International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

EAACK-An Innovative Intrusion Detection System for MANET using Digital Signature

Prof. G. M.Bhandari[1], Swati Pawar[2], Varsha Zaware[3], Ujjawala Bankar[4]

[1, 2, 3, 4]University of Pune, BSIOTR Wagholi, Pune, Maharashtra, India

Abstract: ***In the past few decades the migration to wireless network from wired network has been a global trend. The functionality and features of MANET and the wireless medium also distribution of nodes makes MANET vulnerable to malicious attackers. A new improved technique EAACK (Enhanced Adaptive Acknowledgement) method designed for MANET was proposed for IDS. Here in this scheme we are using Digital Signature for providing more security. EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.***

Keywords: Digital signature algorithm, Enhanced Adaptive Acknowledgement, Mobile Adhoc Network.

1. Introduction

MANET is a wireless network which consists of mobile nodes that form a temporary network without the fixed infrastructure or Central administration. Mobile nodes can communicates directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via 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 functioning of the network proper 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 occurs 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 become 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 in emergency operation like flood, earth quake, etc. 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, Impersonation, Eavesdropping Routing attacks, and Black hole attack, Gray-hole Attack, Man- in- the- middle Attack, Jamming, Replay Attack, and Wormhole Attack.

a) Denial of Service Attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery Exhaustion method.
b) Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.
c) Eavesdropping: This is a passive attack. The node simply observes the confidential information. This Information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.
d) Routing Attacks: The malicious node make routing services a target because it is an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node.
e) Black-hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets.
f) Gray-hole Attack: This attack is also known as routing misbehavior attack which leads to dropping of Messages. Grayhole attack has two phases. In the first phase the node advertise itself as having a valid route to Destination while

in second phase, nodes drops intercepted packets with a certain probability.

g) Man- in- the- middle Attack: Here in this attack data integrity is lost. An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver.

h) Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered and receiver will not get the desired data as network is congested with unwanted packets.

i) Replay Attack: An attacker that performs a replay attack is retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

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

2. Background

2.1 Intrusion Detection in MANETs

In traditional wired networks many Intrusion Detection Systems has been proposed, where all traffic must go through hub, switches, routers, or gateways. Hence, Intrusion Detection Systems can be added to and implemented in these devices easily. On the other hand, Mobile Adhoc Networks do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current Intrusion Detection Systems techniques on wired networks cannot be applied directly to Mobile Adhoc Networks. Many Intrusion Detection Systems have been proposed to suit the characteristics of MANETs.

2.2 Watchdog

The main of the watchdog mechanism is to improve the throughput of the network with the presence of malicious nodes. The watchdog scheme is of two types namely watchdog and pathrater. Watchdog serves as intrusion detection for Mobile Adhoc Network and responsible for detecting malicious node misbehavior in the network. Watchdog detects malicious node misbehaviors by listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a predefined time period, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. At the same time, watchdog maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog scheme accuses the next-hop neighbor to be misbehaving.

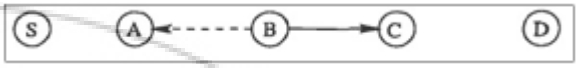

Figure 1: Working mechanism of watchdog

When B forwards a packet from S toward D through C, Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. A can overhear B's transmission and can verify that B has attempted to pass the packet to C. The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. 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.

3. Problem Statement

Enhanced Adaptive Acknowledgement (EAACK) is designed to tackle two of the six weaknesses of Watchdog scheme, namely, false misbehavior and receiver collision.

3.1 Receiver collisions

Node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to Node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at Node C

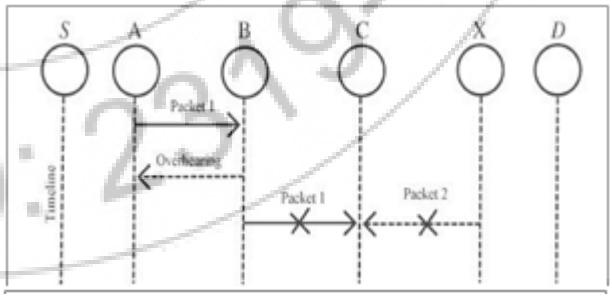

Figure 2: Receiver Collision

3.2 False Misbehavior Report

Node A successfully overheard that node B forwarded Packet 1 to node C, node a still reported node B as misbehaving. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture

and Compromise one or two nodes to achieve this false misbehavior report attack.

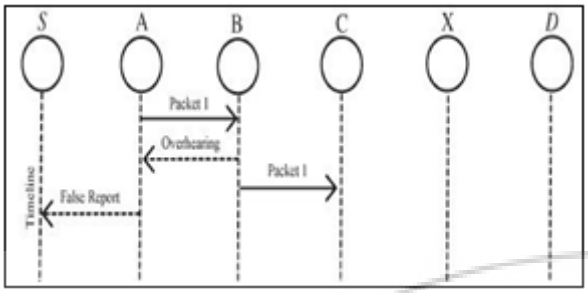

Figure 3: False Misbehavior Report

4. Scheme Description

EAACK is consisted of two major parts, namely, secure ACK (S-ACK), and misbehavior report authentication (MRA). Introduction of digital signature in the EAACK to prevent the attacker from forging acknowledgment packets.

