Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Reducing the Routing Overhead in Secure Mobile AD HOC Networks

Mrs. R. Pravallika
Assistant Professor
Computer Science and Engineering
Vignan's Institute of Engineering for Women (VIEW)
Visakhapatnam, India

G. Anusha
Under Graduate Student
Computer Science and Engineering
Vignan's Institute of Engineering for Women (VIEW)
Visakhapatnam, India

S. Girija
Under Graduate Student
Computer Science and Engineering
Vignan's Institute of Engineering for Women (VIEW)
Visakhapatnam, India

Rajeswari Laxmi
Under Graduate Student
Computer Science and Engineering
Vignan's Institute of Engineering for Women (VIEW)
Visakhapatnam, India

G. Hyndavi
Under Graduate Student
Computer Science and Engineering
Vignan's Institute of Engineering for Women (VIEW)
Visakhapatnam, India

***Abstract*— In a mobile ad hoc network (MANET), while getting the information about intruder from this method the intruders are identified with some extra security related transmission. The drawback of this method that is identifies once the intruder is detected the direction goes on transmitting some extra packets known as intruder check packets which ultimately increase the routing overhead and degrades the performance of network as it hops from the network node so there is a need to work upon and to reduce the routing overhead we are going to propose a protocol for reducing routing overhead in secure mobile ad hoc network. In this work the overview of proposed research direction and the objectives of the work are demonstrated.**

Keywords: Mobile ad hoc networks, RSA algorithm, Ad hoc On-demand Distance Vector Routing (AODV)

I. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of a collection of mobile nodes which can move openly. These nodes are without infrastructure and can be dynamically self-organized into arbitrary topology networks. One of the vital challenges in MANETs is the design and implementation of dynamic routing protocols with less overhead and better performance. Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) protocols have been proposed for mobile ad hoc network. A MANET is a number of mobile wireless devices which are the structure of the network of any pre-existing infrastructure. All mobile nodes work both as a router as well as host. Fixed broadcast range of wireless interface due to, through intermediate nodes the data traffic has sent packet source to destination over multiple hops. Intrusion detection system (IDS) is the process of detecting the activity of intruders which can affect the process of transmission among the nodes. IDS is considered as the first line of defense for security in MANET. An IDS uses methods and complex techniques for identifying abnormal behaviors. They try to find whether there is any malicious activity or not. The main aim of IDS is to detect the attack before the attacker introduces any harm to the network. In this paper, we are focusing on Reduce the routing overhead & increase the packet delivery ratio in Secure Intrusion Mobile ad hoc networks.

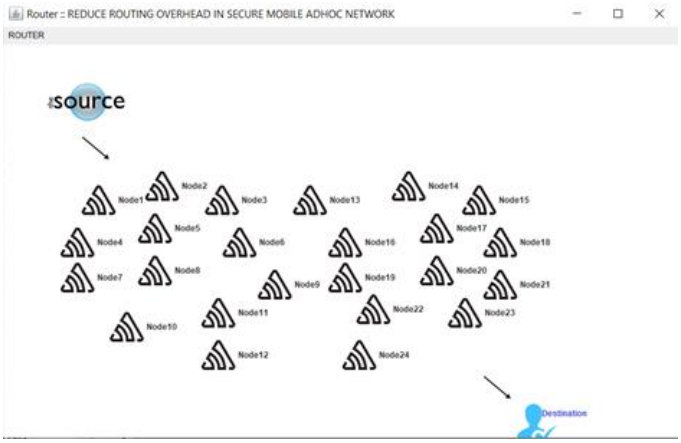

Figure 1: Basic topology of the network

The Network like MANET may or may not be portable. Each user node can be benefitted according to the network id provided by server. Every node in the network must forward the traffic not dependent to its use, and hence it will work as a router.

II. LITERATURE SURVEY

Abdulsalam Basabaa et al [1] implemented an intrusion detection system named Adaptive Three Acknowledgments (A3ACKs). The three major problems of Watchdog technique are solved and robust network security is achieved using the proposed method.

Deepa Krishnan [2] has presented an approach which is based on self-adaptive IDS. The salient feature of this approach is that it makes use of the light weight mobile agents.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Elhadi M. Shakshuki et al [3] introduced new IDS called Enhanced Adaptive Acknowledgment scheme for MANET. Enhanced Adaptive Acknowledgment solves the three major watchdog problems.

Yi Ping et al [4] proposed an intrusion detection system based on timed automata that helps to detect attacks on the dynamic source routing (DSR). The IDS can detect unknown intrusion without trained date or signature but with fewer false alarms.

Vishnu Balan E et al [5] introduced fuzzy based intrusion detection that not only detects attack but also finds the range and extension of attack. Drawback is to reduce the jitter value.

Shengrong Bu et al [6] proposed a scheme that combines authentication and IDS approach in MANET. Multi modal bio metric system is deployed to improve network security.

