ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(26), DOI: 10.17485/ijst/2016/v9i26/97250, July 2016* ISSN (Online) : 0974-5645

A Method to Cope with Black Holes' Attack in Mobile Networks and the Study of their Impact on the Basic Parameters of AODV and DSR Protocol

Ali Akbar Arjmand Hashjin[1*] and Amir Najafi[2]

[1]Young Researchers and Elite Club, Zanjan Branch, Islamic Azad University, Zanjan, Iran; a.a_arjomand@yahoo.com

[2]Department of Industrial Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran; asdnjf@gmail.com

Abstract

Security is one of the most important concerns of the basic capabilities of mobile networks. Black hole attacks are one of the prevalent attacks with which routing protocols of mobile network s encounter. In this paper, a method has been presented to deal with those attacks, at same time considering the quality of service. In this method, packets are sent through configured reservation paths. Simulation is carried out in opnet and the results revealed that the proposed algorithms yield good results in terms of packet delivery ratio and throughput when compared with the Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocol. Throughput parameters after applying proposed technique, show 6.51 percent increase for AODV, and 61.86 percent increase for DSR. Also the packet delivery ratio shows 96,68 increase for AODV while it is almost zero percent for DSR. Of course it must be noted that some increase has been observed in sending and receiving that will completely be explained in simulation part.

Keywords: AODV, Black Hole Attack, DSR, Mobile Ad hoc NETwork (MANET), OPerations NETwork (OPNET), Quality Of Service (QOS)

1. Introduction

The most important quality of Mobile Ad hoc wireless networks is the presence of the dynamic topology that results from the mobility of the nodes. The nodes continuously change their location.

This requires a routing protocol with the capability of adjustment to these changes. Tracking and security are among challenges for these networks[1,2]. Today Ad hoc wireless networks are divided into two types: smart, sensor networks, and ad hoc mobile networks. Routing an Ad hoc networks applies limitations on the network which should be considered when selecting the routing method. For example the feeding resource is limited in the nodes and practically it is impossible to change or recharge it.

That is why the proposed routing method should use the existing energy in the best way, that is , it should be aware of the node resources, and it shouldn't send the package to the destination if the node doesn't have enough resources[3]. Understanding of the probable security attacks against MANET is the major concern; access to service, confidentiality, and comprehensiveness of information can be obtained only when security issues are guaranteed[4]. MANET suffer different kinds of attacks because of lack of infrastructure. Generally there are two attack types: passive and active attacks[5]. In a passive attack, the attacker listens silently to the communication is being stablished within the channel, but it doesn't change anything in the massage.

Thus its aim may be to understand the confidential conversation being transmitted through that channel in the network. On the other hand, during an active attack, the attacker can destroy, change, or decrease the major data. Black hole attack is one of important attacks being involved in the reduction of packages , leading

* *Author for correspondence*

to their loss. Previous research indicates that there are different groups of this attack type on MANET. Such as passive, active, internal, external , routing , and package sending. Some of these attacks are called as" individual attacks", while others are considered as" multi-node and destructive attacks"[5].

Research on MANET networks, mostly focuses on attacks, along with a little attention if they also support service quality. There are no suitable definitions or classifications of this kind of attacks against MANET. Meanwhile the impacts of these attacks on MANET have not been measured in the case of providing quality, because researchers are interested in employing different simulations to represent the attacks and determine their consequences such as their impact on package delivery ratio, and end-to-end potential, and delay. Regarding MANET's vulnerability and consequent problems in such networks, we focused on black hole attacks in our study. We examined the service quality on which the black hole attack happens, and evaluated different related parameters.

In[6] a method is represented in order to provide service quality according to AODV routing protocol to prevent from black hole attacks. A degree of trust has been obtained for each node according its ability of package forwarding. A class is established based on this degree of trust. In the stage of discovery of AODV routing protocol, a path is selected in such a way that more trusted nodes are involved. Also non-trusted nodes can be excluded from the path. Thus, the package is transmitted through a more trusted path rather than being transmitted through the shortest path.

In[7] a new mechanism is represented for on- demand multiple path routing protocol (AMODV) considering security and service quality issues in order to minimize the data redundancy. Meanwhile, in this research, step by step authentication mechanism is employed in order to prevent from attacks.

