International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

The Implementation of Trust Aware EAACK: the Intrusion Detection System to detect malicious nodes in MANET

Mr. Vivek D. Badgujar[1], Prof. Kailash Patidar[2], Prof. Jitendra Rai[3]
[1] PG Student, Software Engineering, SSSIST Sehore, RGPV, Bhopal, India
[2] Head of Department, CSE/IT, SSSIST Sehore, RGPV, Bhopal, India
[3]Asst. Prof., CSE, SSSIST Sehore, RGPV, Bhopal, India

Abstract*— Wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections. A wireless network can be structured to function in either BSS (Basic Service Set) or IBSS (Independent Basic Service Set) mode. In BSS mode, also called infrastructure mode, a number of mobile nodes are wirelessly connected to a non-mobile Access Point (AP). The IBSS mode, also called peer to peer or ad hoc mode, allows nodes to communicate directly (point-to-point) without the need for an AP. An ad hoc network, or MANET (Mobile Ad hoc Network), is a network composed only of nodes, with no Access Point. Messages are exchanged and relayed between nodes. A wireless network is more versatile than a wired one; it is also more vulnerable to attacks. Security has become a primary concern in order to provide protected communication between mobile nodes in a versatile environment. There are both passive and active attacks in MANETs. Here is where the intrusion detection system comes in. Intrusion detection can be defined as a process of monitoring activities in a network system and detect intrusions, the mechanism by which this is achieved is called an intrusion detection system (IDS). Due to Intrusion Detection System the performance of the network will be increased by detecting the malicious nodes in the network. Many intrusion detection systems have been proposed to suit the characteristics of MANETs but they have some drawbacks in it. To overcome the drawbacks new very efficient IDSs is designed known as Enhanced Adaptive Acknowledgement (EAACK). Compared to other IDS, EAACK gives higher malicious- behavior-detection rates in certain conditions without affecting the overall network performances. The proposed Trust aware EAACK scheme uses DSR routing protocol for find out the exact malicious nodes using simulation in the network, it's reduces the false detection rate by using the concept of trust value in large size of MANET.

***Keywords:* - AP, BSS, DSR, EAACK, IDS, MANET.**

I. INTRODUCTION

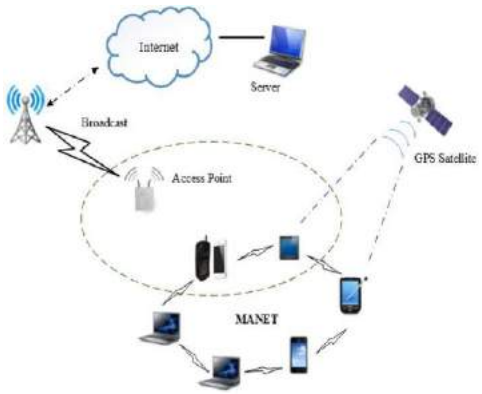


Fig. 1 Basic MANET architecture

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 rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery.

Characteristics of MANETs

- Dynamic topologies.
- Bandwidth constrained, variable capacity links.
- Energy constrained operation.
- Limited physical security.

MANET has been a popular topic of research in recent years with the advent and growth of wireless technology. Two popular types of MANETs are:

- VANET (Vehicular Ad-hoc network)
- IMANET (Internet based ad-hoc networks).

Several routing protocols have been suggested and used for MANET. Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector Routing (AODV) and Destination Sequenced Distance-Vector (DSDV) have been implemented. The mobile ad hoc network has the following typical features:

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

1.1 Intrusion Detection System (IDS)

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. Intrusion detection can be classified based on data as either host based or network-based. A network- based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. The IDS system is an integrated method for detect any attacks by analyzing and continues monitoring network activities. Intrusion detection systems can be run on each mobile node to check local traffic and detect local intrusions. These nodes can communicate local intrusion information to each other as and when needed. Fig.2 shows the local model of intrusion detection system. Each node has local IDS that by this, node can connect to network and local IDS checking all send or receive data in/out node. Other technique is to run intrusion detection system for self and neighbor nodes to check for malicious neighbor. The global intrusion detection system can be deployed for clusters of mobile nodes where head node is responsible for global intrusion detection for its cluster [11].

