ERACK-A New Intrusion Detection System For MANET

Chinthanai Chelvan.K, Herman Jeeva.S, Prasanna.P, Saravanan.D

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 ERACK (Enhanced Robustive Acknowledgement) method designed for MANET was proposed for intrusion detection system for MANET by providing secure Acknowledgement packets. Enhanced Robustive Acknowledgement demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.**

Index Terms — **ERACK (Enhanced Robustive ACKnowledgement), DSA (Digital Signature), S-ACK (Secure ACKnowledgement), MANET (Mobile Adhoc NETwork)**

I. Introduction

This MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Mobile nodes can communicates directly to other mobile nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multi hop scenario. In multi-hop transmission, a packet is forwarded from one node to another, if not it reaches the destination with the help of using routing protocol. 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 of nodes may occur which can severely degrades the performance of network.

Vulnerability is a weakness in security system. A particular mobile system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired mobile network. Some of the vulnerabilities are as follows:-

(a) Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among mobile nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior of mobile node could be better protected with distributed and adaptive security mechanisms.

(b) Bandwidth constraint: Variable lower capacity links exists as compared to wireless mobile network which are more susceptible to external noise, interference and signal attenuation effects.

(c) Limited power supply: The nodes in network need to consider restricted power supply, which will cause several problems. A node may behave in a selfish manner when it is finding that there is only limited power supply.

Routing protocols are generally necessary for maintaining effective communication between distinct mobile nodes. Routing protocol in the mobile Adhoc network not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes in the mobile network. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Routing protocols can be classified into proactive protocol, reactive protocol and hybrids protocol.

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 applications like military conflict and medical application. 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 certain medical emergency situations.

Securing wireless Adhoc network is highly challenging issue. The attacks can be classified in to Denial of Service(DOS)Attack,,EavesdroppingRoutingattacks(EDRA) .

(a) Denial of Service Attack: This attack aims to attack the availability of a node or the entire nodes in the network. If the attack is successful the services will not be available. The attacker node generally uses radio signal jamming and the battery exhaustion method.

(b) Eavesdropping: This is a passive attack. The mobile node simply observes the confidential information. The node information can be later used by the malicious mobile node. The secret information like public key, location, password, private key, etc. can be fetched by eavesdropper.

(c) Routing Attacks: The malicious node make routing services a target because it is an important service in Mobile Adhoc Network. There are two flavors for this routing attack. One of the attack on routing protocol and another is attack on packet forwarding or delivery mechanism.

Regardless of the attractive applications, the features of Mobile Adhoc Network introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These challenges include

(a) Routing: Since the topology of the network is constantly changing, the main issue of routing packets between any pair of nodes becomes a challenging task.

Multicast routing protocol is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between mobile nodes may potentially contain multiple mobile hops, which is more complex than the single hop communication.

(b) Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

(c) Inter-networking: In addition to the communication within an ad hoc network, inter-networking between fixed networks (mainly IP based) is often expected in many cases. The coexistence of such routing protocols in such a mobile device is a challenge for the harmonious mobility management.

(d) Security and Reliability: In addition to the common vulnerabilities of wireless connection, MANET has its particular security problems due to e.g. nasty neighbor relaying data packets. Further, wireless link characteristics introduce also reliability problems in Manet, because of the limited wireless transmission mobile range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), data transmission errors and mobility-induced data packet losses.

(e) Power Consumption: For most of the light-weight mobile node terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power in Manet and power-aware routing protocol must be taken into consideration.

II. BACKGROUND

A. Intrusion Detection in MANET

Many Intrusion Detection Systems has been proposed in traditional wired networks, where all traffic must go through routers, switches or gateways. Mobile Adhoc Networks (MANET) does not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it.

MANET knows how to detect the attackers as soon as they enter the network and able to completely remove the potential damages caused by compromised nodes at the first time. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. The present research mechanism has focused on designing Intrusion Detection Systems to monitor and analyze system events for detecting network resource misuse in a MANET [2][3].

B. Watchdog

The main aim 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 path rater .watchdog serve as intrusion detection (ID) for Mobile Adhoc Network and responsible for detecting malicious node misbehavior in the Mobile Adhoc network [6][10].

The watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If a packet has remained in the buffer for longer than a certain timeout, the watchdog scheme increments a failure tally for the node responsible for forwarding on the data packet. If the tally exceeds a certain threshold bandwidth, it determines that the mobile node is misbehaving and sends a message to the source notifying it of the misbehaving node.

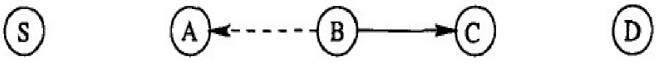

Figure 1: Working mechanism of watchdog

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

The Watchdog fails to detect malicious node misbehaviors with the presence of the following:

1) Receiver collisions; 2) Limited transmission power; 3) False misbehavior report 4) Ambiguous collisions;
5) Collusion; 6) Partial dropping.

