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

An Intrusion Detection System for detecting malicious nodes in MANET using Trust Aware EAACK

Vivek D. Badgujar[1], Kailash Patidar[2], Jitendra Rai[3]
SSSIST Sehore, RGPV, Bhopal, India
badgujarvivek83@hotmail.com

Abstract —Due to limitations of wired network, the transformation has been seen from wired network to wireless network in last few years. Wireless network is a technology that allows users to access easily information and services from regardless of geographical position. Due to mobility & scalability features wireless networks uses in many areas as an applications. Different types of wireless network is available, among all the types of wireless networks (Mobile Adhoc Network) MANET is very important applications. MANET is infrastructure less, IP based network of mobile and wireless machine nodes connected with radio range. In working, the node of a MANET gives decentralized administration mechanism. In MANET working node act as a host and router at within the communication range nodes communicate directly. Otherwise they pass the messages to his neighbor nodes. Due to self-configuring nature MANET becomes very popular in military applications and recovery applications. But due to open medium nodes becomes malicious easily by malicious attackers. For this, Intrusion-Detection System (IDS) is made for protection from malicious attackers. In Intrusion Detection System the performance of the network will be increased by detecting the malicious nodes in the network. Many IDSs is available in the market but have drawbacks available. 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 system uses DSR routing protocol by EAACK for providing better performance for large size MANET. The proposed EAACK scheme find out the exact malicious nodes using simulation, thus reducing the false detection rate EAACK is enhanced by using the concept of trust value.

Keywords: DSR, EAACK, IDS, MANET, Monitor node.

I. INTRODUCTION

Mobile Ad - hoc Network (MANET) gives unique characteristics in a highly challenging network environment such as decentralization, dynamic topology and neighbor based routing. The communication done in MANET is a group of wireless mobile nodes via bidirectional wireless links without any fixed infrastructure [1]. Mobile nodes are acts as a wireless transmitter and a receiver. They are communicating directly with each other or forward message through other nodes [2]. The key advantages of wireless networks are that its ability to send data between different parties and still maintain their mobility. Mobile communication is depending upon the range of transmitters. This means that two nodes are communicated with each other when the distance between the two nodes is in the communication range of their own. MANET is divided into two types of networks, namely, single - hop and multi hop [3]. In a single - hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is not in their radio range. MANET is infrastructure less network, thus all nodes are free to move remotely. MANET infeasible in critical mission applications like military conflict or emergency recovery due to creating a self - configuring and self - maintaining network without the help of a centralized infrastructure, [3].The MANET topology may change uncertainly and speedily due to high mobility of the independent mobile nodes. Also due to the limitations 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. In such case, it is required to develop an intrusion - detection system (IDS) especially for MANETs [4]. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. An intrusion detection system does not include preventing the intrusion from occurring; it can only be detected and

reported to each node in network [5]. Intrusion detection can be classified into either host based or network – based in terms of data. A network - based IDS captures and analyses packets from network traffic while a host - based IDS uses operating system or application logs in its analysis. Packet Drop attack is most important security problems in MANETs [2]. The forwarding function of both routing packets and data packets would be affected in the presence of misbehaving nodes. The node misbehavior can be classified as malfunctioning, selfish and malicious. Malfunctioning nodes are suffered from hardware or network failures. Selfish nodes refuse to forward or drop data packet. Malicious nodes use their resource 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].