1.1.1. IDS architecture

The existing IDS architectures for MANETs fall under three basic categories [14] (a) stand-alone, (b) cooperative, and (c) hierarchical. (a) Stand-alone: in stand-alone architectures every node performs IDSs locally without collaborating and responds locally. This IDS architecture has a drawback for network attacks [17]. There limitation is in terms of detection accuracy and the type of attacks that they detect [14]. (b) Cooperative: in this architecture all nodes in MANET have their own local IDS system. Nodes come to a decision in a distributed fashion cooperatively. Upon determination of an intrusion, nodes share this information, asset attack risk degree and take necessary actions to eliminate the intrusion using active or passive precautions [17]. At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET [18]. (c) Hierarchical: the hierarchical architectures amount to a multilayer approach, by dividing the network into clusters. Specific nodes are selected (based on specific criteria) to act as cluster-heads and undertake various responsibilities and roles in intrusion detection, which are usually different from those of the simple cluster members [14]. The main advantage of this architecture is effective use of constraint resources but has a drawback for highly mobile MANETs for establishing zones and detecting responsible nodes in clusters [16].

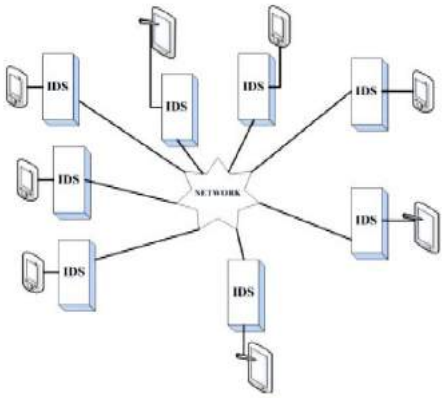


Fig. 2 Sample of Intrusion Detection System

1. 1.2. IDS engine

IDS engine is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Firstly, it performs the appropriate transformations on the selected labeled audit data. Then, it computes the classifier using training data and finally applies the classifier to test local audit data in order to classify it as "normal" or "abnormal" [12].

1.1.3. IDS watermarking techniques

Watermarking is the method for protecting the related data that should exchange between nodes, or is imperceptible added to the cover-signal in order to convey the hidden data. Watermarking techniques are

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

then applied in order to prevent the possible modification of the produced maps [13].

1.2. Attacks on the MANET

Approximately All researchers have two categorize of attacks on the MANETs. They characterized attacks to passive and active. The passive attacks typically involve only eaves dropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, Attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely [15, 16]. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [10, 11, 12, and 13] were first brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in. Packet Drop attack is one of the most important security problems in Mobile adhoc network [2]. Both routing packets and data packets forwarding function would be affected in the presence of misbehaving nodes. The node misbehavior can be classified as malfunctioning, selfish and malicious. Malfunctioning nodes suffer from hardware or network failures. Selfish nodes refuse to forward or drop data packet. Malicious nodes use their resource and aims to fail other nodes or whole network, by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control [3].

1.3 Routing protocols in MANET

In mobile ad hoc networks, the major role is played by routing protocols in order to route the data from one mobile node to another. Due to the limited wireless transmission range, the routing generally consists of multiple hops. These routing protocols are having the functionality of forwarding the data packets from sender to the intended recipient. In such type of networks routing is mostly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements. Mobile Ad-Hoc network routing protocols are commonly divided into three main types Proactive, Reactive and Hybrid protocols [7].

