ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

EAACK-A Secure Intrusion Detection System for MANET

[1]K.Chinthanai chelvan, [2] T.Sangeetha, [3] V.Prabakaran, [4] D.Saravanan

[1, 2, 3]PG scholar, Dept. of Computer Science and Engineering, Pavendar Bharathidasan college of Engineering and Technology, Tiruchirapalli, Tamilnadu, India

[4]Associate Professor, Dept. of Computer Science and Engineering, Pavendar Bharathidasan college of Engineering and Technology, Tiruchirapalli, Tamilnadu, India

ABSTRACT: The migration to wireless network from wired network has been a global trend in the past few decades. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. A new technique EAACK (Enhanced Adaptive Acknowledgement) method designed for MANET was proposed for intrusion detection. EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

KEYWORDS: Digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgement (EAACK), Mobile Adhoc NETwork (MANET).

I. INTRODUCTION

MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Nodes can communicates 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 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 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, Impersonation, Eavesdropping Routing attacks, and Black hole attack, Gray-hole Attack, Man- in- the- middle Attack, Jamming, Replay Attack, and Wormhole Attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

(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. Gray whole 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*: 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.
(i) *Replay Attack*: An attacker that performs a replay attack are 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*: 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.

II.BACKGROUND

A. Intrusion Detection in MANET

Many Intrusion Detection Systems has been proposed in traditional wired networks, where all traffic must go through 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.

B. 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 serve as intrusion detection for Mobile Adhoc Network and responsible for detecting malicious node misbehavior in the network.

Watchdog detects malicious node misbehaviors by promiscuously 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

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.

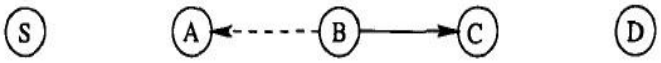

Figure 1: Working mechanism of watchdog

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 path rater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections.The routing information can be passed with the message. The 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.

C. AACK

A new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme Which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

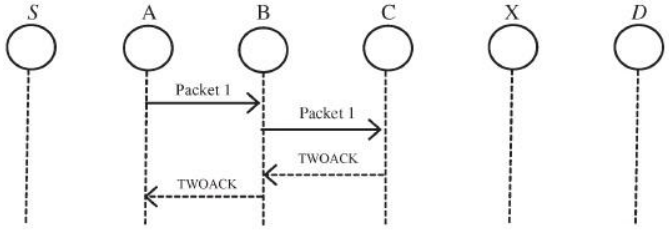

Figure 2: Two ACKnowledgement

III.PROBLEM DEFINITION

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

A. 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.

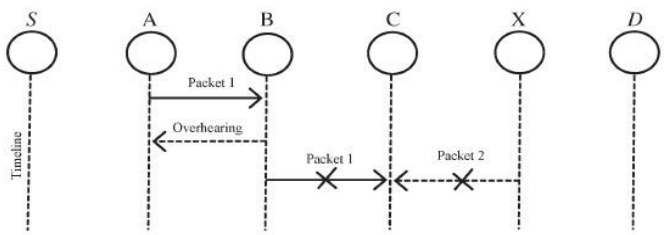

Figure 3: Receiver Collision

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

B. 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.

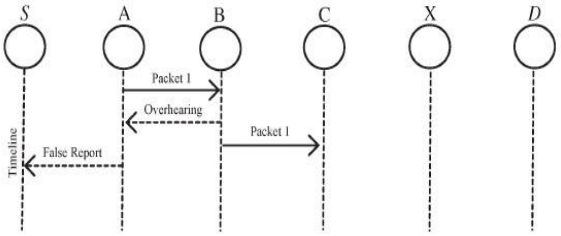

Figure 4: False Misbehavior Report

IV.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.

A. ACK

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in RRACK, aiming to reduce network overhead when no network misbehavior is detected. If ACK scheme fails the node will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

B. 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.

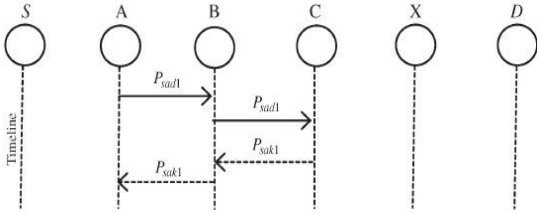

Figure 5: Secure ACKnowledgement

C. 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 re-port and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

D. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

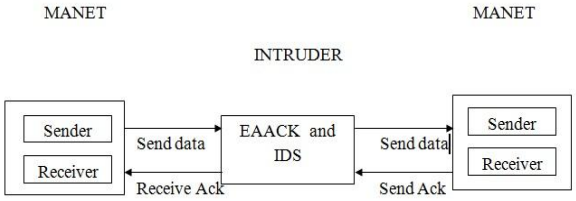

Figure 6: System Architecture

V.PERFORMANCE EVALUATION

A. Simulation Configuration

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

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

Throughput (Tp): It is defined as the average rate of successfully received message is delivery over a communication channel.

