TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4499 - 4502

A Novel Approach to Prevent Black hole Attack in MANET

Nandhini.S[1], Dr.JeenMarseline K.S [2]

[1,2]Assistant Professor, Sri Krishna Arts and Science College, Coimbatore

Article Info
Volume 82
Page Number: 4499 - 4502
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 22 January 2020*

Abstract

Mobile Adhoc Network (MANET) is a set of independent nodes which are capable of self-configuring and self-healing without any centralized infrastructure. The nodes in a MANET are mobile and are able to communicate among themselves over a wireless infrastructure. These nodes are likely to be affected by various types of attacks. Black hole attack is one among them and is a Denial of Service attack. In this attack, a hostile node drops all the packets which are to be sent to the destination instead of relaying them. Here we analyze black hole attack in AODV routing protocol and propose an efficient method of preventing the attack.

Key Words :*AODV routing protocol, Black hole attack, Denial of Service Attack, MANET*

INTRODUCTION

Mobile Ad-hoc Network is a set of autonomous nodes without any centralized infrastructure. Every node in the MANET carries the packets to other nodes in the network [1]. The nodes of MANET are self-configuring and self-healing. As no centralized infrastructure is required they are very useful in applications like natural disaster management. In case of emergency rescue operations, these nodes can quickly form a network without establishing any physical communication network. This results in establishment of a communication network at a lower cost.

The problem with this kind of arrangement is that the nodes are prone to various types of attacks. Two major categories of such attacks are passive attacks and active attacks [2]. In a passive attack the system is monitored for vulnerabilities but data are not altered. In an active attack data are deleted or modified with the help of information gained during passive attack. Black hole attack is a kind of active attack in which a hostile node acts as a genuine node by sending false information to other users in the network. Thus the hostile node drops every vital information it receives instead of forwarding them to the destination [3].

A routing protocol is a set of rules which mentions how routers can communicate among themselves in order to find the optimal path so that the packets can be delivered to the destination on that path. Routing protocols can be categorized into reactive, proactive and hybrid [4]. In proactive routing protocol, all the nodes in the network have their routing information like their neighbors, reachable nodes and the number of hops. In reactive or on-demand routing protocol, the route for sending the packets are formed on demand and there is no need to maintain any status information as that of proactive protocols. A hybrid routing protocol is a mechanism in which both proactive and reactive strategies are applied. When a node wants to identify its neighbors within a zone, it

January - February 2020
ISSN: 0193 - 4120 Page No. 4499 - 4502

follows proactive scheme and if it wants to find the route between two nodes in a specific zone, it follows reactive scheme.

AODV is a reactive kind of routing protocol which establishes the route between the source and destination only when the need arises and so it will not maintain any routing information in its routing table. It is a widely used protocol in MANETs [5]. The advantage of AODV is that it maintains only next hop information and thus does not use source routing information. But the disadvantage is that it may lose the shortest path during the discovery of the path.

In this paper, we analyze various schemes for detecting black hole attacks in MANETs and propose a novel approach to prevent such attacks in AODV protocol.

II. REVIEW OF LITERATURE

There are many researchers working on the area of detection and prevention of black hole attacks. AbdellahNabou and My DrissLaanaoui and Mohammed Ouzzif [1] evaluated how two routing protocols perform when a black hole attack occurs in MANET. They have taken one proactive and one reactive routing protocol namely OLSR and AODV for evaluation purpose and analyzed the effect of black hole attack in a mobile environment. They have concluded that AODV routing protocol is more prone to black hole attack.

Samia Khan and MohdFadleeA.Rasid and FazirulhisyamHashim and ThinagaranPerumal [2] proposed a method to reduce the ill effects of two types of attacks namely black hole and Distributed Denial of Service attacks. In the propose method, AODV protocol is modified using MAC authentication and symmetric encryption. They proposed a solution to secure the routing path and also to authenticate all the nodes available in the network.

VentrapragadaSreePooja and NagulapallyManisha Reddy and TodupunooriRohit and S Sudeshna [3] used cryptographic techniques to provide security and reliability to data packets. Taku Noguchi and Mayuko Hayakawa [5] proposed a new threshold-based prevention mechanism using multiple RREPs. Their simulation result shows that throughout and packet deliveries are improved when compared to existing methods.

Gibson CHENGETANAI [6] proposes a solution to reduce collaborative black hole attack in MANET by checking the sequence number during the process of route discovery. Amar Taggu and AbhishekMungoli and AniTaggu [7] propose an algorithm which is used to detect the intrusion in the system when a black hole attack occurs. They have used a light-weight mobile agent which detects these problems.

Ida Nurcahyni and HelmiHartadi [8] made a comparative study of AODV and DSR protocols. After analyzing QoS parameters they concluded that AODV is better than DSR routing protocol.

Fan-Hsun Tseng and Li-Der Chou and Han-Chieh Chao [4] made an extensive survey on black hole attacks. They analyzed various proactive and reactive protocol schemes and suggested a hybrid protocol scheme to minimize the attacks.

III. ROUTING PROTOCOLS

In MANETs, every node helps to carry the information along the path from the first to the last host to enable communication in the network. This helps to choose the shortest optimal path in order to deliver the packets to the intended recipient. There are three different categories of routing protocols available. They are proactive or table driven, reactive or on-demand and hybrid [9].

1.1 Proactive or table driven protocols

These types of protocols send the packets to the intended recipient according to the information stored in a routing table. This table will have several details, like neighbors of the node, the optimal path and number of hops from the current node to the

January - February 2020
ISSN: 0193 - 4120 Page No. 4499 - 4502

destination. Every node maintains this routing table in the network and it has to keep on updating this table to find the optimal path and to send the packet to the correct receiver. The benefit of this scheme is that the routes are already discovered and sufficient information is kept in the table. Whenever a node wants to transmit data packets, this table is referred. But a major issue may arise in this scenario. The maintenance of the table is an overhead especially when the number of communicating nodes is high. Optimized Link State Routing Protocol (OLSR) belongs to this category of protocol.

1.2 Reactive or on demand routing protocols

In this scheme, the routes to send the packets are discovered only on demand. The routing information is not stored in its table. When this scheme is used, the routing overhead becomes less, as maintenance of static routing information is not necessary. But there is a problem in this procedure. It may lose the shortest path during the process of finding the route. An example protocol which falls under this category is AODV.

1.3 Hybrid routing protocols

It is a combination of both reactive and proactive features of protocols. The routing follows proactive mechanism for short distance and reactive mechanism for long distance routes. The advantage is this approach is that it eliminates the disadvantages of both the methods and includes the advantages of the two methods. Zone Routing protocol (ZRP) is a kind of hybrid protocol.

IV. BLACK HOLE ATTACK

The process of finding the route for an AODV protocol is described as follows: When a node in the network wishes to transmit information, it initially broadcasts a message in the network as a route request packet (RREQ). The node which receives this request, checks its routing table. It checks whether there is an entry for the intended recipient node. If there is an updated or fresh entry in its routing table, it reacts to this message by issuing a route reply packet (RREP). In order to know the latest path to the destination, the protocol uses a destination sequence number (DSN). The path information in a node is updated only if the sequence number of the current packet received is greater than the previous sequence number stored in it. The presence of a hostile node in this scenario prevents the data packets from reaching the destination. When RREQ is sent by a node, the hostile node replies back with a false RREP with higher DSN and one hop count. Upon receiving this, the data packets will be routed to the hostile node instead of the genuine one. Once the hostile node starts receiving the data packets, it will not route these packets to the correct receiver, instead it drops the packets. This situation ultimately results in Denial of Service attack [10].

