Detection of Isolation Attack using Olsr Protocol on Manet

C.Bhuvaneshwari, S.Sathya, S.Manasa Reddy

Abstract: Iin this paper, we propose a method to improvise the MANET security and defense which can oppose intrusion attacks to minimize intrusion. Sending data across networks are difficult in the Mobile ADHOC networks. The vulnerability of data transfer among the networks results in the vulnerability of the routing protocols. This can also ensure the isolation of the node that has been attacked in the MANET environment. The optimized link state routing OLSR helps in the finding and separation of the node that has been faked or intruded.

Keywords: MANET; security; defense; OLSR; routing protocols.

I. INTRODUCTION

MANET is used in the base nodes to through the broadcast process. Each sensor node is connected to the base station via which they transmit their messages. This process is energy engulfing and traffic intense. The MANET network contains sub networks which are limited in the transmission range of the wireless network. The sensors placed in one arena[1] may not communicate with the sensor in the neighbouring arena. The data collection from the sensor nodes thus proves to be expensive problem. Energy for the sensor in MANET comes from the other sensors. When an intrusion happens, one or other node is added among the MANET nodes. The fake node consumes high level of energy, which results in high energy usage of the MANET network. MANET works dynamically with self-created sets of independent nodal regions. The nodes doesn't have any specific task to perform by itself. They don't assume they're local to perform a particular task. Based on the network whereabouts, the nodes will make decisions independently using already existing network structure. ADHOC networks are known for changing the topology or the network of the system, which makes the nodes liable to less protection, combined with truancy of central admin and high dependent nodal cooperation. When the topology changes time and again, the boundary of the network is collapsed. Firewalls are out of scope to operate in these regions. The securing of MANET network is thus highly threatened issue. The content and context in the MANET environment is vulnerable to data breaches. Eavesdropping or injection of messages into this space is really very difficult. The attacks are of two types:

1. Active attacks
2. Passive attacks

Passive attacks doesn't have liability to inject any messages but doesn't listen to the channel. Passive attack discovers the important data and barred the network from developing new traffic in the channel. The active attack includes messages into the network but results in the modification of messages like insertion and deletion. In MANET, the DOS attacks, disclosure attacks and impersonation of the users can be major issue. Performance [2] of a network is highly threatened and degraded by the denial of service attack which is degraded by throughput. Performance of the network is reduced by the denial of the service on the malware nodes, their traffic pattern and throughput. The wireless network throughput is reduced by the DOS attacks in the system. The network resources are threatened and the data is put to fall. The data in the routing protocol can overflow in some instances. The main objective of the DOS attack is to temporarily or permanently disturb the services which limit the number of users accessing the system. The attack aims at unabrupt usage of the network which makes in incapable of providing normal service which reduces the bandwidth and puts the target or destination port under risk. The stream of packets which corrupts the network is the key for these attacks to enter the victims system. It can also deny access of the clients who are promptly using the system. In this paper, we propose a system using the OLSR (Optimized link state routing) protocol which helps in reducing the vulnerability of the data in the mobile ADHOC networks. The security and defense in the proposed system is high that the data cannot be stolen and the fake intruded node can be found easily.

II. RELATED WORKS

A MANET may be a most promising and quickly growing technology which is predicated on a self-organized and quickly deployed network. Due to its nice options, MANET attracts completely different world application areas wherever the networks topology changes terribly quickly. However, in several researchers try to get rid of main weaknesses of MANET like restricted information measure, battery power, procedure power, and security. Though plenty of work underneath progress during this subjects significantly routing attacks and its existing countermeasures. the prevailing security solutions of wired networks cannot be applied on to MANET, which makes a MANET rather more liable to security attacks.

Revised Manuscript Received on June 15, 2019

C.Bhuvaneshwari, Cse, Ve L Tech Rangarajan Dr.Sagunthala R&D Institute Of Science And Technology.

S.Sathya, Cse, Vel Tech Rangarajan Dr.Sagunthala R&D Institute Of Science And Technology.

S.Manasa Reddy, Cse, Vel Tech Rangarajan Dr.Sagunthala R&D Institute Of Science And Technology.

In this paper, we've got mentioned current routing attacks in MANET. Some solutions that believe cryptography and key management seem promising, however they're too costly for resource constrained in MANET. They still not good in terms of trade-offs between effectiveness and potency. Some solutions in work well within the presence of 1 malicious node, they might not be applicable within the presence of multiple colluding attackers. Additionally, some could need special hardware like a GPS or a modification to the prevailing protocol.

The malicious node(s) will attacks in MANET victimization completely different ways, like causation faux messages many times, faux routing information, and advertising faux links to disrupt routing operations.

III. EXISTING SYSTEM

We have seen large scale attacks on various high profiles services on the web. The existing systems use many active techniques which are used to transfer data packet among the regions. The routing by reactive routing doesn't concentrate on communicating to all nodes. But proactive communication [3] communicates to all nodes. In fictitious communications a fake node is created. The fake node communicates to all the other nodes in the MANET network. The attacker, for this reason, chooses to enter using a node. All nodes are communicating to other through a region. The main problem that we face is that of the support given to the fictitious nodes. The attacker thus enters into the region, steals the available information and incorporates risk into the nodes.

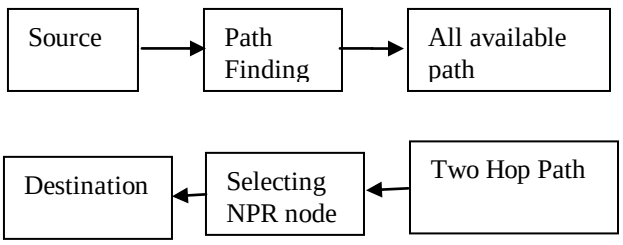
IV. PROPOSED SYSTEM

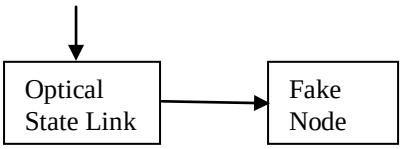
Considering the number of attacks that originate by faking the node in the transmission of data among the MANET network nodes [4], we propose a system which can mitigate the amount of energy utilized by increasing security and defense of the system by isolation of the node. We make use of OLSR, Optical Link Stating Router, which can segregate the affected node from all the other healthy nodes.

The proposed system is been divided into four modules in the paper. The first module concentrates on the network formation by finishing the multipoint relaying. The second module is all about receiving the data packets using OLSR through the MPR. The third module helps to isolate the nodes without attacking it in the network. Fourth and final nodes, concentrates on the eradication of the fake node from the network.

I. ARCHITECTURE DIAGRAM

The Architecture of the above proposed system is depicted as follows:





V. MODULES

As discussed above, to track the attack and intrusion in the data nodes, the following four methods have been used by us in the proposal:

Network Formation

In this module, the network topology is maintained and the OLSR focusses in selecting the nodes as MPR. The TC messages are timely updated as the MPRs. The shortest distance between the nodes are taken into consideration for calculation.

Finding the Best Multipoint Relaying (MPR)

OLSR receives the MPR [5] selector packets with the help of TTL systems. The 1-hop and 2-hop neighbors are categorized to select the MPR. The minimal MPR set is rolled to play the topology related control messages.

Isolation without Detection Attack

In the network, the fake node is used only to select its next adjacent node. It tends to set up a virtual link by a HELLO message. The MPR target node will select the attacker. The TC messages are always generated and transmitted by the fake nodes which sets out to attack.

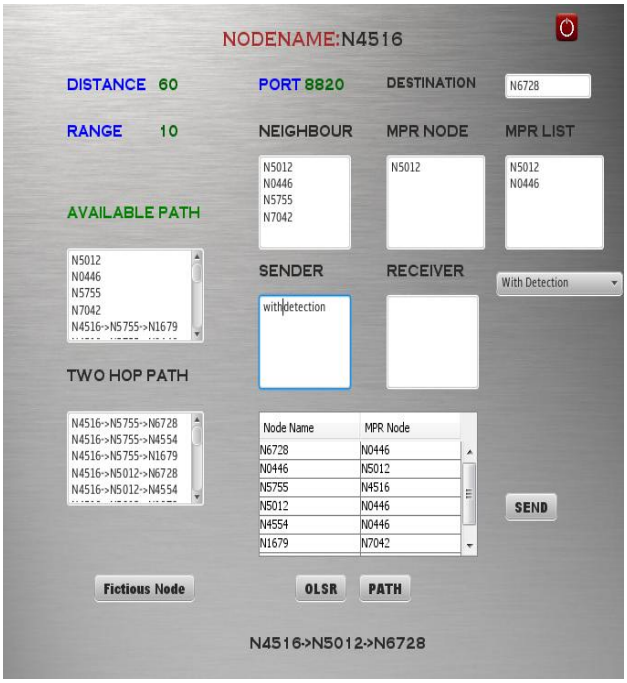
Isolation Attack with detection

The fictitious nodes as discussed, attacks only its adjacent node. The communication doesn't happen in any other node. Hence, the OLSR table will update its information from time to time, which prevents the attack and security breaching from one node to the other.

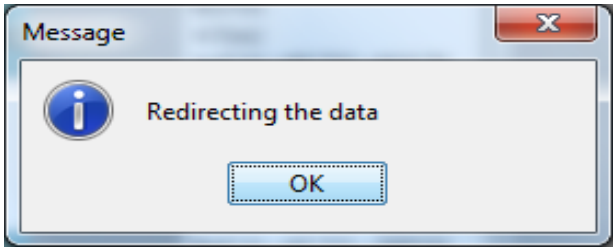
The four modules are used to track and locate fictitious nodes in the system. After location, the OLSR sends broadcast message to other nodes in the system exposing the fake node.