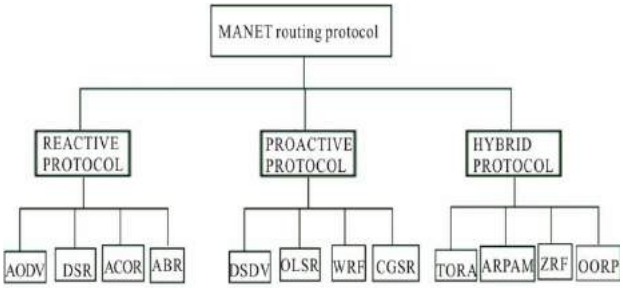


Fig. 3 Classification of routing protocols

i) Proactive Protocols: This type of routing protocol, maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. An example of proactive routing protocol is Destination sequenced distance vector (DSDV).

ii) Reactive Protocols: Reactive routing protocol is also known as on demand routing protocol. In this protocol route is discovered whenever it is needed Nodes initiate route discovery on demand basis. Source node sees its route cache for the available route from source to destination if the route is not available then it initiates route discovery process. The on- demand routing protocols have two major components. ***Route discovery***: In this phase source node initiates route discovery on demand basis. Source nodes consults its route cache for the available route from source to destination otherwise if the route is not present it initiates route discovery. The source node, in the packet, includes the destination address of the node as well address of the intermediate nodes to the destination. ***Route maintenance***: Due to dynamic topology of the network cases of the route failure between the nodes arises due to link breakage etc. so route maintenance is done. Reactive protocols have acknowledgement mechanism due to which route maintenance is possible Reactive protocols add latency to the network due to the route discovery mechanism. Each intermediate node involved in the route discovery process adds latency. These protocols decrease the routing overhead but at the cost of increased latency in the network. Hence these protocols are suitable in the situations where low routing overhead is required. There are various well known reactive routing protocols present in MANET for example DSR. Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach [18]. In Dynamic Source Routing (DSR), shown in Fig. 4, the protocol is based on the link state algorithm in which source initiates route discovery on demand basis. The sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet. DSR

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

was designed for multi hop networks for small Diameters. It is a beaconless protocol in which no HELLO messages are exchanged between nodes to notify them of their neighbors in the network.

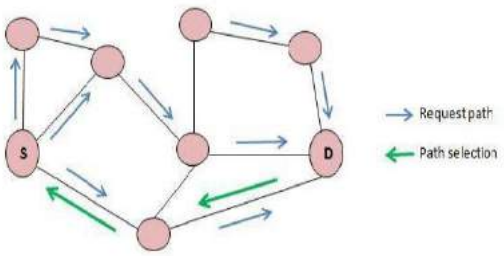


Fig. 4 Dynamic Source Routing (DSR)

iii) Hybrid Protocols: This type of routing protocol combines the advantages of reactive and proactive routing protocols. Examples of Hybrid routing protocols are ZRP [6].

II. RELEATED WORK

This section provides an overview of the background information and related work that is important for the understanding of proposed system. The existing Intrusion Detection Systems for MANET is briefly introduced, which are used for detecting malicious nodes and mitigating routing misbehavior. The various techniques that have been applied to detect malicious node in network are discussed in this section. Following are several different approaches for intrusion detection system. The comparison of reviewed intrusion detection techniques used to detect malicious nodes in MANET is shown in Table 1. The Table 1 also discusses strengths and weaknesses of respective IDS technique [1, 3]. The discussion in related work section and Table 1 confirms that existing techniques cannot solve the problem of receiver collision, limited transmission power and false misbehavior report.

Table 1

COMPARISON OF INTRUSION DETECTION SYSTEMS FOR MANET

Name of IDS (Year)	Algorithm / Protocols	Strengths	Weaknesses
Watchdog and Path rater (2000)	DSR Protocol	Improves the throughput of network with the presence of malicious nodes.	Fails to detect malicious misbehaviors with the presence of ambiguous collisions, receiver collisions ,limited transmission power, false misbehavior report ,collusion partial dropping.
TWOACK (2007)	DSR Protocol	Solves the receiver collision and limited transmission power problems of Watchdog.	The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.
AACK (2010)	DSR Protocol	Compared to TWOACK, AACK significantly Reduces network Overhead while still capable of maintaining or even surpassing the same network throughput.	It is crucial to guarantee that the acknowledgment packets are valid and authentic.
EAACK (2013)	Digital Signature algorithm and DSR	i. Solves the three weaknesses of Watchdog scheme, false misbehavior, limited transmission Power and receiver collision. ii. Prevents the attacker from forging acknowledgment packets.	This scheme produces more routing overhead if numbers of malicious nodes are increased.

