ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Trusted Dynamic Source Routing in MANETs

Siri, Deepika

PG Scholar, Dept. of C.S.E., PES College of Engineering, Mandya, India

Assistant Professor, Dept. of C.S.E., PES College of Engineering, Mandya, India

ABSTRACT: Mobile Ad-hoc Network has gained a capable ground in wireless network. Manet is a self-organizing framework with no brought together support or centralized system. The system topology in Manet is exceptionally powerful in view of regular node portability. This is the reason securing a Manet assumes an imperative part and it is additionally a troublesome assignment. Subsequently to improve the security in Manet, this paper extends dynamic source routing protocol, named as Trusted Dynamic Source Routing (T-DSR). With the guide of Intrusion Detection System(IDS) and trusted based routing attack discovery and disposal are completed in five stages in particular one-jump neighbour identification stage, flooding attack identification stage, Route discovery stage, information transmission stage and data dropping attack identification stage. The proposed T-DSR goes for identifying and isolating flooding assault, black hole attack and grey hole attack.

KEYWORDS: Mobile Ad-hoc Network, Intrusion Detection System, Trust Parameter, Multipath Routing, Flooding attack and Data Dropping attack detection and isolation.

I. INTRODUCTION

The current patterns in wireless networks have changed the lives of the individuals. The new remote innovations make a huge potential for the cutting edge Mobile Ad-hoc Networks (MANETs) and applications. The entry of remote advances, for example, Bluetooth and Wi-Fi empowers potential applications in the individual and neighbourhood situations. The MANET is a multi-hop distributed communication network comprising of a collection of mobile nodes that operate in a dynamic and self organized manner [1]. The system network changes progressively because of the arbitrary versatility of portable nodes without any predefined framework. Every portable node plays out the information sending just through single or multi-jump correspondence because of the restricted transmission range.

As a result of dealing with, it is a difficult task to gain skilled wireless intercommunication over mobile phones. Mobile ad hoc networks (MANETs) are collections of autonomous mobile nodes with links that are made or broken in an arbitrary way [2]. The structure changes constantly by virtue of the versatility of portable nodes. Routing protocols are utilized to locate an appropriate way to route the packets from the source to the destination. The outline of these routing protocols must be effective in spite of dynamic system conditions. In a MANET, the mobile node forming dynamic network topology and the nodes located within the transmission range of a node are called neighbours [1].

The neighbours transmit the data to different nodes inside the transmission area. A node transmits the information through an arrangement of various jumps (multiple hops) when it needs to send the information to a non neighbouring node or a far off node. Henceforth security is a challenging issue. The MANET needs to give a solid and secure planning over mission-fundamental conditions like hospital facilities and military applications. Many routing strategies have been proposed in Manets. These conventions work amazingly in conditions, where the versatile nodes are trusted and many of the techniques are based on single-path routing. If the attacker is successful is breaking the dedicated link, then the whole communication is lost. In other multi-hop routing strategies security issues are not fully considered. In other words, the existing multipath routing protocols are not designed with the aim of provisioning security in mind [3].

II. RELATED WORK

In [1] this paper, to reduce the hazards from malicious nodes and enhance the security of the network in MANET it extends an Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing protocol, named as Trust-based Secured Ad hoc On-demand Multipath Distance Vector (TS-AOMDV), which is based on the nodes' routing behaviour. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

