ISSN:0975-9646

R.Vineeth et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4231-4237

A Robust Trust Aware Secure Intrusion Detection for MANETs

R.Vineeth[1], Dr. N. K. Sakthivel[2], Dr. S. Subasree[3]

[1] *PG Student, Computer Science and Engineering, Nehru College of Engineering and Research Centre.*

[2] *Vice Principal, Nehru College of Engineering and Research Centre.*

[3] *HOD/Head Computer Science and Engineering, Nehru College of Engineering and Research Centre.*

***Abstract*— Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. The characteristics of MANETs such as, dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. The migration to wireless network from wired network has been a worldwide trend within the past few decades. To amend to such trend, it is vital to strengthen its potential security issues.. In this paper, a new routing mechanism to combat the common selective packet dropping attack. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of new scheme compared with EAACK with respect to packet drop, packet delivery ratio and throughput.**

***Keywords*— MANET, Watchdog, Digital signature algorithm, Enhanced Adaptive Acknowledgment, Trust Aware Secure Intrusion Detection System.**

I. INTRODUCTION

obile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure-less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network [2], is self-organizing and adaptive. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. In other words a MANET is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed, this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. In a MANET [5], nodes within each other's wireless transmission ranges can communicate directly, however, nodes outside each other's range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Every node functions as a router. The success of communication highly depends on other nodes cooperation.

Mobile Ad-hoc network [1], require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. Pictorial representation of MANET is shown in Fig 1. They can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost. Applications such as military exercises, disaster relief, and mine site operation may benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility.

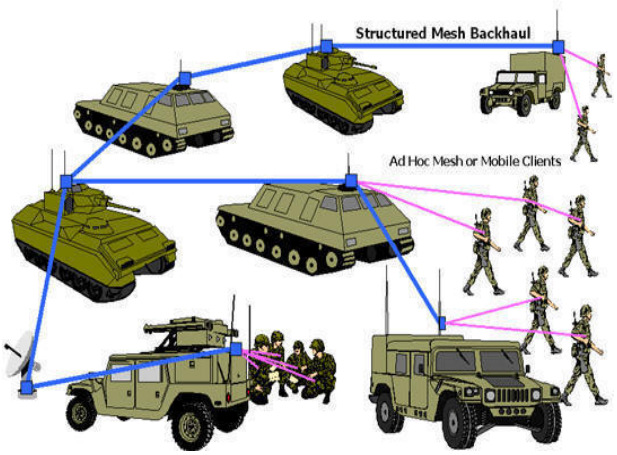


Fig.1. Example of mobile Ad-hoc network

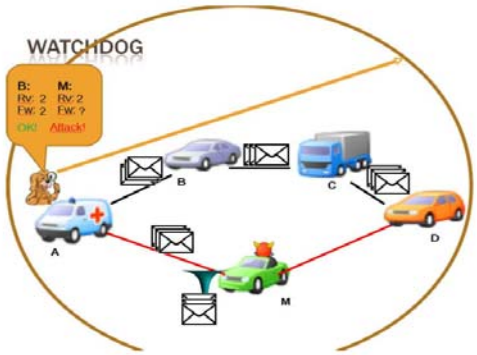
However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. Due to the limitations [6], of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. In next section, three existing approaches, namely, Watchdog, TWOACK and AACK are been discussed.

I. BACKGROUND

A. Intrusion Detection System

Intrusion detection is very important aspect of defending the cyber infrastructure from attackers or hackers. Intrusion prevention technique such as filtering router policies and firewalls fail to stop such kind of attacks. Therefore, no matter how well a system is protected, intrusion still occurs and so they should be detected. Intrusion detection systems are becoming significant part of security and the computer system. An intrusion detection system[3], is used to detect many types of malicious behaviours of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. 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 (IDS) to monitor and analyse system events for detecting network resource misuse in a MANET.

1) Watchdog Mechanism: Marti *et al.* proposed [1], Watchdog mechanism which aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely watchdog and pathrater. Watchdog serves as an intrusion detection system for MANETs. Watchdog detects malicious misbehaviours by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Watchdog is the most primitive mechanism for detecting the attacks in Mobile Ad-hoc network. Fig 2 represents the operation of watchdog mechanism.