III. PROPOSED WORK

The proposed system named as EAACK with Trust scheme is consisted of four major parts, namely, ACK (Acknowledgement), secure ACK (S-ACK), and misbehavior report authentication (MRA) and finally, considers the trust value for eliminating the attacker[19], as shown in Fig. 5. In this proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

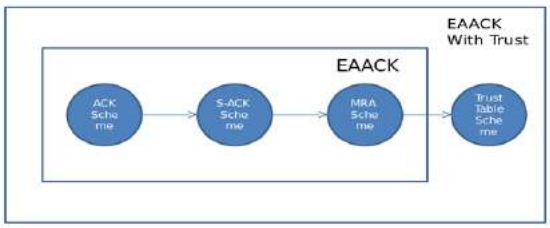


Fig. 5 Proposed System

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

1) ACK Scheme

In the ACK, the aim is to reduce the network overhead when no network misbehavior is detected. It is end to end acknowledgment scheme. ACK Scheme shown in fig. 6. The destination node is required to send

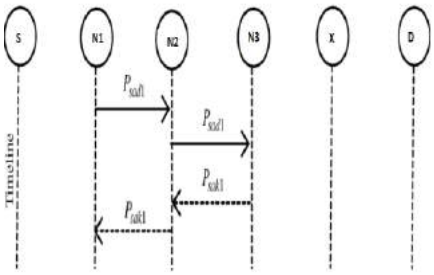


Fig. 6 ACK scheme

Back an acknowledgment packet to the source node when it receives a new packet. The basic flow is, if Source node S sends an ACK data packet Pad1 to destination Node D, and if all the intermediate nodes between S to destination node D are cooperative and successfully receives the P ad1, then for node D it is necessary to send back ACK acknowledgment packet Pack1 from the same route but in reverse order. If the Pack1 packet is received to node S in the predefined time period, then the packet transmission is successful from source node S to destination node D. Otherwise it switch to S-ACK mode and send out S-ACK data packet to detect misbehaving node in the route[1].

2) Secure acknowledgment (S-ACK) Scheme

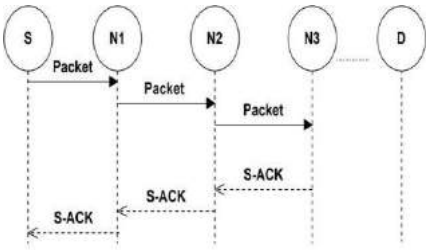


Fig.7 S-ACK scheme

Fig. 7 Explains source sends S-ACK packet in the intention of detecting misbehaving nodes in the route. S-ACK sends acknowledgment back to source after the packet reaches consecutive three nodes ahead the route. The third node required to send an S-ACK acknowledgement to first node. S-ACK mode facilitates easy detection of misbehaving nodes in the presence of receiver collision and limited power for transmission. N1, N2, N3 are three consecutive nodes. N1 sends S-ACK data packet to N2 which is next in the route and N2 relays it to N3. When N3 receives the S-ACK data packet it acknowledges N2 with S-ACK acknowledgement packet and N2 acknowledges back to N1. If N1 doesn't receive the acknowledgement within a particular time it will report N2, N3 as malicious nodes by generating a misbehavior report. This misbehavior report is sent back to the Source. To validate this report the source switches itself to MRA mode [3].

3) Misbehavior report acknowledgment (MRA)

This MRA scheme is designed to resolve the limitations of watchdog where it fails to detect the misbehaving node with the presence of false misbehavior report. This false misbehavior report can be generated by the attacker's by reporting falsely for the innocent nodes as malicious. The goal of MRA scheme is to authenticate whether the destination node has received the reported missing packet from a different route. In the MRA mode source node find for an alternate route to the destination node. If there is no other route is exists, the source node starts a DSR routing request to find another route. By adopting the alternate route for the destination node then it can avoid the misbehavior reporter node. When the destination node receives the MRA packet it searches it's knowledge base and compares to that the reported packet was received or not, if it is already received then it conclude that this is a false misbehavior report and whoever send it, is marked as malicious. Otherwise the false misbehavior report is trusted and accepted.