III. PROBLEM DEFINITION

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

A. Receiver Collisions

In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it . If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives it. Thus, B could skip retransmitting the packet and leave A none the wiser. B could also purposefully cause the transmitted packet to collide at C by waiting until C is transmitting and then forwarding on the packet [1][4].

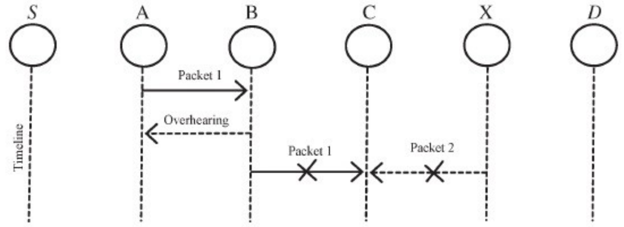

Figure 2: Receiver Collision

B. False Misbehavior Report

Node A could report that node B is not forwarding packets when in fact it is. This will cause S to mark B as misbehaving when A is the culprit. This behavior, however, will be detected. Since A is passing messages on to B (as verified by S), then any acknowledgements from D to S will go through A to S, and S will wonder why it receives replies from D when supposedly B dropped packets in the forward direction. In addition, if A drops acknowledgements to hide them from S, then node B will detect this misbehavior [5][7][8].

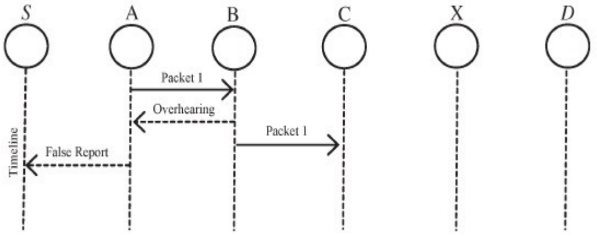

Figure 3: False Misbehavior Report

IV. SCHEME DESCRIPTION

ERACK [6][10] is consisted of three major parts, namely ACKnowledgement, secure ACK (S-ACK) and misbehavior report authentication (MRA). Introduction of digital signature in the ERACK to prevent the attacker from forging acknowledgment packets (FAP).

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 [6[8].

B. S-ACK

S-ACK [8] scheme is an improved version of TWOACK scheme. The principle is to let each and every three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive mobile nodes in the route, the third mobile 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.

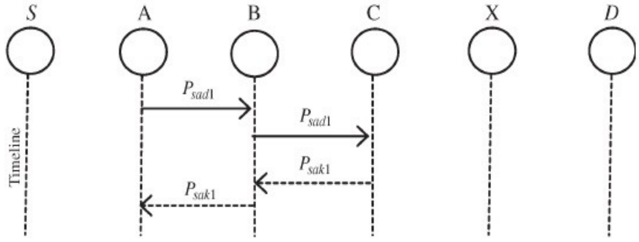

Figure 4: Secure ACKnowledgement

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 [5][7][8].

By adopting an alternative route to the destination node, the misbehavior reporter mobile node. When the destination node receives a Misbehavior Report Authentication packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received node, then it is safe to conclude this is a false misbehavior re-port and whoever generated this report is marked as malicious node. Otherwise, the misbehavior report is trusted and accepted.

D. Digital Signature

RRACK is an acknowledgment-based Intrusion Detection Systems. They all rely on acknowledgment packets to detect misbehaviors in the mobile network. Thus, it is extremely important to ensure that all acknowledgment packets in RRACK are authentic and untainted. To ensure the integrity of the Intrusion Detection Systems, RRACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted [9].

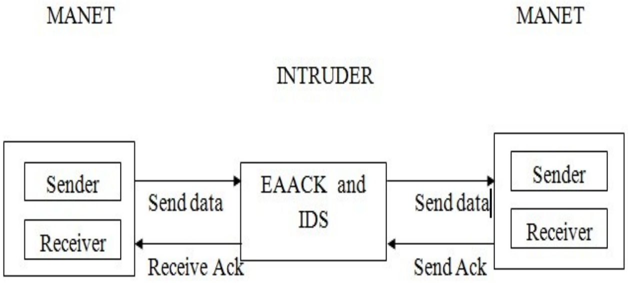

Figure 5: System Architecture

V. PERFORMANCE EVALUATION

A. Simulation Environment

The network simulator (ns-2) helps us to evaluate the communication aspects of our method, such as route discovery and average route load in adhoc wireless network. Simulation with the following parameters has been done to study the effects of the node selfishness, monitoring technique and proposed approach on the performance of MANETs.

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.

B. Simulation Results

In this section we analyze the results obtained from simulation experiments carried out in ns-2 to study the impact of selfish nodes on the network and to evaluate the network with different approaches under different conditions.

Figure shows the comparison of network performance in terms of network throughput when we use different mobility of the mobile nodes in the presence of selfish nodes. Initially nodes are uniformly distributed and node mobility are emulated according to the random way point model. We run simulations with the assumption of selfish nodes as 0, 10, 20, and 30 with pause time to 10ms with random source and destination pairs through the simulations. And also compares the packet delivery ratio of the original DSR scheme,Watchdog scheme and the proposed ERACK scheme.