Fi. 2 Operation of Watchdog

Node A cannot transmit all the way to node M, but it can listen to node B's traffic. Thus, when A transmits a packet for B to forward to M, A can often tell if B transmits the packet or not. The watchdog mechanism can detect misbehaving nodes at forwarding level and not at the link level. Watchdog scheme fails to detect malicious misbehaviours with the presence of

- Ambiguous collisions
- Receiver collisions
- Limited transmission power
- False misbehavior report
- Collusion
- Partial dropping

2) TWOACK: TWOACK proposed [1], by Liu *et al.* is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

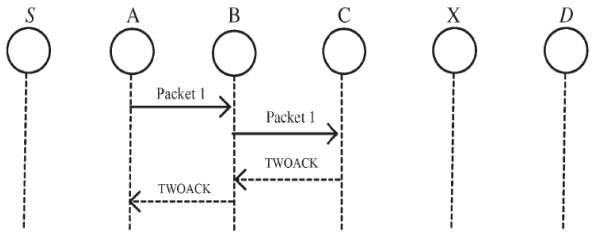


Fig. 3 TWOACK scheme.

The working process of TWOACK is demonstrated in Fig. 3 node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains the reverse route from node A to node C and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node

C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

3) AACK: Sheltami *et al.* proposed [1], a new scheme called AACK which is based on TWOACK Acknowledgement. AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme called ACK which is identical to TWOACK and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report.

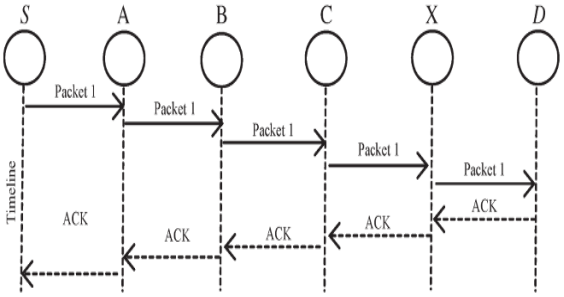


Fig. 4: AACK Scheme

In the ACK scheme, as shown in the Fig.4 the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. In this network all the intermediate nodes simply forward this packet to the next nodes. When the destination node D receives Packet 1, it is vital to send back an ACK acknowledgment packet to the source node S down in reverse order of the same route. Within a predefined time, if the source node S receives this ACK acknowledgment packet from the destination node, then the packet transmission from node S to node D is successful. Or else, the source node S will switch to TACK scheme by sending out a TACK packet. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic. To address this concern digital signature is adopted in EAACK.

II. Problem Definition

After AACK scheme, E.M. Shakshuki et al. proposed Enhanced Adaptive ACKnowledgement (EAACK) scheme, where digital signature is used to prevent the attacker from forging acknowledgement packets. EAACK is consists of three parts, namely, ACK, secure-ACK (S-ACK) and misbehaviour report authentication (MRA). 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. S-ACK 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 introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. The MRA scheme is designed to resolve 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.

A. ACK

ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S 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

It is an improved version of the TWOACK intrusion detection system. 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 introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. In S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S.

C. MRA

The Misbehaviour Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehaviour report can be generated by malicious attackers to falsely report that 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 core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent the misbehaviour 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 misbehaviour report and whoever generated this report is marked as malicious, otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

D. Digital Signature

EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviours in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regarding to this concern, digital signature is incorporated in EAACK scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.

E. Trust identification

In this module, we calculate the trust between the nodes. Where the nodes are classified as Unknown, and Known. Trust classification and calculation is made on demand based on the data transfer route request.

UNKNOWN

- Node x have never sent or received any messages to and from node y
- Trust levels between them are very low.
- Probability of malicious behavior is very high.
- Newly arrived nodes are grouped in to this category.

KNOWN

- Node x have sent or received some messages to and from node y
- Trust levels between them are neither low nor too high.
- Probability of malicious behavior is to be observed.

COMPANION

- Node x have sent or received plenty of messages to and from node y
- Trust levels between them are very high.
- Probability of malicious behavior is very less.