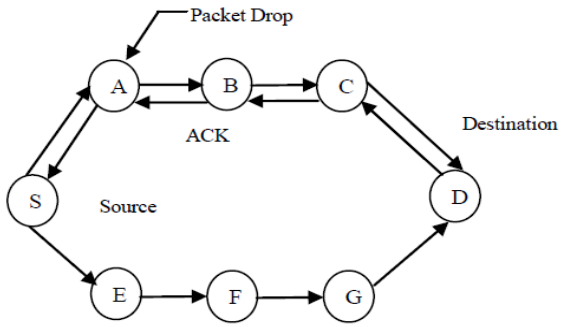

Fig.1 Attack Scenario in MANET

The Fig.1 shows an attack scenario. The source node S sends ACK data packet to Destination node D, then for node D it is necessary to send back ACK acknowledgment packet to S. If packet is not received in predefined time period then it switches to S-ACK mode and send out SACK data packet to detect misbehaving node in the route. In S-ACK mode it detects two misbehaving nodes in network. In MRA mode it authenticate whether the destination node has received the reported missing packet from a different route and also it finds out the real malicious node in network. The Fig.2 shows each incoming packet is dropped by malicious node in network. The source node A is trying to establish a connection to destination node E. Node A broadcast RREQ message, Node B and D receives RREQ and update a route to its previous hop and send RREQ to Node C. Node C is a malicious node which drops the received request so node A cannot communicate with node E. In this way Node C receives any packet will not forward and drop all the packets. One of the fundamental challenges of MANET is the design of dynamic routing protocols with good performance and less overhead [6]. Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks from unauthorized access, use, modification or destruction. A security attack is any action that compromises the security of information in an unauthorized way. The attack may alter, release, or deny data [14] [15] [16]. The attacks on the MANET can be classified into two categories: passive and active attacks. Both passive and active attacks can be made on any layer of the network protocol stack [17].

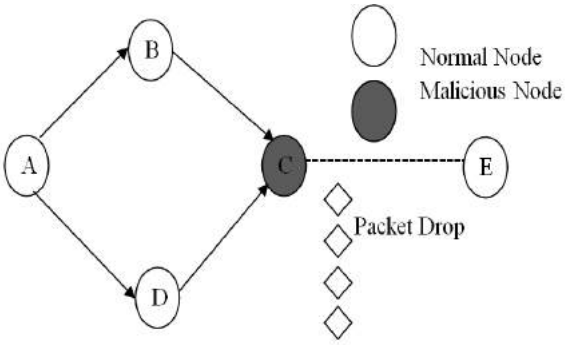

Fig. 2 Packet Drop Attack by Malicious Node.

Passive Attacks: A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. Passive attacks are very hard to detect because they do not involve any alteration of the data.

Active Attacks: An active attack attempts to change or destroy the system resources. It gains an authentication and tries to affect or disrupt the normal functioning of the network services by injecting or modifying arbitrary packets of the data being exchanged in the network. An active attack involves information interruption, modification, or fabrication. 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].

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: This type of routing is also known as on-demand routing protocol. If a node wants to send a packet to another node then this protocol finds the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On demand Distance Vector routing (AODV) and 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. S. Marti, T. J. Giuli, K. Lai, and M. Baker [8] proposed a Watchdog and Pathrater scheme of intrusion detection system for MANET is introduced that aims to improve the throughput of network with the presence of malicious nodes [12]. Watchdog is able to detecting malicious nodes rather than links. The watchdog is based on reactive feedback that is overhearing to confirm whether the next node has forwarded the packet or not. Pathrater works as response system. Once Watchdog node identifies malicious node in the network, the Pathrater cooperates with the routing protocols to avoid the reported node in the future transmission. The standard is Dynamic Source Routing protocol (DSR) in that the routing information is defined at the source node [2]. So because of this it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping. N. Nasser and Y. Chen [9] proposed Ex Watchdog which extends from Watchdog proposed in that solving the problems of the Watchdog scheme which is the false misbehaving problem, where a malicious node falsely reports other nodes as misbehaving while in fact it is the real intruder. When the source receives a report about misbehaving node, it will find another path to ask the destination node about the number of received packets. If it is equal to the packets that the source has sent, then the real malicious node is the node that reports other nodes as misbehaving. Otherwise node being reported malicious do misbehave. But there is limitations in this scheme if the true misbehaving node is in the all available paths from source to destination then it is impossible to confirm and check the number of packets with the destination. K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan [10] proposed a TWOACK scheme which aims to solve the problem of receiver collision and limited transmission power of Watchdog. TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from source to destination. But the acknowledgment process required in every packet transmission process added a considerable amount of unwanted network overhead. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [12]. Al-Roubaiey, T. Sheltami, A. Mahmoud , E. Shakshuki and H. Mouftah [11] proposed a AACK is a network layer acknowledgement based scheme which detects misbehaving node instead of misbehaving link and an end to end acknowledgment based scheme, to reduce the routing overhead of TWOACK. The AACK scheme may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets. AACK still suffers from the partial dropping attacks and false misbehavior report. N. Kang, E. Shakshuki and T. Sheltami [3] proposed

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

Enhanced Adaptive Acknowledgment scheme which consist of three parts Acknowledgment, Secure Acknowledgment, misbehavior report authentication. This scheme is capable of detecting malicious nodes despite the existence of false misbehavior report. Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami [1] proposed EAACK scheme with digital signature to prevent the attacker from forging acknowledgment packets. All acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver, because of that it causes the network overhead. Durgesh Wadbude and Vineet Richariya [13] give secure Ad hoc On Demand Distance Vector Routing (AODV) a novel algorithm for the operation of such ADHOC networks. Each Mobile node operates as a specialized router and routes are obtained on demand. After over viewing two intrusion detection techniques watchdog and TWOACK, the AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report. So, the EAACK system is designed to solve the problem of false misbehavior report.

