existing EAACK algorithm is implemented in this environment and its performance is analyzed.

From fig. 1 there are 50 nodes, of which the source node is node 8 and the destination node is node 20. The data is being transferred from source 8 to destination 20 via the route 8-11-10-20. Based on the behaviour of algorithm, graphs are generated for the performance metrics routing overhead, delay, packet delivery ratio, packet loss ratio.

B. Results

The graph results obtained after the execution of existing EAACK algorithm for various performance metrics are as follows. Fig. 2, 3 and 4 shows how the performance of EAACK degrades performance.
The graphs depict that the routing overhead and delay increases while packet delivery ratio reduces in cases of link breakage, source maliciousness and partial packet dropping. These graph results clearly show the inefficiency and unreliable nature of EAACK algorithm, the network performance degrades as it tries to tackle the network attacks. In this project, we aim to improve the security of network against intrusion detection by modifying the existing EAACK algorithm to withstand various attacks from malicious nodes. This will enhance the network reliability.

VII. PROPOSED SCHEME DESCRIPTION

1. Simple network with transmission

2. Mobile nodes and Data transmission

While sensing nodes with individual network, source node started transmission of data to destination node through intermediate node.
3. Acknowledgement process

Destination sends acknowledgement message (ACK) to source for confirmation of data delivery. Secure ACK (S-ACK) process started when source does not receives ACK message.

4. Detection and Prevention of malicious nodes

S-ACK begins for three consecutive nodes for malicious node detection. Means third intermediate node 4 sends acknowledgement packet to node 3, but node 3 does not send ACK packet to node 5. Hence intermediate node 2 sends misbehaviour report to source node.

ADVANTAGES

Thus, the improved EAACK works successfully in

1. Detecting malicious nodes during link breakage, source maliciousness.
2. Identifies partial packet dropping.
3. Identifies forged acknowledgments and false misbehaviour report.

VIII. PERFORMANCE EVALUATION

RESULTS
Thus, based on the individual graphs obtained we have generated a comparison graph for the purpose of evaluating the performance of existing EAACK with our proposed EAACK algorithm as shown in fig.2,11 and 12.

![Fig.11: Main Delay](image1)

![Fig.12: Main PDR](image2)

Above graph shows the network performance of improved EAACK which is marked in Red line in comparison with previous work. The comparison graph results clearly infer how well the performance of network has been enhanced by our improved EAACK scheme.

**IX. CONCLUSION AND FUTURE WORK**

Intrusion detection has caused a major threat in MANETs for many years. In our project we have taken efforts to reduce various network attack issues like partial packet dropping, forged acknowledgments, false misbehaviour reports, receiver collision, and limited transmission. Also, the SHA+AES algorithm handles situations of link breakage and source maliciousness. Apart from detecting malicious nodes in MANETs, the improved EAACK also takes care of network performance as the performance metrics routing overhead and delay are reduced while packet delivery ratio is increased. We hope these results will be of some use in future study in this area helping the growing interest and resulting in the invention of new IDSs.

**References**

Pooja P. Mokadam, received the B.E. degree in Information Technology from Smt.Radhikatai Pandav College of Engineering, Nagpur and M.Tech degrees in Computer Science & Engineering from Vidarbha Institute of Technology in 2013 and 2015, respectively.