Adnan Nadeem et al [7] utilized a combination of anomaly based and knowledge based intrusion detection to protect MANETs from various attacks. But the problem in the IDS is that it causes more harm to network while isolating the attacker in some cases.

Sumit, S et al [8] used effective k-means to isolate attacker nodes from the network in zone routing protocol(ZRP). The drawback of false identification has to be reduced.

Abirami, K.R et al [9] presented a scheme which uses challenge key to detect replica nodes with high accuracy detection rate.

T. Poongothai et al [10] presented intrusion detection technique using machine learning approach. The IDS architecture combines rough set theory and support vector machine to increase the detection rate.

III. ATTACKS IN MOBILE AD HOC NETWORKS

Attacks in MANETs are classified into two types, namely active and passive attacks. Passive attack never disrupts the operation of the network. But the active attack disrupts the operation of the network by modifying the data. The attacks in MANET are classified into two types as DATA traffic attack and CONTROL traffic attack. Some of them are given below

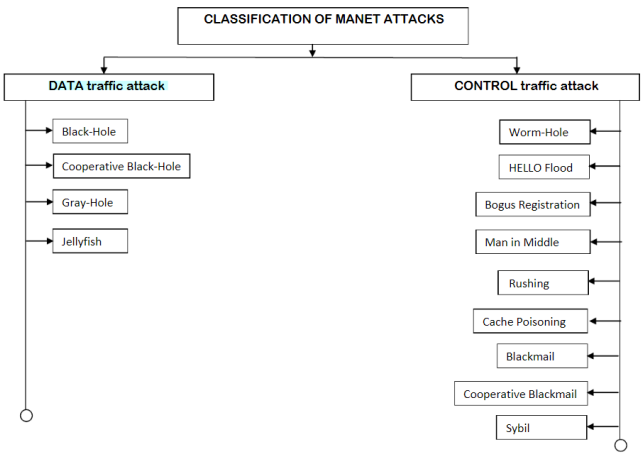

Fig 2. Different types of attacks in MANET

DATA TRAFFIC ATTACK

DATA traffic attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets. Some types of attacks choose victim packets for dropping while some of them drop all of them irrespective of sender nodes. This may highly degrade the quality of service and increases end to end delay. This also causes significant loss of important data.

Black Hole Attack: In this attack, the malicious node wrongly advertises right paths to destination node during path finding process in the route update messages.

Cooperative Black-Hole Attack: This attack is similar to Black-Hole attack, but more than one malicious node tries to disrupt the network simultaneously. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an Ad Hoc network. Mostly the only solution becomes finding alternating route to the destination, if at all exists.

Gray-Hole Attack: Gray-Hole attack has its own characteristic behaviour. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behaviour:

(i) Node dependent attack – drops DATA packets destined towards a certain victim node or coming from certain node, while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.

(ii) Time dependent attack – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances.

Jellyfish Attack: Jellyfish attack is somewhat different from Black-Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it delays them before finally delivering them. It may even scramble the order of packets in which they are received and sends it in random order. This disrupts the normal flow control mechanism
used by nodes for reliable transmission. Jellyfish attack can result in significant end to end delay and thereby degrading QoS. Few of the methods
used by attacker in this attack:

(i) One of the methods is scrambling packet order before finally delivering them instead of received FIFO order. ACK based flow control mechanism will generate duplicate ACK packets which will unnecessarily consume precious network bandwidth and battery life.

(ii) Another method can be, performing selective Black-Hole attack by dropping all packets at every RTO. This will cause timeout in sender node at every RTO for that duration. If nodes use traffic shaping, default flow control mechanism might be triggered to the sender node as it is same as destination overwhelm

CONTROL TRAFFIC ATTACK

Mobile Ad-Hoc Network (MANET) is inherently vulnerable to attack due to its fundamental characteristics, such as open medium, distributed nodes, autonomy of nodes participation in network (nodes can join and leave the network on its will), lack of centralized authority which can enforce security on the network, distributed co-ordination and cooperation. The existing routing protocols cannot be used in MANET due to these reasons.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Wormhole Attack: The attacker passes the data from one location to another by creating a tunnel path in the network.

Bogus Registration Attack: A Bogus registration attack is an active attack in which an attacker disguises itself as another node either by sending stolen beacon or generating such false beacons to register himself with a node as a neighbour. Once registered, it can snoop transmitted packets or may disrupt the network altogether. But this type of attack is difficult to achieve as the attacker needs to intimately know the masquerading nodes identity and network topology. Encrypting packets before sending and secure authentication in route discovery (SRDP, SND, SNRP, ARAN, etc) will limit the severity of attack to some extent as attacker node has no previous knowledge of encryption method.

Man in Middle Attack: In Man in Middle attack, the attacker node creeps into a valid route and tries to sniff packets flowing through it. To perform man in middle attack, the attacker first needs to be part of that route. It can do that by either temporarily disrupting the route by deregistering a node by sending malicious disassociation beacon captured previously or registering itself in next route timeout event. One way of protecting packets flowing through MANET from prying eyes is encrypting each packet. Though key distribution becomes a security issue.