VI. EXPERIMENTAL RESULTS

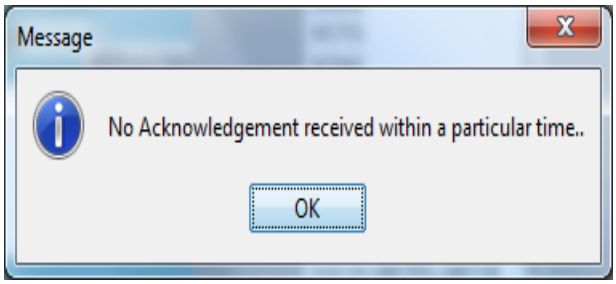
We carried out our experiment in the above set set-up and the following is the workflow of how the system actually works in detecting the fake nodes.



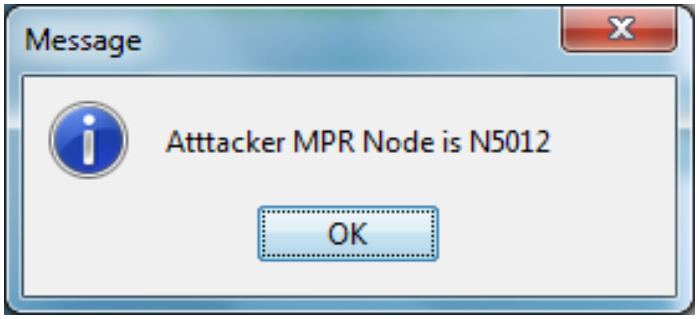
This is the experimental set up when the sender sets out to detect the node that has been faked. The main objective is to find which node is the attack node and to intimate to other nodes in the network.



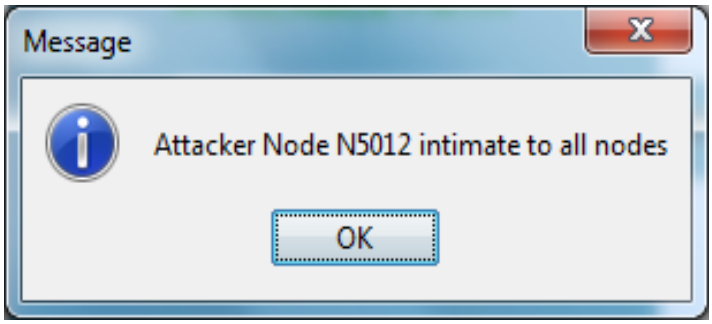
Once the node is asking to send messages, the data is redirected to the nodes in the network. It tries to get acknowledgement from the network.



If no acknowlegement is received within the particular timed interval, then the node is definitely fake.



The attacker node is thus determined, and in the following action, the message about the attacker node is intimated to all the other nodes in the network.



Hence, the intrusion attack and fake nodes can be easily detected with the proposed method using OLSR.

VII. CONCLUSION

In the web based applications and networks, we have seen large number of attacks that can intrude the privacy of the system. These are either main in the middle or intrusion which can change the data packets and messages sent from one point to the other.

Hence, in this paper, we have formulated a method to prevent DOS attacks on various nodes that are there in the MANET network. The nodes are checked for fictitious nodes which tend to be the attacker node spreading malware information and messages. MANET security and defense is drastically improved by the method that we have proposed in the paper. The data sent across the networks are not tracked and is authenticated. The use of OLSR ensures the isolation of the fake node from that of the nodes that are secure in the system. This on the whole, reduces the intrusion rate in the system.

REFERENCES

1. Dr.M.Sreenivasan, P.Rajikumar, "A Study on Routing Protocols of MANET in Wireless Sensor Network," SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) – volume 2 Issue 3 May to June 2015.
2. Ahmed Al-Maashri Mohamed Ould-Khaoua, Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic.

3. Surendra H. Raut, Hemant P. Ambulgekar, "Proactive and Reactive Routing Protocols in Multihop Mobile Ad hoc Network," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
4. S. R. Das, C. E. Perkins, E. M. Royer and M. K. Marina, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," in IEEE Personal Communications Magazine, special issue on Mobile Ad Hoc Networks, Vol. 8, No. 1, pp. 16-29, Feb 2015.
5. Juan Antonio Cordero, "MPR+SP: Towards a Unified MPR-Based MANET Extension for OSPF," Proceedings of the 44th Hawaii International Conference on System Sciences – 2011.
6. R Bhuvaneswari,N Balamathy, S Premalatha, V Manimozhi, S Parvathi, A Kumaresan "An Improve Performance, Discovery and Interruption of Sybil Attack in MANET" Middle-East Journal of Scientific Research 23 (7): 1346-1352, 2015

AUTHORS PROFILE

C.BHUVANESHWARI, M.E, CSE ASSITANT PROFESSOR VEL TECH RANGARAJAN DR.SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY,AVADI, HENNAI-600062.IEEE WIE MEMBERSHIP.

S.SATHYA B.TECH, CSE, VEL TECH RANGARAJAN DR.SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY,AVADI, CHENNAI-600062.

S.MANASA REDDY B.TECH, CSE VEL TECH RANGARAJAN DR.SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY, AVADI, CHENNAI-600062.