proposed TS AOMDV aims at identifying and isolating the attacks such as flooding, black hole, and gray hole attacks in MANET. With the help of Intrusion Detection System (IDS) and trust-based routing, attack identification and isolation are carried out in two phases of routing such as route discovery and data forwarding phase. To improve the routing performance, the IDS integrate the measured statistics into the AOMDV routing protocol for the detection of attackers. This facilitates the TS-AOMDV to provide better routing performance and security in MANET. In [2] this paper, a wireless multi-hop network is taken into consideration, one of the important challenges is how to route packets efficiently. The availability of many intermediate nodes between a source and a destination results in having many optional paths/routes to follow. The challenge is to pick an optimal path that satisfies the needed performance requirements - this is the responsibility of the routing protocol. The focus of this depth paper is showing the unifications and distinctions of routing functions for the four multi-hop networks. In addition, a generic routing model is proposed that can be the foundation of the wireless multi-hop routing function and can be inherited by any wireless multi-hop routing protocol. As well, we present our view of the ideal wireless multi-hop routing protocol along with several open issues. In [3] authors surveyed the state-of-the-art of secure multipath routing protocols in WSNs and discussed a number of security issues related to multipath routing itself. The protocols have been categorized based on their security purpose and the security implementation approach they adopt. There are protocols that aim in securing the multipath routing procedure itself. Other protocols are designed to detect and recover from specific attacks while others support the operation of other security areas in WSNs. They have also overviewed the security requirements of sensitive applications that use WSNs and argue that mission- critical applications place importance differently than what constitutes the traditional security requirements chain. They have listed the reasons that drive the need for security in multipath routing promoting a better understanding of the risks that exist and also we have defined a new threat model that can be used to compromise routing in WSNs. Furthermore, authors discuss performance evaluation issues and propose a basic set of performance criteria that should be considered. Finally, authors discuss future directions and open issues. In [4] authors have seen the number of attacks happened in network layer and especially for gray hole attack. Due to its dynamic nature, MANET is prone to different limitations and weakness. To overcome this problem authors have to use a new technique which should be designed. Authors aim was to detect and mitigate the false node which is acting as a normal node, which is very hard to find out. But if a new approach is designed for detecting the attacker node, safety in the network can be ensured. Once security is lost in the network then the entire network will get failed. Gray hole attack ultimately decrease the concert of the network. The main goal of the gay hole attack should be the improvement of security and as well as the performance of the network. During the survey we addressed how the attack has been happened in the network layer. In [5] this paper, all routing security issues to which MANETs are vulnerable are being presented. A classification of security threats gathering selfish behaviours and malicious attacks was proposed. For countermeasures, authors have highlighted the main classes of solutions, and discussed advantages as well as drawbacks of the most popular propositions in the literature. MANET security constitutes a complex and challenging area, in which research is still being performed and will result in the discovery of new threats as well as the development of new countermeasures.

III. PROPOSED ARCHITECTURE

Step 1: One Jump Neighbour identification Module:

At first every node needs to recognize its initial neighbour i.e. One jump neighbour. When all the one jump neighbours are distinguished, information bundles can be sent. To recognize the neighbours we have utilized UDP "HELLO" protocol. At first every node will communicate a "HELLO" packet. Every one of the nodes which are in the transmission of MANET will get this packet and stores the source ip address. These neighbouring nodes will now unicast another "HELLO" packet to the source as an answer. Thus "HEELO" packets are transmitted between all the neighbouring nodes. Each recognized one jump neighbour are set with two parameters/factors i.e "Source-Trust" and "Router Trust" and instated to its default values i.e "1". IDS administration is sent at every node to screen every one of the exercises of each neighbouring node. All the TCP/UDP packets will be typified by IP Packets which holds sender and destination IP address. At the point when a hub gets a "HELLO" packet, IDS extracts the ip address of the source node from the system and stores it. The IDS is responsible for authorized communication An IDS encourages a total directing security by watching both the control packets and information packets that include in the steering.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Step 2: Flooding attack detection module:

Flooding is a Denial of Service attack which brings a system or administration around flooding it with huge measure of movement. The flooding attackers ordinarily floods massive RREQ packets into the system. They purposefully surge fake route request with non-existing goal IP and interepts the ordinary working of system. This disturbs the entire system. With a specific end goal to abstain from flooding attack, the T-DSR counts the packet produced at source hub. At the point when RREQ packets occur, the IDS retrieve the IP address of the source node in that packet, and add it to the RREQ counter of that source node from which request occurs. At that point it registers the Source-Trust parameter. Source-Trust Parameter is ascertained by,

$$\text{Source-Trust} = (\text{RREQ Count})^{-1} \quad \text{eq. (1)}$$

In the event if the Source-Trust estimation of a node is lesser than the threshold, then that node is checked RED in the kept up log to demonstrate it as malicious node. The entire RREQ packet from the relating source node is dropped (rather than rebroadcasting). No packets are transmitted or received from that node for further correspondence.

Step 3: Route discovery module:

With the assistance of trust based directing and IDS the attack recognition and attack isolation in T-DSR are done in two phases, for example, route revealing stage and information transmission stage. The trust gotten from IDS is connected while settling on choice about rebroadcasting the RREQ packet. This module utilizes DSR Routing Protocol to locate an ideal way between any source and destination nodes. Source node that does not have a route to the destination rather which has information to be sent to that goal, starts a RouteRequest packet. This RouteRequest is overflowed all through the system. Every node, after getting a RouteRequest packet, rebroadcasts the packet to its neighbours in the event that it has not sent it as of now. Before rebroadcasting the RREQ packets to its neighbours, every node checks the Source-Trust parameter estimation of the node that has communicated the RREQ packets. On the off chance if the Source-Trust parameter is lesser than the threshold, then the RREQ packet from that particular source is dropped (rather than rebroadcasting) to avoid the flooding attack. Each RouteRequest conveys a sequence number created by the source node and the way it has crossed. A node, after accepting a RouteRequest packet, checks the sequence number on the packet before sending it. The packet is sent just on the off chance that it is not a copy RouteRequest. Consequently, all nodes with the exception of the destination node forward a RouteRequest packet. A destination node, subsequent to getting the main RouteRequest packet, answers to the source node through the turnaround way the RouteRequest packet had crossed.