In[2] the impact of black hole attacks on ad-hoc mobile networks is investigated using both, reactive and preventive protocols along with a comparison of vulnerability of them against the attacks, both no techniques are represented to deal with attacks.

In[8] a description is given about existing application and QoS routing algorithms in ad-hoc wireless networks. The limitations of routing algorithms are analyzed in this thesis. They are: disability to meet ad-hoc wireless networks' requirements (such as high accuracy, low over load, extensibility in large network, possibility of QoS routing representation and…). During a black hole attack, a destructive node employs its routing protocol to advertise that it has the shortest path to the destination node or package that it is going to track. This hostile node advertises its access to new paths, regardless of its routing table control. In this way, the attacking node will always be available in response to path demand and consequently tracks and protects the data package[9].

2. Problem Statement

The structure of these networks is based on the use of radio signals instead of wire and cable. In fact, the attackers will be able to misrepresent themselves as a member of the networks, by using these signals, to access to the vital information, attack the service-givers of the organization, destroy the data, make disorders in the communication among nodes, produce false and misleading data, misuse the effective bandwidth of the network and many other destructive activities. As a whole, from a security point of view, there are some common facts within all wireless networks[6]:

- Attackers can easily access to information resources existing in the computational systems by passing the security precautions.
- DOS attacks on wireless, mobile equipment and systems are very common.
- Portable and pocket computers with the capability of using wireless networks can be easily stolen. This can be the first step to penetrate the network.

A hacker can easily find a way to wired network by penetrating the wireless network through using common points existing between a wireless network in an organization and its wired network(which is often considered as a main and more important one).

3. Quality Of Service (QoS)

Representation of a proper solution to provide QoS in MANET requires a cooperation and interaction among different components. The components can consist of[10]:

3.1 Routing Protocols in MANET

In AODV, the source node sends a FREQ massage to the entire network through a flooding manner. After receiving this message, the destination sends a single broadcast PREP in response to the source. Intermediate nodes receiving this response massage, update their routing table based on the route taken by this message for the future use. This information goes to the cache of the node. TTL field and sequence number are used to avoid resending the RREQ message. When discovering of a path fails, a RERR message is sent to the source[11].

DSR is a routing protocol for wireless networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. There are 2 major phases: Route discovery uses route request and route reply packets. Route maintenance–uses route error packets and acknowledgments.

The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use within networks containing unidirectional links, use of only "soft state" in routing, and very two hundred nodes, and is designed to work well with even very high rates of mobility[11].

3.2 A Resource Reservation Plan

Generally, each node in the network has a set of limited resources. The capability of the node at a given time, can he defined by access to these resources. There are different node resources according to the network that they operate in, such as switch circuit, change message, connection-oriented, connection, etc. Generally, node resources consist of band width, buffer, propagation delay, transfer time, and processing power. Service quality has always been a major challenge for IP-based networks, especially for the internet. Due to the presence of non-connection oriented quality in IP protocol, no connection is established before sending data. There are several suggestions to solve this problem, one of which is PSVP.

3.3 QoS with the Ability to Control the Middle Layer of Access (MAC)

This component is placed by default.

4. Description of RSVP Protocol

RSVP is a signaling protocol for reserving network resources on the internet to support single-broadcast and multi-broadcast communications. In order to adjust the resource reservation in nodes along the path between transmitter and the receiver, to types of massages, namely path and RESV are used in RSVP.

First the sender sends the path message to the receiver so that a path can be found from the transmitter to the receiver for a particular stream. When the host keeps the path message, the message is recorded in the opposite direction of the path message host and received from the direction of the path message, toward the route.

The path messages pass one after another and finally reach the receiver. The receiver answers with RESV message in order to provide reservation resources for the specific stream, the RESV message is transmitted along the same path, that is , the path massage route. Upon the arrival of the RESV message, each host in the route, with keep the sources for the particular stream, if sufficient sources are available[12].