The percentage of selfish nodes in the network varied from 0 to 40%. The packet delivery ratio decreases as more as nodes in the network are selfish. This is due to the problem of missing routes and the overhead of searching for alternative routes. When compared with the original DSR scheme, the proposed ERACK scheme maintains a relatively high packet delivery ratio (Throughput).

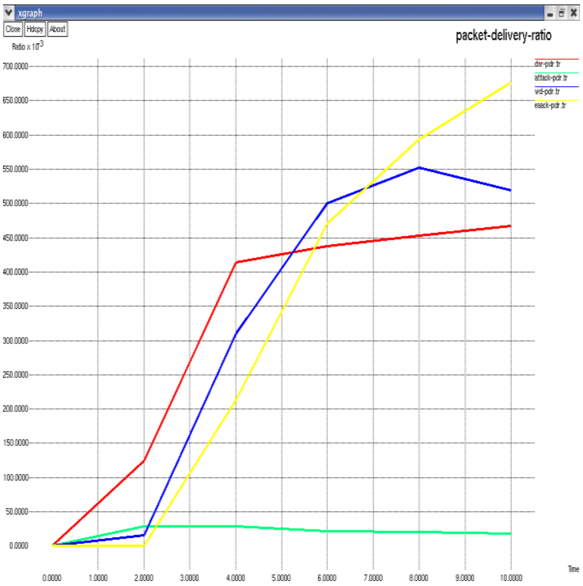

Figure 6: PDR Graph

Comparing the throughput of the DSR ,Watchdog and ERACK schemes for different percentages of selfish nodes. It can be observed that the throughput of the ERACK is relatively higher than the Watchdog scheme and the original DSR scheme. This is due to the increase of data traffic being delivered successfully in the ERACK scheme.

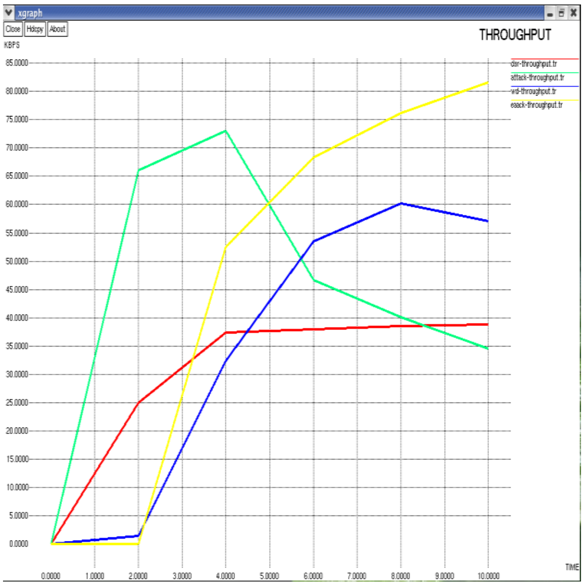

Figure 7: Throughput Graph

Comparing the energy of the DSR ,Watchdog and ERACK schemes for different percentages of selfish nodes. It can be observed that the energr of the ERACK is relatively higher than the Watchdog scheme and the original DSR scheme. This is due to the increase of data traffic being delivered successfully in the ERACK scheme.

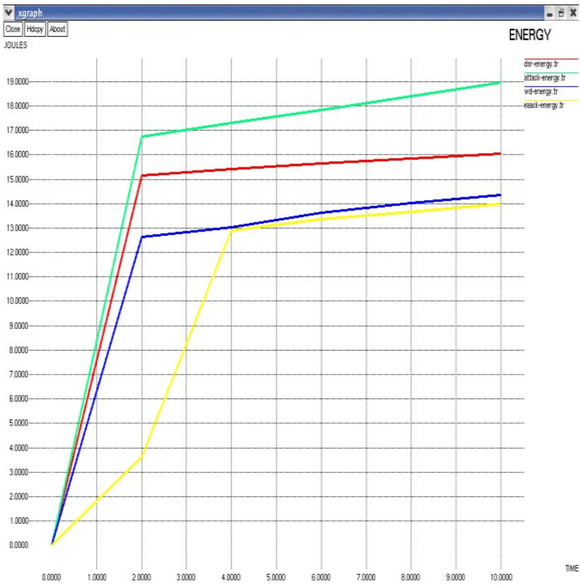

Figure 6: Energy Graph

VI. CONCLUSION

The Packet-dropping attack has always been a major threat to the security in MANETs. In the new technique the Intrusion Detection Systems named ERACK protocol specially designed for MANETs and compared it against other popular mechanisms such as Watchdog scheme in different scenarios through simulation methodology. The results demonstrated positive performances against

Watchdog in the cases of receiver collision and false misbehaviour 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-Detection System for MANETs ”, IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

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.

Mr. HERMAN JEEVA S 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. PRASANNA P received the BE degree in Information Technology from St. Kurinji College of Engineering and Technology; Trichirappalli in 2010.He is currently doing his ME in Computer Science 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.