International Journal For Technological Research In Engineering
Volume 4, Issue 9, May-2017 *ISSN (Online): 2347 - 4718*

RESISTANCE OF BLACKHOLE ATTACKS ON MANET'S WITH THE SUPPORT OF MODIFIED DYNAMIC SOURCE ROUTING PROTOCOL

Bhavana K S[1], Ravi P[2]
[1]PG Scholar, [2]Assistant Professor
Department of CSE, VidyaVardhaka College of Engineering, Mysuru, India

Abstract: The most recent technology which is being an interesting topic in Mobile Ad-hoc Networks. Due to the enhancement in the field of technology there is a vast improvement in the field of communication, which led to the changes in the medium from, wired to wireless medium. One of them in mobile ad-hoc network. The wireless medium which has many advantages like low resource consumption, high performance, capability and so on. Since it is a wireless there is a security breach in the network. The security threats may include blackhole attack, gray hole attacks & other attacks. These attacks cause denial of services which decreases the performance. This paper includes the mechanism called as blackhole resisting mechanism, which includes neighbor identification fake request transmission, original request transmission, route discovery and optimal route selection. By adopting these schemes we can detect the blackhole nodes & exclude them prevent the attack.

Keywords: Manets, Blackhole attack, Dynamic Source Routing Protocol, Blackhole Resisting Mechanism.

I. INTRODUCTION

The mobile ad-hoc network is a collection of portable nodes which form a network without any help of the administrator and also 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.

In these types of network the nodes act as both source and destination. The data is transferred using the intermediate nodes. The vulnerability is a main issue in security system in the networks. MANET is more vulnerable than a wired network because it has no centralized system to monitor, dynamic topology, cooperativeness, scalability and so on. Due to the elasticity of the Manets they can be easily prone to attacks like blackhole or grayhole attacks. Blackhole attack is usually active in the network layer. Here first the attacker sends the fake routing information claiming that he has the original or valid route information regarding the destination, due to this the other intermediate nodes in the networkincludes this node in the route and passes the packets to this malicious node. Once this malicious node receives the packet instead of forwarding them it drops the packet which causes the denial of service and thus a blackhole attack occurs. The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.

DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network.

II. RELATED WORK

The security issues in the Manets still exist since it's a wireless network. In Manet it is difficult to find the malicious node. Few changes are required in the existing system that is being used [1].In the existing system the system uses the AODV protocol which uses a blackhole resisting mechanism which depends on some threshold and some timers which are used to calculate whether the node is malicious or not. "Preventing Blackhole Attacks in Manets using Secure Knowledge Algorithm" has a technique in which the promiscuous mode to ensure data delivery to receiver node [2]. "Securing Manet against Cooperative Blackhole attack and its Performance Analysis-A Case Study" has an approach in which the malicious intruder will be removed through malicious node detection system through collecting some information [3].The paper "Modified DSR Protocol for Detection and Removal of Selective Blackhole Attack in Manets" has an approach where the first node picks up the shortest path for transmission [4].

III. PROPOSED SYSTEM

The Enhanced Dynamic Source Routing Protocol Support for the Resistance of Blackhole Attacks on MANET's proposes a unique approach to detect the malicious node which causes the blackhole attack. It uses the DSR and Self Protocol Trustiness.

It operates in five steps:-

- One Hop Neighbor Identification.
- Fake Route Request Transmission.
- Node Classification.
- Route Discovery
- Optimal Path Selection.

A. One Hop Neighbor Identification

The one hop neighbors are identified by sending a hello broadcast request in the network.

B. Fake Route Request Transmission

Each node has to monitor his neighbors. In this step each ode will send a random fake request generated from non-existent source to non- existing destination at a random interval of

time which has been set to the following limits.

MIN NORMAL 30 s MAX NORMAL 90 s
MIN TRUST 90 s MAX TRUST 150 s

C. Node Classification

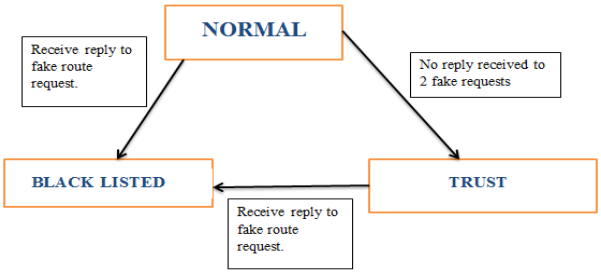

Fig: 3.1 Node Classification

Based on the replies received by the source or the intermediate node the node which replied to the request will be either put on to blacklist or it will be put on the trust based on the maximum trust values assigned to it which is MAX_TRUST=2. If the value is decremented and becomes zero then it will be put under blacklist.

D. Route Discovery

Using the Dynamic Source Routing (DSR), the path between the source and the destination is found out. Here it also checks for the source address and destination address and compares them with the values recorded in the table and if it is found in the blacklist then it doesn't select in the path between and the source and destination, else if it is in trust list then it will include in the path.

E. Optimal Route Selection

Once the paths are found out, this will select the best or the optimal path which is free from malicious node or the blackhole node for the data transfer.

The following figure shows the procedure:

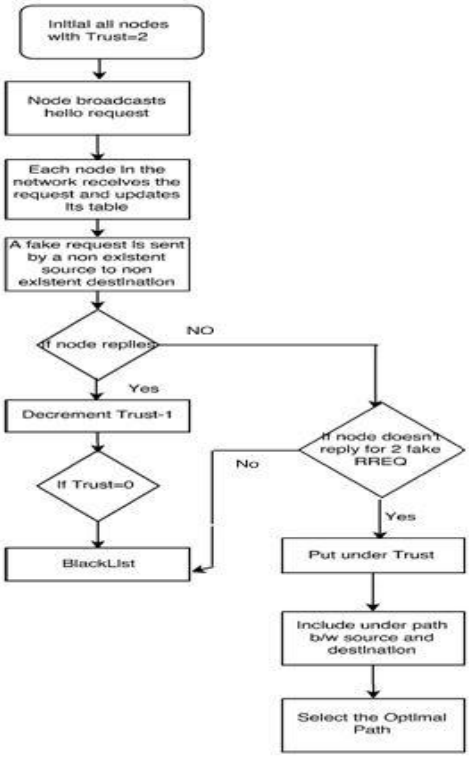

Fig 3.2: Process Flow

IV. CONCLUSION

Many of the researchers have implemented many ways to deal with the malicious node. This approach is to resist the blackhole attacks and prevent the loss of data and denial of service. The proposed scheme has been implemented practically in real time to find out the results. This approach increases the adaptability to resist the blackhole attack and also this approach reduces the resource consumption by the use of enhanced DSR protocol and Self Protocol Trustiness.

V. FUTURE WORK

The future work is expected to be done on the various routing protocols which will be able to deal with the various security issues in the Manets.

REFERENCES

[1] Mohamed A Abdelshafy and Peter J King. "Resisting Blackhole Attacks on MANETs". Consumer Communications & Networking conference on IEEE, 2016.

[2] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015.

[3] Bhandare, A. S., and S. B. Patil. "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study." Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on. IEEE, 2015.

[4] Moharlalpriya M and Krishnamurthi I. "Modified DSR protocol for detection and removal of selective blackhole attack in Manet", 2014 Comput.Electr.Eng.,40: 530-538.

[5] L. Tamilselvan and V. Sankaranarayanan. Prevention of blackhole attack in MANET. In 2nd International Conference on Wireless Broadband and Ultra-Wideband Communications, pages 21–21, Aug 2007.

[6] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.

[7] Kshirsagar, Vishvas, Ashok M. Kanthe, and Dina Simunic. "Analytical approach towards packet drop attacks in mobile ad-hoc networks." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.