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 as shown in Fig. 3. The Fig. 4 Explains the EAACK with Trust components. 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.

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. 5. The destination node is required to send 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.

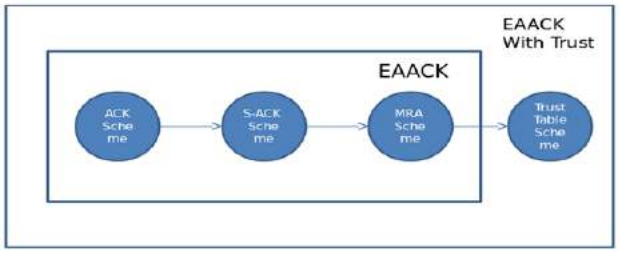

Fig. 3 Proposed System

DATA	ACK	S-ACK	MRA	TRUST

Fig. 4 EAACK with Trust Components

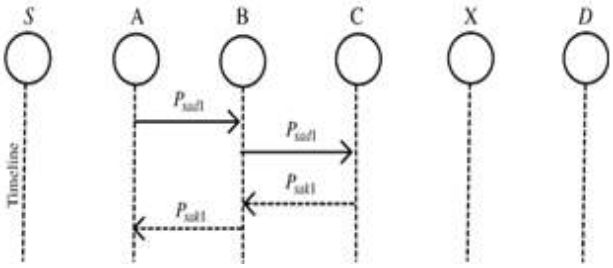

Fig. 5 ACK scheme

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.

2) Secure acknowledgment (S-ACK) Scheme

In the S-ACK, the principle is to allow 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 back an S-ACK acknowledgment packet to the first node. The purpose of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

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

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

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.

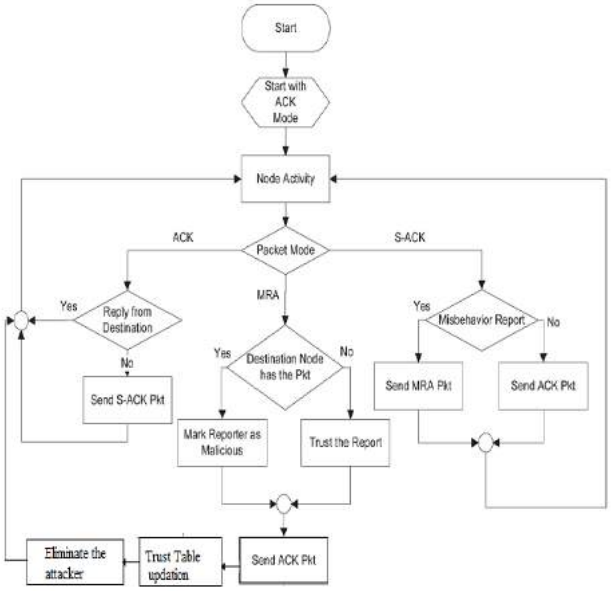

Fig. 6 Flow chart for EAACK with Trust

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) {
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#
}

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, pp. 1089- 1098, March 2013.

[2]. Anantvalee, Tiranuch and Jie Wu., "A survey on intrusion detection in mobile ad hoc networks", in Wireless Network Security, pp. 159-180, 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, pp. 216-222, ACM, 2010.

[4]. Ranjitj Bhosale and Prof. R. K .Ambekar, "A Survey on Intrusion detection System for Mobile Ad-hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 6, pp. 7330-7333, 2014.

[5]. Ashish T. Bhole and Archana I. Patil, "Intrusion Detection with Hidden Markov Model and WEKA Tool", International Journal of Computer Applications (IJCA), Vol. 85, No. 13, pp. 27-30, Jan 2014.

[6]. 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.

[7]. 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.

[8]. S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, ACM 2000.

[9]. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network", in IEEE International Conference on Communications (ICC'07), pp. 1154-1159, Jun 24–28, 2007.

[10]. 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.

[11]. 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.

[12]. U. Sharia Began 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.

[13]. 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.

[14]. W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2010.

[15]. A. J. Meekness, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, ISBN: 0849385237, 1996.

[16]. C. Gandhi and M. Dave, "A Review of Security in Mobile Ad Hoc Networks", IETE Technical Review, ISSN: 02564602, pp.335-344, Vol. 23, No. 6, 2006.

[17]. C. Siva Ram Murthy and B.S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Pearson Education, ISBN: 978-81-317-0688-6, 2006.