4) Elimination of malicious node using trust table

Initially equal trust value is maintained for all the nodes in the network. Whenever a node is detected as the malicious node, its trust value is reduced and the source broadcast an "alert" message to all the nodes in the network. Every node in the system is given second chance to increase its trust level by properly participating in the routing process. Every other node updates its trust table. If the particular node repeats its misbehavior in the second chance, it is eliminated from the network. It means, no other nodes should communicate with the misbehaving nodes in the future.

***Algorithm*:**

```
#routing packets from source to destination#
Create a list N (all); #A set contains all the information
about nodes#
Initiate Route discovery using RREQ and RREP;
Transmit the packets (Sdata to Ddata)
#checking node activity#
If {Dack == receive} {
        Ddata;
}
else {
                Initiate Sack
        }
If (Received data == Sack) {
```

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

```
        Misbehavior report (a);
        If (Misbehavior reports (a) ==0) {
                Send Dack;
        }
else {
                Initiate MRA;
        }
If (Received data == MRA) {
        Find another path to Destination;
        If (Destination node doesn't have packet) {
                Trust the report
        }
        else {
                Mark reporter as malicious;
        }
Create a list H (i); # storing information about malicious nodes#
}
```

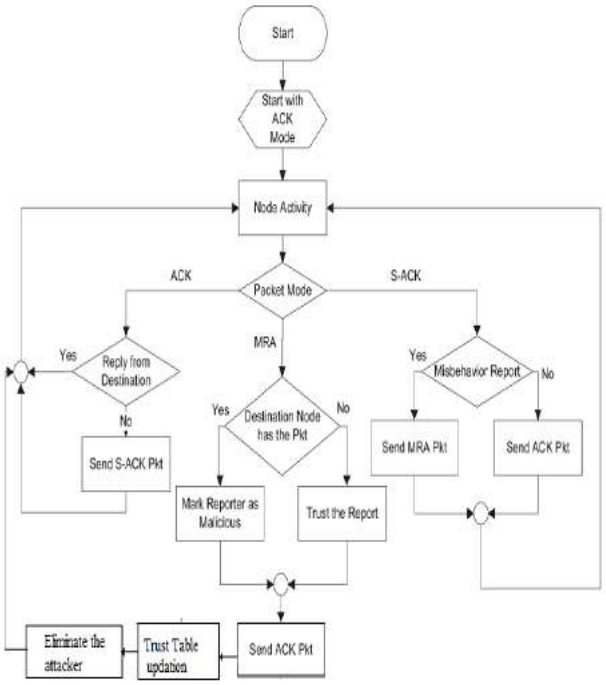


Fig. 8 Flow chart for EAACK with Trust

IV. PERFORMANCE EVALUATIONS

1. Simulation methodology

The simulation environment created using Network Simulator (NS2), version 2.35 on Ubuntu 14.04(LTS) run on laptop with core i3 CPU and 6GB RAM. We adapted NS 2.35 default scenario to contain 50 nodes scattered on 600 x 600 m flat area. The Random Waypoint mobility used with pause time zero and nodes moving speeds are 1 m/s for low speed network, and 10m/s for high speed network. Physical layer and 802.11 MAC layer are used in wireless extension of NS2. We used User Datagram Protocol (UDP) traffic with Constant Data Rate (CBR) 4 packets/second and packet size 1024 B. NS2 Simulator generates a tcl (Tool Command Language) file. On running the tcl file, it results into two more files, first the trace file which contains all the information regarding the network and seconds the nam (Network animator) file which is a visual aid showing how packets flow along the network and shows the Virtualization of the network corresponding to the trace file. All routing protocols in NS2 are mounting in the directory of "ns-2.35". The performance differentials are analyzed using packet delivery ratio, and routing overhead.