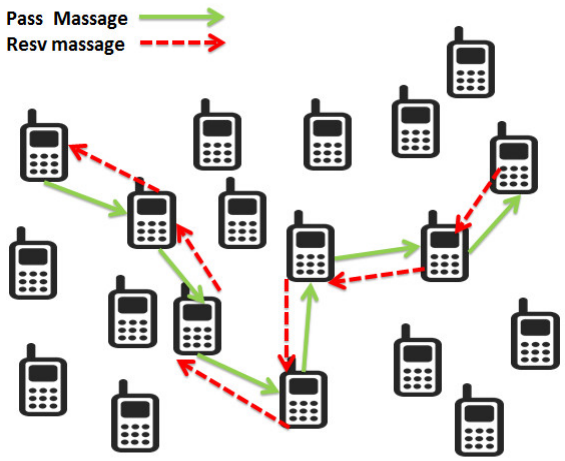

Figure 1. RSVP protocol.

5. Black Hole Attack

Regarding the fact that MANET is a set of nodes that from a temporary network without a centralized control, the nodes should interact to each other according to an unconditional trust. This feature leads to the susceptibility of MANET to more attacks comparing to other types of network. Practically, MANET can be attacked through several and different ways.

Before closer investigation, security attacks should

be classified within the framework of MANET[13]. This classification can be conducted based on the operation type (active vs. passive), source of attack (internal vs. external), power and capacity of attackers (wired vs. mobile) and the number of attackers (individual vs. group)[14]. During a black hole attack, nodes initially behave in a normal form. They receive FREQ from neighboring nodes and give back the RREP response message to the sender of PRRQ.

Thus, according to the traditional routing protocol of AODV, a high sequence number also is assigned to the node. Therefore, the node actively participates in the process of discovering the AODV routing path, and the path is established by the node.

At first, the actual path seems to stablish in the source and the destination. Therefore they begin to transfer the data. But after it, harmful nodes deny the completeness of the package, and swallow it. Thus the package drops, rather than advancing toward the destination. This node is known as the black hole node, and this phenomenon is called the black hole attack. Apparently, the black hole attack ruins the quality of service through package drop. Several ways have been suggested by researchers to deal with this problem. We will represent one of them. In order to find out the attack type in AODV, two types can be described[15].

5.1 Internal Black Hole Attack

This type of black hole attack has an internal malicious node between the source and destination paths. That node changes into an active element to destroy the data path as soon as possible. At this stage, it is able to start its attacks along with data transfer. This is an internal attack because the node itself belongs to the data path. Due to the difficulty in identification of the malicious node , the internal black hole attack is more harmful.

5.2 External Black Hole Attack

External attacks are physically located outside the network. They prevent from access to the network traffic, or create traffic in the network, or disrupt the entire network. External attacks can turn into internal ones when they control the internal malicious node and activate it to attack the other nodes in ad-hoc mobile networks[13].

6. The Proposed Solution

One of the important issues in ad-hoc mobile network area is the quality of service. It is not easy to support the quality of service in these networks because of topology changes and also use of shared media by the network nodes. A lot of work has been done in order to ensure the quality of service. An instance is the protocols of routing. The important issue in QoS routing is not only to find a path from the source to the destination, but also we need a path that is able to provide the quality of service in terms of bandwidth and delay.

Most of routing protocols designed for these networks, only work on the step basis, regardless of the quality of service within the established routs. In this paper, our main focus is on the impact of quality service on the black hole attack. Different features will be discussed and the percentage of the rise of decline in parameters will be evaluated.

The purpose of this paper is to analyze the quality of service during a black hole attack. To do this, we will give a general definition of the black hole attack and after reviewing the quality of service, some important performance metrics of MANET, such as end-to-end delay, packet delivery ratio , and throughput will be discussed.

7. Simulation Results

In this research, we used two scenarios. In the first scenario, the black hole attack was performed on 20 nodes in a 500 meter environment. In the second scenario, in addition the former operations, the quality of service also was performed. OPNET 14.0 was employed to conduct the simulation and to analyze the obtained results. Figure 2 shows the simulation environment.

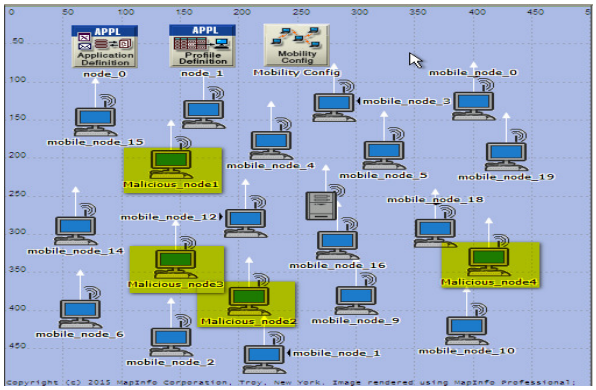

Figure 2. Simulation environment.

Table 1. Simulated parameters

Simulator	OPNET 14.0
Examined protocols	AODV, once performing black hole attack, once performing it along with QoS
Simulation duration	180 seconds
Simulation area	500 m^2
Nodes number	20 nodes
Transfer protocol	Video
Frame inter-arrival time	10 frame/ sec
Frame size	128*120 pixel
Nodes speed	20 m/s

8.1 Packet Delivery Ratio

This refers to the ratio of the total number of data packets delivered to their destinations by the source node. It is another performance measuring metric used to determine the degree of efficiency and precision of MANET routing protocol[16]. The reduction percentage was measured as follows:

Supposing A to be equal to the first amount, when the black hole attack was performed, and B, equal to the second amount, when QoS also was performed, the rise or reduction was: If B is bigger than A, the rise percentage is (b-a)* (100/a), and if B is smaller than A, the reduction percentage is (be-a)*(100/b).

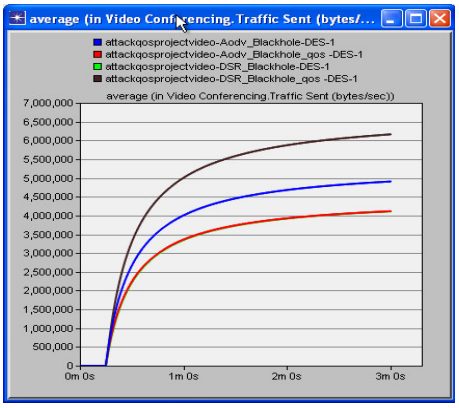

Figure 3. Traffic sent simulation.

The number of received packets for AODV during the time of black hole attack was 44347082.22, while the number of sent packets for the same tome was 3793221542, so the ratio of packet delivery is 0.01. Also the number of sent packages was 3183193825.

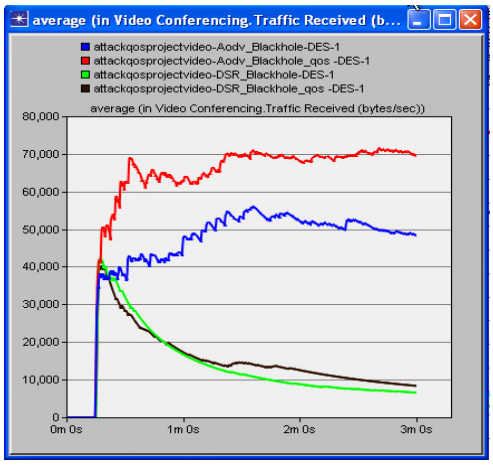

Figure 4. Traffic receive simulation.

Thus the ratio of packet delivery is 0.3 it means that we have 96.69 percent increase in packet delivery according to the percentage of decrease or increase norm on the other hand, the number of received packets was 13149550.49 for DSR when the black hole attack happened while the number of sent packets was 3172079629. Thus the ratio of packet delivery is 0.00.

Also, the number of received packets for DSR was 14503851.91 when black hole attack happened and the quality of service was applied, while the number of sent packets was 4746865927 during the same time. Thus the ratio of packet delivery is 0.0.

8.2 Throughput

Throughput points to the amount of data that can be sent from the source to the destination, depending on the bandwidth. It is a criterion to measures the data rate (bits per second) produced by the application[16].

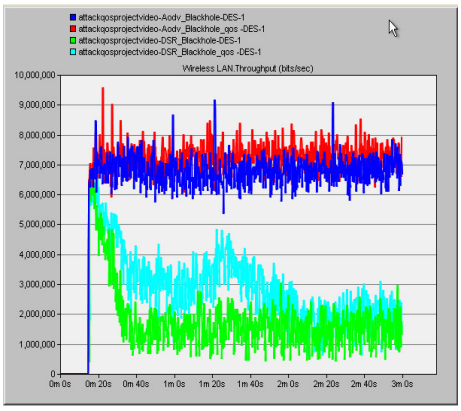

Figure 5. Throughput simulation.

The total amount of throughput for AODV during the occurrence time of black hole attack was 6199539911.11 bits per second when the black hole attack happened and the quality of service also was applied.

Therefore, there was 6.52 percent increase in the amount of throughput. This means that throughput also improves by applying the quality of service. Meanwhile, the total amount of throughput for DSR was 1618072000.00 bits per second at the time of black hole attack occurrence, while it was 2614633777.78 when black hole attack happened and the quality of service also was applied. Therefore, it can be concluded that there was an increase of 61.58 percent in the amount of throughput. This indicates that throughput also improves with the application of the quality of service.

9. Conclusion

In this paper, the Quality of Service (QS) was proposed to solve the problem of black hole attack, and the parameters of packet delivery ratio were evaluated. The number of received packets for AODV during the time of black hole attack was 44347082.22, while the number of sent packets for the same tome was 3793221542, so the ratio of packet delivery is 0.01. Also the number of sent packages was 3183193825.

Thus the ratio of packet delivery is 0.3. it means that we have 96.69 percent increase in packet delivery according to the percentage of decrease or increase norm. on the other hand, the number of received packets was 13149550.49 for DSR when the black hole attack happened while the number of sent packets was 3172079629. Thus the ratio of packet delivery is 0.00.

10. References

1. Chadha MS, Joon R. Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs. International Journal of Soft Computing and Engineering (IJSCE). 2012; 2:375-81 .
2. Ullah I, Rehman SH. Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols. Master Thesis Blekinge Institute of Technology. Sweden, June; 2010.
3. Dorri A, Kamel SR, Kheyrkhah E. Security challenges in mobile ad hoc networks: A survey. International Journal of Computer Science and Engineering Survey (IJCSES). 2015; 6:15-29.
4. Chahal P, Tak GK, Tomar AS. Comparative Analysis of Various Attacks on MANET. International Journal of Computer Applications. 2015; 11:42-46.
5. Asokan R. A review of Quality of Service (QoS) routing protocols for mobile Ad hoc networks. Wireless Communication and Sensor Computing, 2010. ICWCSC 2010. International Conference; 2010. p. 1-6.
6. Bar RK, Mandal JK, Singh M. QoS of MANET Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack. International Conference on Computational Intelligence: Modeling Techniques and Applications. 2013; 10:530-37.
7. Sedaghat S, Jahrom Adibniya F, Derhami V. A mechanism-based QoS and security requirements consideration for MANETs QoS routing Telecommunications (IST), 2012 Sixth International Symposium; 2012. p. 1123–28.
8. Chen T. Efficient Routing and Quality of Service Support for Ad Hoc Wireless Networks. Ph.D. Thesis, Science Department, University of California at Los Angeles, USA, Los Angeles; 2005.
9. P. Virada, V. Tamilarasan S. Securing and preventing AODV routing protocol from black hole attack using counter algorithm. International Journal of Engineering Research and Technology (IJERT). 2012; 1(5):1-6.
10. Perkins DD, Hughes HD. A survey on quality-of-service support for mobile ad hoc networks. Special Issue: Mobile Ad Hoc Networking – Research, Trends and Applications. 2002; 2:503-13.
11. Paul B, Bhuiyan KA, Fatema K, Das PP. Analysis of AOMDV, AODV, DSR, and DSDV routing protocols for wireless sensor network. Computational Intelligence and Communication Networks (CICN), IEEE; 2014. p. 364–69.
12. Pana F, Put F. A Survey on the Evolution of RSVP. Advanced Computing and Communication Technologies (ACCT), 2012 Second International Conference on, IEEE; 2013. 99:1-29.
13. Sharma N, Sharma A. The Black-Hole Node Attack in MANET. Communications Surveys and Tutorials IEEE; 2012. p.546–50.
14. P. Virada V. "Securing And Preventing AODV Routing Protocol From Black Hole Attack Using Counter Algorithm"; International Journal of Engineering Research & Technology (IJERT); 2010,8,.
15. Singh H, Singh G, Singh M. Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack. International Journal of Computer Applications. 2012; 42:43-46.
16. Chaba Y, Singh Y, Joon M. Simulation based performance analysis of on-demand routing protocols in MANETs. Computer Modeling and Simulation, 2010. ICCMS '10. Second International Conference; 2010. 3:80-83.