F. Trust aware routing

Based on the results on the previous module, trust aware routing module is made, where the problem of packet dropping is avoided by making the transmission in the trust aware routing nodes.

III. METHODOLOGIES

It is highly vital to guarantee that the data packets are valid and authenticated in the existing system. In order to ensure the integrity of the IDS, EAACK requires data packets to be encrypted before they are sent out and verified until they are accepted. EAACK uses AODV routing protocol to find the shortest path in the network to reach destination. Then it encrypts the data packet with hash key and send to the destination. The destination decrypts the data and check the hash value for data integrity. If the route has attacker nodes and if the sender does not receive acknowledgement packets then the packets will be sent in the new route. If any node wants to send packet to neighbouring node then first source node generate the packet and send to the neighbouring node. The sent packet is sent to acknowledge system. After that it send packet according to mode and detect the intruder in the system, If intruder or misbehaving node is detected then alert will be triggered by the same node that detect the misbehaving node. When a node detect malicious node it will inform the source node by sending an acknowledgement, which is a small packet that is generated by the routing protocol and extract the route from source route of corresponding data packet and the packet will be sent in a new route.

Security based on hash function has always been an integral part of cryptography. Using a simple hash algorithm, hash value from a string of plain text can be generated. The hash value will be attached to packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted, otherwise the packet is discarded. In either case, an acknowledgement packet will be sent back to sender to inform of the status of the packet.

For encryption and decryption feature CESAR cipher is implemented with a pre-shared key. These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text to three positions. Encryption and decryption of data is shown in Fig. 5..

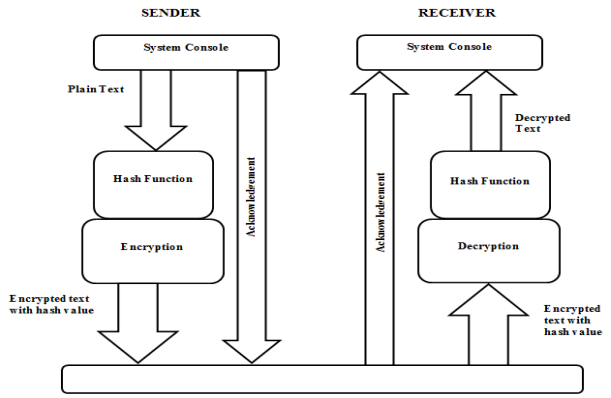


Fig.5 Logical Design of encryption and decryption system

IV. SIMULATION MODEL

Our simulation contains 30 nodes scattered on a 800X800 meter flat space for data transfer. This space makes the maximum hops to be 3. The physical layer and 802.11 MAC layer are included in the wireless extensions of NS2 Table 1.1 shows the other simulation parameters. UDP traffic with constant bit rate (CBR) is used with packet size of 512 bytes and data rate of 4 packets per second. 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 T7250 CPU and 3GB RAM. In this section based on the simulation environment and methodology performance is compared for EAACK and Trust Aware Secure Intrusion Detection System.

A. Simulation parameters

Parameter	**Value**
Number of nodes	30 nodes
Simulation area	800 meter x800 meter
Simulation time	10 sec
Packet size	512 bytes

Table 1.1 Simulation Parameters

These following metrics are used to evaluate the performance of IIDS for existing and proposed technique which are defined as follows:

1.) *Packet delivery ratio* (PDR): It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.
2.) *Routing Overhead (*RoH): This is the ratio of routing related packets in bytes (RREQ, RREP, RERR, AACK,) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgments, alarms and switching over head is included.
3.) *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.
4.) *Throughput:* The average rate of successful message is delivery over a communication channel.

During the simulation, the source route broadcasts an RREQ message to all the neighbours within its communication range. Upon receiving this RREQ message, each neighbour appends their addresses to the message and broadcasts this new message to their neighbours. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message. To compare the performance of EAACK and Trust Aware Secure Intrusion Detection System, two situation settings are simulated for differing kinds of misbehaviours or attacks.

Scenario 1: During this situation, we tend to simulate a basic packet- dropping attack. Malicious nodes merely drop all the packets that they receive.

Scenario 2: This situation is meant to check IDSs' performances against false misconduct report. During this case, malicious nodes continuously drop the packets that receive and remand a false misconduct report whenever it's potential.

It is highly vital to guarantee that the data packets are valid and authenticated. In order to ensure the integrity of the intrusion detection system, Trust aware system requires data packets to be encrypted before they are sent out and verified until they are accepted. To address the problem of using extra resources due to the introduction of security in MANETs, new scheme namely Trust Aware Secure Intrusion Detection System is adopted to achieve the goal of finding the most optimal solution for using security in MANETs.

B. Simulation results

This section describes on comparing the performances of EAACK scheme as well as Trust Aware based intrusion detection scheme. The figures given below is the results of simulation and these provide high quality in data delivery with high security provided by Trust Aware Secure Intrusion Detection System when compared to EAACK scheme.

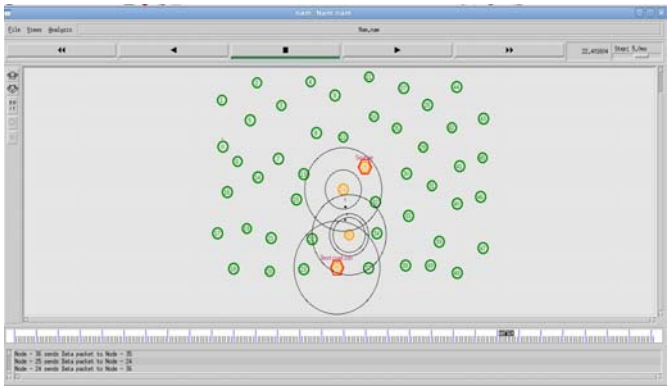


Fig. 6 Simulation of EAACK Scheme

Fig.6 represents the simulation of EAACK scheme. Here the source node is 25 and destination node is 35. When data is being sent from source to destination packet drop happens.

Node 24 is the intruder which drops the packet which leads to missing data at destination.

The following figure represents the simulation of Trust Aware Intrusion Detection Scheme.

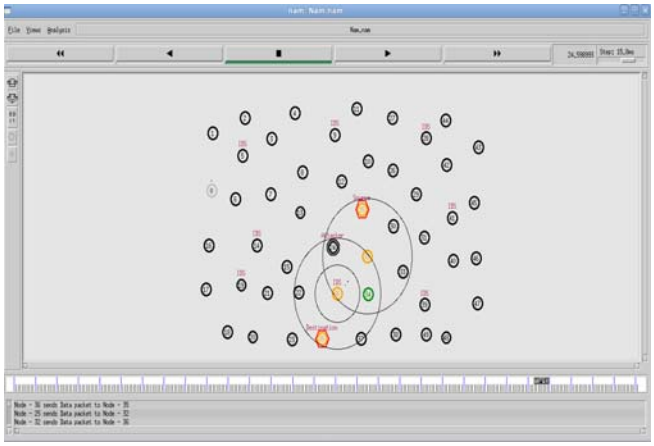


Fig. 7 Simulation of Trust Aware Intrusion Detection Scheme.

Here the source node is 25 and destination node is 35. Since there lies an intruder in the path, a new path is been chosen and data is sent to the destination node through the new path, as shown in Fig 7. New route is chosen based on the dynamic source routing mechanism which chooses the nearest possible path to reach the destination.
Packet dropping has always been a major threat to the security in MANETs and thus Trust Aware Secure Intrusion Detection System, (TASID) can reduce the packet drop when the attackers are smart enough to forge acknowledgment packets which can be represented graphically in Fig. 8.