Table 2 Simulation Parameters

Software for simulation	Network simulator 2.35
Channel	Wireless
Simulation runs time	50 seconds
Area in which nodes move	600X600
Packet size	1024bytes
Speed	1m/s to 10 m/s
Routing Protocol	DSR
Propagation model	Two Ray Ground
Network Interface Type	Wireless Physical
Queue Type	Drop Tail
IFQ-Length	50 Packets
MAC Type	Mac/802.11
Antenna Type	Omni Antenna

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.

$$PDR\ (\%) = \frac{\text{Number of Received Packets at destination}}{\text{Number of packets generated by source node}}$$

Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions.

$$RO = \frac{\text{Number of Routing Packets Sent}}{\text{Number of Data Packet Sent}}$$

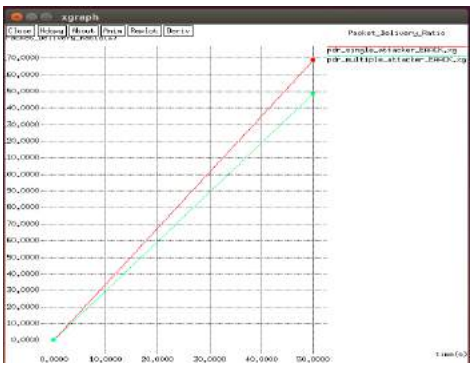
The proposed work is implemented for varying number of nodes and number of misbehaving nodes for different scenarios and compares the performance in terms of packet delivery ratio and routing overhead in EAACK system using Trust table.

2. Simulation results and discussion

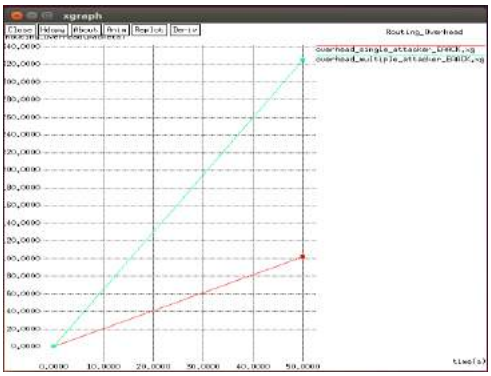
Comparative Graphs:

1] Packet Delivery Ratio with single_attacker_EAACK Vs multiple_attacker_EAACK. When the numbers of attacker's percentage are increased the packet delivery ratio is decreased.

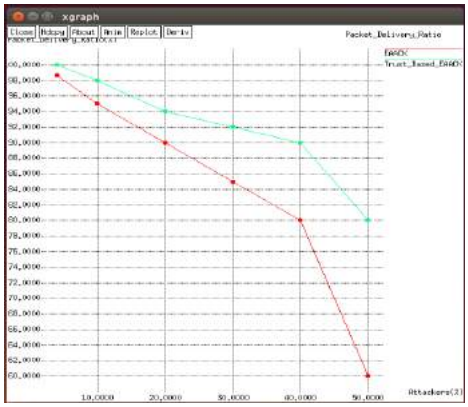
International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)



2] Routing overhead with single_attacker_EAACK Vs multiple_attacker_EAACK. When the numbers of attacker's percentage are increased the overhead is increased.

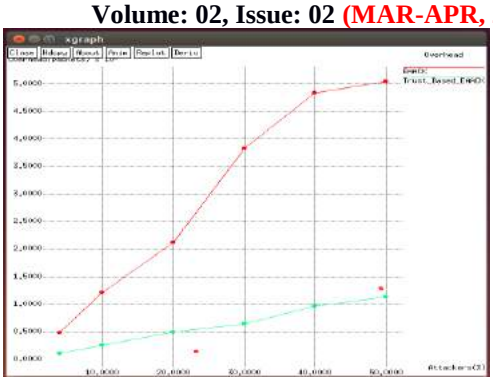


3] Packet Delivery Ratio with EAACK Vs Trust_Based_EAACK



When the numbers of attacker's percentage are increased the packet delivery ratio is decreased. The trust based EAACK scheme Provides better packet delivery ratio when compared to the existing EAACK scheme.

4] Routing Overhead with EAACK Vs Trust_Based_EAACK. When the numbers of attacker's percentage are increased the overhead is increased. The trust based EAACK scheme provides reduced overhead when compared to the existing EAACK scheme.



IV. CONCLUSION

The packet drop attack by malicious node has always been a major threat to the security in MANET. Compared to other approaches, The Proposed scheme EAACK shows higher malicious-behavior-detection rates in certain conditions without affecting the overall network performances. The proposed system EAACK detects the actual malicious nodes, thus reducing the false detection rate. EAACK is enhanced by using the concept of trust. A monitor node is placed in each link of data transmission to monitor the behavior of the routers. Once the malicious nodes are detected by both EAACK and behavior checking mechanism via monitors, trust value of the malicious nodes is reduced, and the information about the malicious node is broadcast to entire network. Malicious node is restricted from the router selection in future by other nodes in the network for the data transmission.

REFERENCES

[1] Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, "EAACK –A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, 2013.

[2] Anantvalee, Tiranuch and Jie Wu., "A survey on intrusion detection in mobile ad hoc networks", in Wireless Network Security, springer US, 2007.

[3] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami, "Detecting misbehaving nodes in MANETs", in Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services, ACM, 2010.

[4] M. Saravananand D. Jagan, "A Neighbor Knowledge with Zonal Routing Protocol to Reducing Routing Overhead in MANETs", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 3, pp. 3503-3507, 2014.

[5] Prachee N. Patil and Ashish T. Bhole, "Black hole attack prevention in mobile Ad Hoc networks using route caching", in 10thIEEE International Conference on Wireless and Optical

Communications Networks (WOCN), pp. 1-6, July 2013.

[6] K. Liu, J.Deng, P. K. Varshney and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs", IEEE Transactions on Mobile Computing, Vol. 6, No. 5, pp. 536–550, May 2007.

[7] Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki and H. Mouftah, "AACK-Adaptive Acknowledge Intrusion Detection for MANET with Node Detection Enhancement", in 24thIEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 634-640, 2010.

[8] U. Sharmila Begam and Dr. G. Murugaboopathi, "A Recent Secure Intrusion Detection System for MANETs", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 3, Special Issue 1, pp. 54-62, January 2013.

[9] Durgesh Wadbude and Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 4, pp. 274-279. April 2012.

[10] D.B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[11] Dang, N., & Mittal, P., (2012). Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology, 1, 1.

[12] Mitrokotsa, A., Tsagkaris M., and Douligeris, Ch. (2008) Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms, Boston: Spring, 256.

[13] Mitrokotsa, A., Komninos, N. and Douligeris, Ch., (2007) Intrusion Detection with Neural Networks and Watermarking Techniques for MANET, Pervasive Services, IEEE International Conference.

[14] Panos, Ch, Xenakis, Ch and Stavrakakis, I.S. (2010). A novel intrusion detection system for MANETS International Conference on Security and Cryptography.

[15] Blazevic, L., et al. (2001). Self-organization in mobile ad-hoc networks: the approach of terminal nodes, IEEE Communications Magazine.

[16] Sharman, R., & Sharma, S. , "Performance analysis of intrusion detection in MANET, Computer Technology and Applications 2011.

[17] Mutlu, S., & Yilmaz, G., Distributed cooperative trust based intrusion detection framework for MANETs, The Seventh International Conference on Networking and Services, 2011.

[18] Li, Y., & Wei, J. Guidelines on selecting intrusion detection methods in MANET, Proceedings of the Information Systems Education Conference, 2004.

[19] Vivek D. Badgujar, Kailash Patidar, Jitendra Rai "An Intrusion Detection System for detecting malicious nodes in MANET using Trust Aware EAACK", International Journal of Current Trends in Engineering & Technology (IJCTET), Vol. 2, Issue 2, pp. 184-189, March- April 2016.