All malicious mobile nodes to send out false misbehavior report to the source node whenever it is possible. This type of scenario setting is designed to test the IDS's performance under the false misbehavior report.

Average End to End Delay (AED): The average end-to-end delay for all successfully received packets at the destination. It is calculated for each data packet b subtracting the sending time of the packet from the received time at final destination. Then the average represents the AED.

$$AED = \frac{\sum_1^N (T_{Rceived} - T_{Sent})}{N}$$

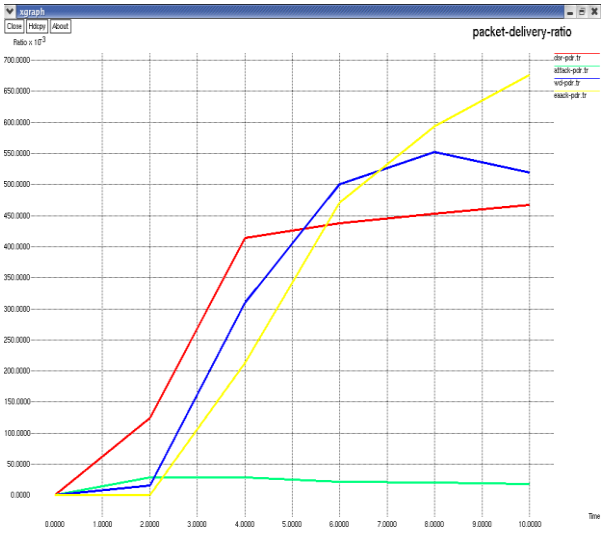

Figure 7: PDR Graph

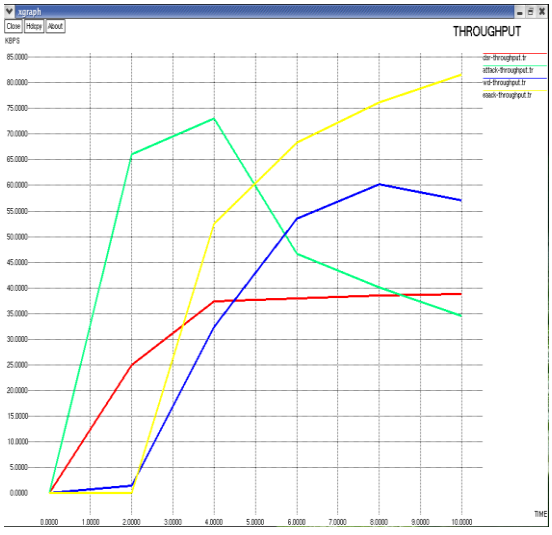

Figure 8: Throughput Graph

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

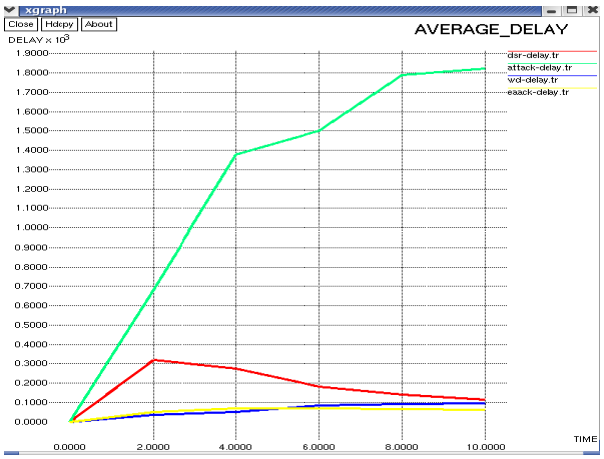

Figure 9: Delay Graph

VI.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, "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, July 2010.

[2] Anand Patwardhan and Iorga, "Secure routing and Intrusion Detection in Adhoc networks," in Proc. 3rd Int. Conf.Pervasive Comput. Commun. Pp. 191–199, 2005.

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

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

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

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

[7] Rajaram and Gopinath, "Efficient Misbehavior Detection System for MANET," Dec 2010.

[8] Rajyalakshmi and Anusha, "Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System, "July 2013.

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

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

BIOGRAPHY

Mr. CHINTHANAI CHELVAN K received the BE degree in Computer Science from Angalamman College of Engineering and Technology; Trichirappalli in 2011.He is currently doing his ME in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli.

Ms. SANGEETHA T received the BE degree in Computer Science from New Prince Shri Bhavani College of Engineering and Technology; Chennai in 2012.She is currently doing her ME in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli.

Mr. PRABAKARAN V received the BE degree in Computer Science from St. Joseph's College of Engineering and Technology; Thanjavur in 2012.He is currently doing his ME in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli.

Mr. SARAVANAN D received the B.E degree in Electrical and Electronics Engineering from Maharaja Engineering College, Tiruppur in 2000 and received the M.E degree in Computer Science and Engineering from Annamalai University, Chidambaram in 2005. He is currently doing the Ph.D. in the area of MANET and also working as an Associate Professor in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli with 11 years of teaching experience and his area of interest include MANET.