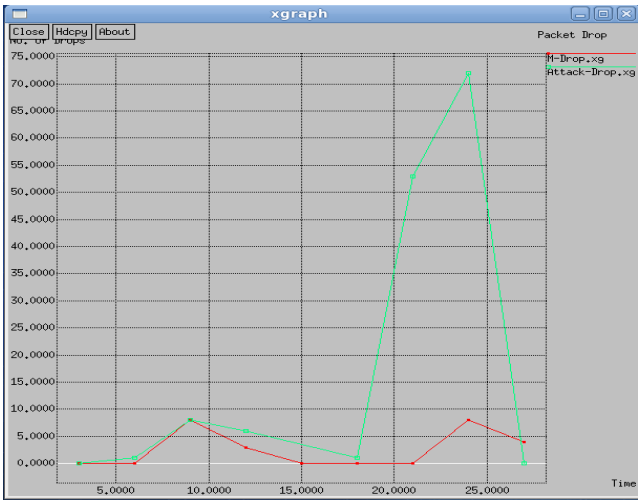


Fig. 8 Comparison of Packet drop

Packet delivery ratio is the ratio of the total number of packets received at the destination to the total number of sent packets by the source. Packet delivery ratio is more in Trust Aware Secure Intrusion Detection System when compared to EAACK. The graphical representation is shown below Fig. 9.

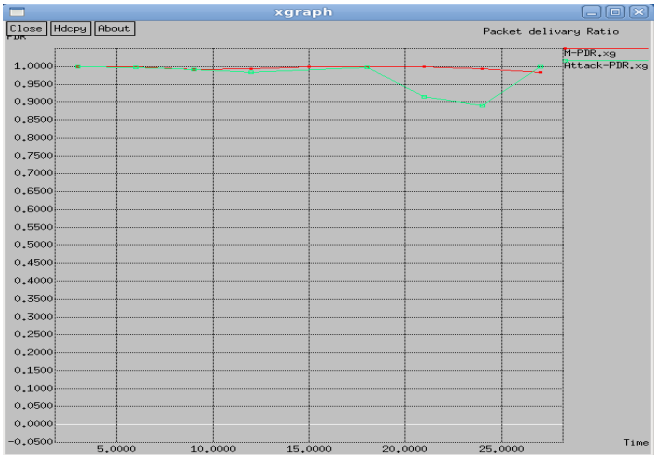


Fig. 9 Comparison of Packet delivery ratio.

Throughput is the average rate of successful message which is delivered over a communication channel. Throughput is more in Trust Aware Secure Intrusion Detection System than in EAACK. High rate of throughput is provided by Trust Aware Secure Intrusion Detection System than in EAACK is graphically represented in Fig. 10.

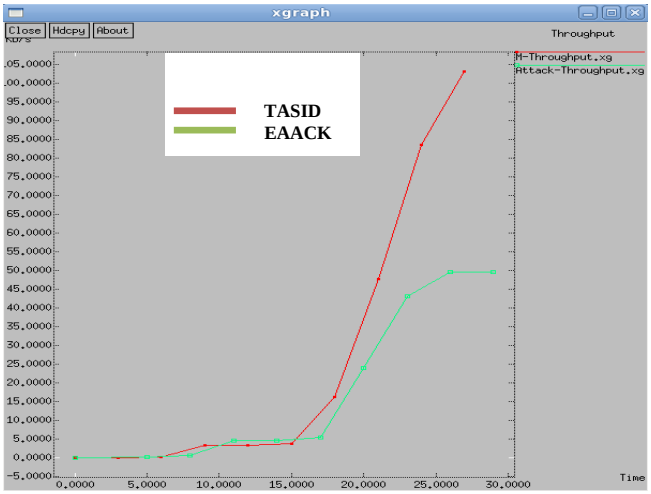


Fig. 10 Comparison of Throughput

CONCLUSION

Packet-dropping attack has always been a major risk to the security in MANETs. In this work an Intrusion Detection System namely Trust Aware Secure Intrusion Detection System for MANETs is compared against the existing EAACK mechanisms in different scenarios through simulations. The results demonstrated optimistic performances against EAACK in the cases of receiver collision, false misbehaviour report and limited transmission power. Although it generates more Routing Overhead in the present scheme as demonstrated for some cases, it can vastly advance the network's Packet Delivery Ratio, when the attackers are smart enough to forge acknowledgment packets. To increase the merits of the present work, plans have made to investigate the possibility of implementing hybrid cryptography techniques to further reduce the network overhead caused by security.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETS" *IEEE Trans. Ind. Electron.*, Vol. 60, No. 3, pp. March 2013.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008

[5] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.