4.1 S-ACK

S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node the intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision.

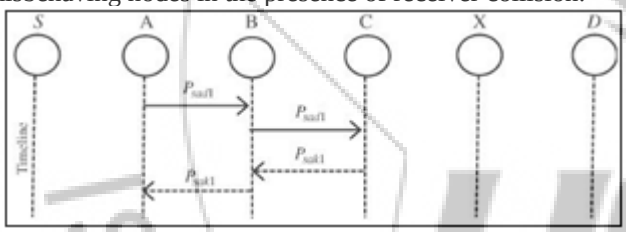

Figure 4: Secure Acknowledgement

4.2 MRA

The Misbehavior Report Authentication (MRA). Scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route by adopting an alternative route to the destination node, the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted

4.3 Digital Signature

EAACK is an acknowledgment-based IDS. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

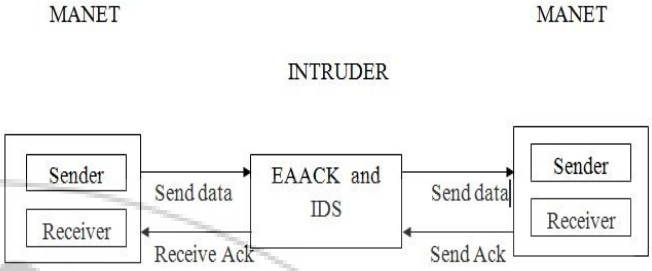

Figure 5: System Architecture

5. Performance Evaluation

A. Simulation Methodologies

The performance of EAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

- Scenario 1: In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against weaknesses of Watchdog, namely, receiver collision.
- Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.
- Scenario 3: This scenario is used to test the IDSs' performances when the attackers are smart enough to forge acknowledgment packets and claiming positive result while, in fact, it is negative. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

B. Simulation Configuration

Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

$$PDR = \frac{\sum Received\ packets\ at\ destinations}{\sum Sent\ packets\ by\ sources}$$

All acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network.

Figure 6: Graph Representing Variations of PDR

Throughput: The average rate of successful message is delivery over a communication channel.
All malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report.

Figure 7: Graph Representing Variations of Throughput

6. Conclusion

Packet-dropping attack has always been a major threat to the security in MANETs. In the new technique the Intrusion Detection Systems named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms such as Watchdog scheme in different scenarios through simulations. The results demonstrated positive performances against Watchdog in the cases of receiver collision and false misbehavior report.

References

[1] Aishwarya Sagar and Meenu Chawla. (July 2010) " Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET " IJCSI International Journal of Computer Science Issues, Vol.7, Issue 4, No 1.

[2] Anand Patwardhan A., Parker J., Joshi. and Iorga M. (2005) "Secure routing and Intrusion Detection in Adhoc networks" in Proc. 3rd Int. Conf. Pervasive Comput. Commun.,pp. 191–199.

[3] David Johnson and Maltz D. (1996) "Dynamic Source Routing in Adhoc wireless networks" in Mobile Computing. Norwell, MA: Kluwer, ch. 5,pp. 153–181

[4] Kalman Graffi.,Mogre.,Matthias Hollick and Ralf Steinmetz. (Nov 2007) "Detection of Colluding Misbehaving Nodes in Mobile Adhoc and Wireless Mesh Networks" In: IEEE Global Communications Conference (IEEE GLOBECOM).

[5] Kejun Liu.,Deng J. and Varshney P. (May 2007) " An acknowledgment-based approach for the Detection of routing misbehaviour in MANETs" IEEE Trans. Mobile Comput., vol. 6, no. 5.

[6] Nidal Nasser and Chen Y. (Jun 2007) "Enhanced Intrusion Detection Systems for discovering malicious nodes in mobile Adhoc network" in Proc. IEEE Int.Conf. Commun., Glasgow, Scotland.

[7] Rajaram A. and Gopinath S. (Dec 2010) "Efficient Misbehavior Detection System for MANET".

[8] Rajyalakshmi G. And Anusha K.(July 2013) "Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System".

[9] Rivest R., Shamir A. and Adleman L. (Feb 1983) " A method for obtaining digital signatures and public-key cryptosystems ", Commun. ACM, vol. 21, no.2,pp. 120–126.

[10] Shakshuki M., Nan Kang. and Sheltami R. (March 2013) " EAACK- A Secure Intrusion-Detection System for MANETs " IEEE Transactions on Industrial Electronics, vol. 60, no. 3.

[11] Sohail Abbas., Madjid Merabti. and David Llewellyn-Jones. (2010) "A Survey of Reputation Based Schemes for MANET" ISBN: 978-1- 902560-24-3.

[12] Sujatha S. and Lakshmi B. (2010) "A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme In Receiver Collisions – An IDS In Wireless Mobile Ad-Hoc Networks" ||Volume||2 ||Issue|| 9 ||Pages|| 32-40||c||.

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

[14] Tarag Fahad. and Robert Askwith. (2006) "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks".