ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs19822019.pdf
https://doi.org/10.30534/ijiscs/2019/19822019

Gray-Hole Attack Minimization for Ad-Hoc Networks Using Contradiction

AthiraHarikrishnan[1], JasmineJoseph[2], Fathima Manzoor[3], Tinu Thomas [4]
[1]MLMCE, Indian,athirahari@gmail.com
[2]MLMCE,Indian,jasjoseva@gmail.com
[3]MLMCE, Indian,fathima@gmail.com
[4]MLMCE, Indian,tinu.thomas@manglam.in

ABSTRACT

Each device in a Mobile Ad-hoc Networkcan move independently in any direction, and will thereforefrequently changes its links to other devices. Each must forward traffic distinct to its own use, and therefore be a router. MANETs has a routable networking environment on top of a Link Layer ad hoc network and it is a kind of wireless ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. Gray hole attack is the kind of denial of service attack. In this attack, the router which is mesh behave just not well and a subset of packets are forward and handle by receiver but leave by others. An algorithm is used to detect the malicious nodes using the contradiction to minimize the gray hole attack.

Key words : MANET, Ad-hoc network, Service attack

1. INTRODUCTION

Mobile ad-hoc network is wireless network which is able to transmit the information from source to destination. Mobile ad hoc network is can described as the network that has many free and autonomous nodes.The mobile fragments can be arrange in the different methods and operated with no strict top-down network administration. To establish communication between the sender and the receiverit does not require any fixed wired network. The network is able to establishing by the use of transmitter, receiver, processor and the battery. The mobile ad hoc network used in many real time applications like military service, disaster management, air pollution monitoring etc. Mobile ad-hoc network has some security limitationsdue to the open communication media. In the MANET there is possibility of information leakage in the network. Major threats in the mobile ad-hoc network isGray-hole attack. In gray-hole attack selective dropping of the packets is happened, the information cannot able to further transmit after packet dropping. Attacker is able to cunningly manipulate routing.

2. BACKGROUND

We took gray-hole attack minimization using contradiction as our research area, because security is an important issue in the internet world.

[1] In VANETs by using an automatic optimization toolthe optimal parameter tuning of OLSR routing is done. Optimization strategy based on coupling optimization algorithms is used to do this task. By comparing the optimized OLSR configurations with standard one in RFC 3626 and with human expert configurations found in the present era of the art. The validated optimized configurations found by comparing with each other and with the standard tuning in RFC 3626 and studying the performance in the terms of QoS over 54 VANET scenarios.While using the automatically tuned configurations on the VANET scenario employed during the optimization task all the packets are delivered correctly increasing the PDR regarding the standard configuration by 8.34% and between 6.66% and 28.57% regarding the other expert-defined configurations. The optimized configurations dramatically reduce the routing load generated by OLSR.According to these results, the automatically tuned OLSRs by using met heuristics are more scalable than the standard version because they are less likely to be affected by medium access and congestion problems. Specifically, the PSO obtained configuration obtained the best tradeoff between the QoS and routing workload.

[2] The wormhole attack is a serious threat in wireless networks against many ad hoc network routing protocols and location-based wireless security systems. Most of the existing ad hoc network routing protocols without mechanism to defend against the wormhole attack is unable to find routes longer than one or two hops, disrupt thecommunication. The general mechanism called packet leashes for detecting and defending against wormhole attacks and to implement temporal leashes presented in the design and performance analysis of a novel efficient protocol called TIK, which provides instant authentication of received packets.

[3]A HADOF is defend against routing disruption attacks launched by inside attackers, which can be implemented upon the existing source routing protocols. HADOF can capable of adaptively adjusting routing strategies according to network dynamics and nodes' past records and current performance. It can handle various attacks launched by malicious nodes, such as black hole, gray hole, and frame-

up. The HADOF introduces little overhead for the existing routing protocols, and is fully distributed.

[4] The routing security issues of MANET analyzes the type of attack in the black hole this can easily deployed against a MANET, and propose a feasible solution for it in the AODV protocol. The limitation of the proposed method is it works based on an assumption that malicious nodes do not work as a group.

3. PROPOSED SYSTEM

The main goal of the proposed system is that it is able to minimize the gray hole attack. During the gray hole attack there is a chance of malicious nodes should confuse the sender node that it is able to send the information quickly to the destination node. If the sender sends the information to the malicious node the information can be manipulated by the attacker. It causes a serious security threat. In order to avoid the gray hole attack an algorithm can be used in this context to find the malicious node from the original intermediate node. The spanning tree algorithm is used to find the contradiction and the attacker node.

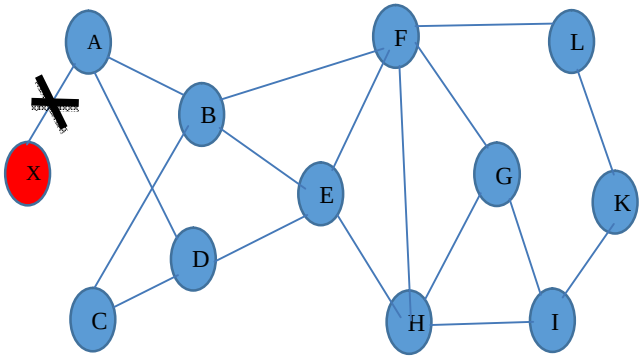

Figure 1: Gray hole attack

In figure 1 A is the source node and H is the destination node. B,D are the neighbouring node. X is the malicious node that have the capability to manipulate the data.

A is the source node wishes to send the message to destination node H through neighbouring node. B and D are the neighbouring nodes of A.

X claims that by passing information through its neibouring node that is a non-existent node,the message reaches the destination fast.B claims that by passing information through its neibouring node E that is an existent node, the message reaches the destination fast.Here the idea contradiction arises.

We are using BFST and MST for identify the attacker by the contradiction between nodes, then we can send our message from source to destination without any presence of malicious code.

4. RESULT

In our project, we are finding presence of an attacker. If the attacker is present in the network, immediately dropping the path to the attacker. For this BFST and MST algorithm are used on the basis of contradiction idea.

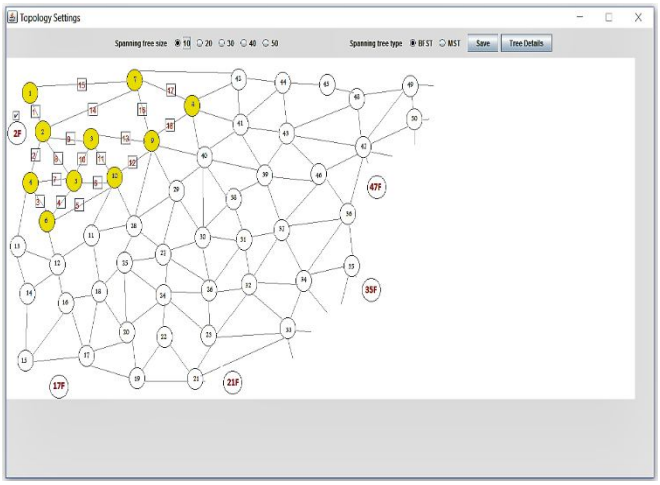

Figure 2: Topology setting

The maximum capability of spanning tree size is 50 in our project. But in figure 2 we are setting the spanning tree size as 10.

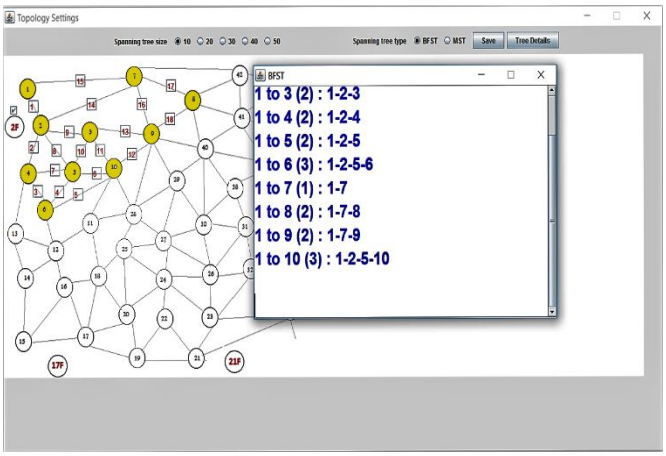

Figure 3: Tree details of BFST

Figure 3 represent the tree details of BFST (Breadth First Search Tree), it shows the shortest possible path to reach the destination.

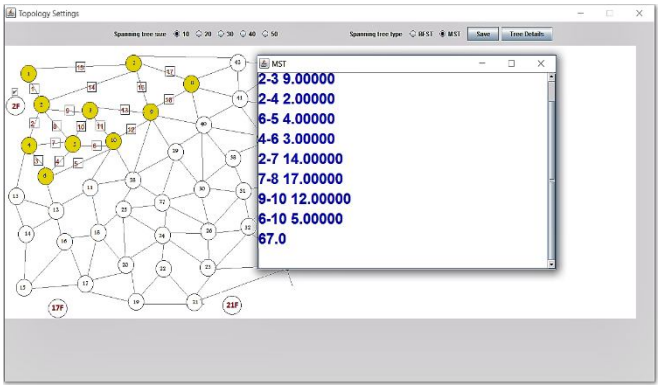

Figure 4: Tree details of MST

Figure 4 represent the tree details of MST (Minimum Spanning Tree), possible path to reach the destination is identified using weights in the intermediate path.

5. CONCLUSION

This paper presents algorithms for networks like MANET, IoT, VANET etc.. for mitigating gray hole attack.Using BFST and MST we are able to identify the attacker node. Through these two algorithms we are finding the shortest path, we can drop the path where attacker node found. to attacker. After finding the attacker node we can drop the path to that attacker.

In our paper we are using contradiction idea for finding the attacker node and original node to transmit the message.

REFERENCES

1. J. Toutouh, J. Garcia-Nieto, and E. Alba, "**Intelligent olsr routing protocol optimization for vanets**," IEEE Transactions on Vehicular Technology, vol. 61,no. 4, pp. 1884–1894, May 2012. https://doi.org/10.1109/TVT.2012.2188552
2. Y.-C. Hu, A. Perrig, and D. B. Johnson, "**Wormhole attacks in wireless networks**," IEEE Journal on Selected Areas in Communications, vol. 24,no. 2, pp. 370–380, Feb 2006. https://doi.org/10.1109/JSAC.2005.861394
3. W. Yu, Y. Sun, and K. J. R. Liu, "**Hadof: defense against routing disruptions in mobile ad hoc networks**," in Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., vol. 2, March 2005, pp. 1252–1261 vol. 2.
4. H. Deng, W. Li, and D. P. Agrawal, "**Routing security in wireless adhoc networks,**" IEEE Communications Magazine, vol. 40, no. 10, pp. 70–75, Oct 2002. https://doi.org/10.1109/MCOM.2002.1039859