Step 4: Data transmission module:

This paper utilizes multihop data transmission protocol for effective information transmission. This procedure is done in view of the router-trust value to avoid data dropping attack. Once the ideal route has been found the data packets must be productively sent to the destination. At the point when any node needs to develop communication with different nodes which are out of range, the packets must be transmitted through at least one intermediate node. Before sending the data packets to the router, each node checks the router-trust parameter in estimation of all its neighbouring nodes. A neighbouring node which has most astounding trust value is chosen for information transmission and information is sent through that node. A period out clock named ACK_REC_TOT (Acknowledgment Reception Time-Out-Timer) is kept up for Acknowledgment Reception from the destination node.

Step 5: Data dropping attack detection phase:

Two types of data dropping attacks are identified ad isolated in this paper. They are black hole attack and grey hole attack. Black hole attack is most frequently caused attack which stops forwarding the packet which it has received. As a malicious node receives the RREQ packet, it will send a false RREP packet instantly with a modified high sequence number [4]. Destination node assumes that this is a valid route and starts forwarding the packets. Grey hole attack is a refined form of black hole attack, in which a malicious node drops only selected packets and forwards the others, depends on the source or the destination of packets [5]. The trust estimation of the node which goes about as router demonstrates the steady nature of data transmission through that point. IDS organization is passed on at each node to screen the neighbouring node that is decided for data transmission. IDS calculates Router-Trust Parameter by using,

$$\text{Router Trust} = \text{Received Packet Count/Forwarded Packet Count} \quad \text{eq. (2)}$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Before sending the data packet, every node checks the router trust in estimation of all its neighbouring nodes. The node which has the most essential trust value is regarded as trusted neighbour and this node is selected to forward the data to its neighbours. Similarly all the intermediate nodes follow the same procedure to forward the packets. If the trust regard is abnormal, the present data transmission through that malignant node is blocked. If the trust factor falls below the threshold, then that node is stamped RED in the table to exhibit it as a malicious node. Data transmission through that node is blocked. Thusly, another trusted router is looked over in the table to resume data transmission through it.

IV. CONCLUSION AND FUTURE WORK

In this survey, a Trusted Dynamic Source Routing (T-DSR) was obviously anticipated that it would complete security in MANET. The proposed T-DSR distinguishes and stays away from three sorts of attacks to be specific flooding attacks, black hole attack and grey hole attack. The IDS related with every node, performs two operations, for example, calculating the request packet generation rate at the source and calculates the ratio of number of packets received by a node and number of packets a node has successfully transmitted to destination. Source trust and Router trust parameters were successfully calculated and attacks were successfully detected and isolated.

REFERENCES

1. Abrar Omar Alkhamisi and Seyed M Buhari, IEEE 30th International Conference on Advanced Information Networking and Applications, 2016.
2. Binod Vaidya, and JaeYoung Pyun, JongAn Park, SeungJo Han, " Secure Multipath Routing Scheme for Mobile Ad Hoc Network", Third IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.
3. Eliana Stavrou, Andreas Pitsillides,"survey on secure multipath routing protocols in WSNs," Computer Networks, vol. 54, no.13,pp 2215–2238, 2010
4. Shanmuganathan, V., and T. Anand. "A Survey on Gray Hole Attack in MANET." IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), pp. 2250-3501, 2012
5. Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim. “Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks”, 2013 UKSim 15th International Conference on Computer Modelling and Simulation.

BIOGRAPHY

Siri is a final year student in Computer Science Department, PES College of Engineering, Mandya, India. She received Bachelor of Engineering (B.E) degree in 2015 from MIT college of Engineering, Mysore, India. Her research interests are Computer Networks, Artificial intelligence, Robotics, etc

Mrs. Deepika is working as Assistant Professor in Computer Science Department, PES College of Engineering, Mandya, India. She received Master of Technology (Mtech) degree in 2014 from NIE college of Engineering, Mysore, India. Her research interests are Computer Networks (wireless Networks), Computer Graphics, Network Security and Cryptography etc.