V. PROPOSED SOLUTION

There are several methods available to find the existence and avoidance of black hole attacks in the literature. The solutions fall under the following categories: Cryptographic methods, Overhearing, Acknowledgement, Cross checking, Clustering, Intrusion Detection System, Sequence number threshold based, Trust based and Cross layer. Each of the above categories of solution has both advantages and disadvantages. In our proposed method, we try to overcome the disadvantages of the currently available methods. In order to alleviate the black hole attack in the network, every node in the network contains a routing table which has information about the neighbor and updated routing information. In addition to this one more RREQ packet, called PRIOR-RREQ has to be added which will exist in the table for a fixed time interval. Before the actual RREQ packet is broadcast in the network, this PRIOR-RREQ will start the route discovery process. If any hostile node exists in the network, it will immediately respond to this PRIOR-RREQ packet without consulting its routing table. The PRIOR-RREQ packet will then check the sequence number of the destination and the hop

January - February 2020
ISSN: 0193 - 4120 Page No. 4499 - 4502

count. If the node gets an immediate RREP packet with high DSN and hop count as 1, the node number is stored in its routing table and marked as hostile node. Once it is marked, further RREP packets from that node are discarded. After this step, the node which marked the hostile node entry broadcast that message in its routing table to the rest of nodes in the network so that all the hosts in the network knows the presence of hostile node. Thus the remaining nodes also start avoiding the malicious node thereby preventing the black hole attack.

VI. CONCLUSION AND FUTURE WORK

Due to the autonomous nature of nodes in the MANET, the nodes are prone to several attacks. The black hole attack is a well-known security attack under AODV routing protocol. Hence to find out and avoid such attacks we proposed a new threshold based method which identifies the malicious node and prevents the denial of service attack (DoS) in the network. Our next work will focus on validating the proposed method using simulation experiments and to improve the AODV routing protocol to make it more reliable and secure against the black hole attack.

REFERENCES

[1] Abdellah Nabou, My Driss Laanaoui, and Mohammed Ouzzif, “Evaluation of MANET Routing protocols under Black Hole Attack Using AODV and OLSR in NS3,” 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 2018, pp. 1-6.

[2] S. Khan, F. Hashim, M. F. A. Rasid and T. Perumal, "Reducing the Severity of Black Hole and DDoS Attacks in MANETs by Modifying AODV Protocol using MAC Authentication and Symmetric Encryption," 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN), Kuching, 2018, pp. 109-114.

[3] Ventrapragada Sree Pooja,Todupunoori Rohit,Nagulapally ,Manisha Reddy,S Sudeshna , “Mobile Ad-hoc Networks Security Aspects in Black Hole Attack,”Conference: 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)

[4] Fan-Hsun Tseng, Li-Der Chou1 and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Human-centric Computing and Information Sciences 2011, 1:4

[5] P. N. Patil and A. T. Bhole, "Black hole attack prevention in mobile Ad Hoc networks using route caching," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, 2013, pp. 1-6.

[6] G. Chengetanai, "Minimising Black Hole Attacks to Enhance Security in Wireless Mobile Ad Hoc Networks," 2018 IST-Africa Week Conference (IST-Africa), Gaborone, 2018, pp. Page 1 of 7-Page 7 of 7.

[7] A. Taggu, A. Mungoli and A. Taggu, "ReverseRoute: An Application-Layer Scheme for Detecting Blackholes in MANET Using Mobile Agents," 2018 3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Bangkok, Thailand, 2018, pp. 1-4.

[8] Ida Nurcahyani and Helmi Hartadi, “Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET)”, Conference: 2018 International Symposium on Electronics and Smart Devices (ISESD)

[9] NitinKhannaa,,MonikaSachdeva, “Acomprehensivetaxonomyofschemestodetectand mitigate blackholeattackanditsvariantsinMANETs”, Computer Science Review, volume 32, May 2019

[10] Shashi Gurung and Siddhartha Chauhan, “A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET”, Wireless Netw DOI 10.1007/s11276-017-1622-y

[11] Muhammad Salman Pathan, Jingsha He, Nafei Zhu, Zulfiqar Ali Zardari, Muhammad Qasim Memon, Aneeka Azmat, “An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 1, 2019