Rushing Attack: In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node
broadcasts a RREQ (route request) message in neighbourhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker quickly forwards with a malicious RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node.

IV. REDUCE THE ROUTING OVERHEAD

While getting the information about intruder from this method the intruders are identified with some extra security related transmission. The drawback of this method that is identified once the intruder is detected the direction goes on transmitting some extra packets known as intruder check packets which ultimately increase the routing overhead degrades the performance of network so there is a need to work upon and to reduce the routing overhead.

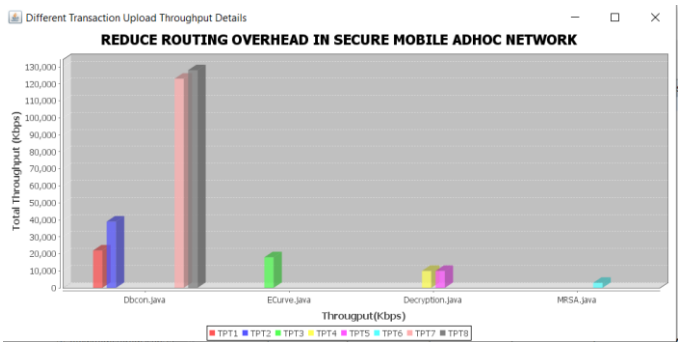

Figure 2: Routing overhead

Figure 2. Has routing overhead. It clearly shows that secure IDS method have less overhead because of additional intruder check packet compared to existing A3ACK method with intruders.

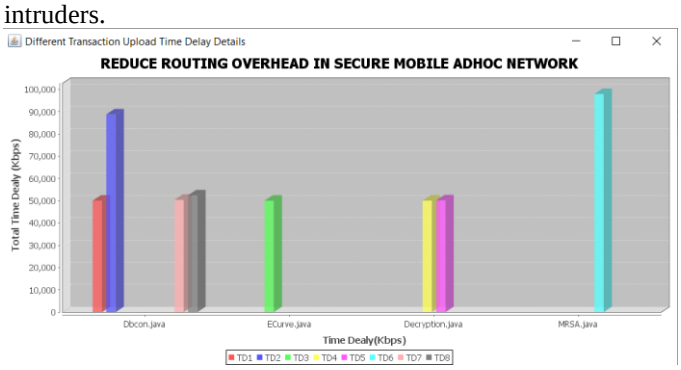

Figure 3: Upload transaction time delay

Figure 2. Has time delay in routing overhead. It clearly shows that secure IDS method have more overhead because of additional intruder check packet compared to existing A3ACK method with intruders.

4.1 METHODOLOGY

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. In this we also use the RSA algorithm for the encryption and the decryption of the data and to initialize the mac address we use the IP Address so that the

V. CONCLUSION

Mobile Ad hoc networks are easily affected by various types of network layer attacks. These attacks affect the performance of MANETs drastically. Our proposed Method to reduce the routing overhead in Secure mobile ad hoc network successfully reduce the routing overhead. Using this method the routing overhead will reduce

VI. REFERENCES

[1] Abdulsalam Basabaaa, Tarek Sheltamia and Elhadi Shakshukib, “Implementation of A3ACKs intrusion detection system under various mobility speeds,” Procedia Computer Science 32 , 2014, pp. 571 –578.

[2] Deepa Krishnan, “A Distributed Self-Adaptive intrusion detection system for Mobile Ad-hoc Networks using tamper evident mobile agents,” Procedia Computer Science 46,2015, pp. 1203 – 1208.

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, “EAACK— A secure intrusion detection system for MANETs,”

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013.

[4] Yi Ping, Jiang Xinghao, Wu Yue and Liu Ning, "Distributed intrusion detection for mobile ad hoc networks," Journal of Systems Engineering and Electronics, Vol. 19, No. 4, 2008, pp. 851–859.

[5] Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G, "Fuzzy based intrusion detection systems in MANET," 2nd International Symposium on Big Data and Cloud Computing, Procedia Computer Science 50, 2015, pp. 109 – 114.

[6] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, No. 3, March 2011.

[7] Adnan Nadeem and Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, Vol. 52, 2015, pp. 2047–2058.

[8] A. Esfandi, "Efficient anomaly intrusion detection system in adhoc networks by mobile agents," IEEE International Conference on Computer Science and Information Technology, July 2010.

[9] Sumit, S., D. Mitra, and D. Gupta, "Proposed intrusion detection on ZRP based MANET by effective kmeans clustering method of data mining," IEEE International Conference on Reliability, Optimization and Information Technology, 2014, pp. 156-160.

[10] Abirami, K.R., M.G. Sumithra, and J. Rajasekaran, "An enhanced intrusion detection system for routing attacks in MANET," IEEE International Conference on Advanced Computing and Communication Systems, 2013.

[11] Maria Alexandrovna Gorlatova: Review of Existing Wormhole Attack Discovery Techniques

[12] Piyush Agrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf