www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 10 Oct 2015, Page No. 14698-14709

Prevention of Blackhole Attack over AODV and DSR MANET Routing Protocol

Shabnam Sharma, Meenakshi Mittal
Computer Science and Technology
Central University of Punjab, Bathinda.
Computer Science and Technology
Central University of Punjab, Bathinda.

Abstract
Wireless technology is one of the biggest contributions to mankind. In wireless system, transmission of information can be done without the need of wires and cables. Mobile Adhoc Networks (MANETs) do not have any centralized administration. They are infrastructure-less networks. They do not contain any networking device like routers or access points. MANETs are self-starting and dynamicnetwork comprising of mobile nodes. Mobile Ad-hoc networks require routing protocols for communication among nodes. Due to the lack of centralized management, various attacks are possible in MANETs such as passive or active attacks. Blackhole attack is an active kind of attack in which a malicious node pretendsto have a shortest and fresh path to the destination. Blackhole attack affects the performance by disrupting the normal communication in the network. Therefore, there is need to prevent the network from attack. In this paper, prevention of blackhole attack is done over AODV and DSR routing protocol with Random Waypoint Model. Malicious nodes in the network are known and if malicious nodes encounter in between the route from source to destination, then intermediate node have to simply discard that path and have to find an alternate path.The simulation results show that AODV routing protocol performs best and is suitable for highly dynamic networks.

1. INTRODUCTION

Wireless industry has seen tremendous growth in last few years. The advancement in growing availability of wireless networks and the emergence of handheld computers, cell phones,etc. are playingimportant role in our day to day life. Accessing Internet services from anywhere becomes easy with the help of mobile devices. [1]. In Wireless network, there is no physical wired connection between sender and receiver but rather thenetwork is connected wirelessly to maintain the communication. Wireless Networks can be categorized into two classes as infrastructure-based networks and infrastructure-less networks[2]:

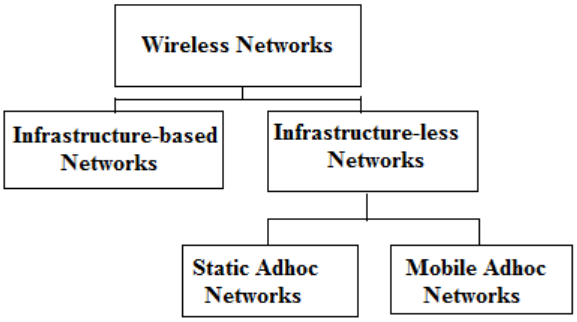

Figure 1 Classification of Wireless Networks

Infrastructure-basedwireless networks rely on the access points. Access point is responsible for coordinating communication between nodes. Examples are like wireless network set up in offices, homes, hospitals, airports where client

DOI: 10.18535/ijecs/v4i10.26

connect to the internet with the help of an access point. Figure 2 shows infrastructure based wireless network. In infrastructure based networks, at the time of communication access points are fixed, and nodes within the transmission range can communicate.

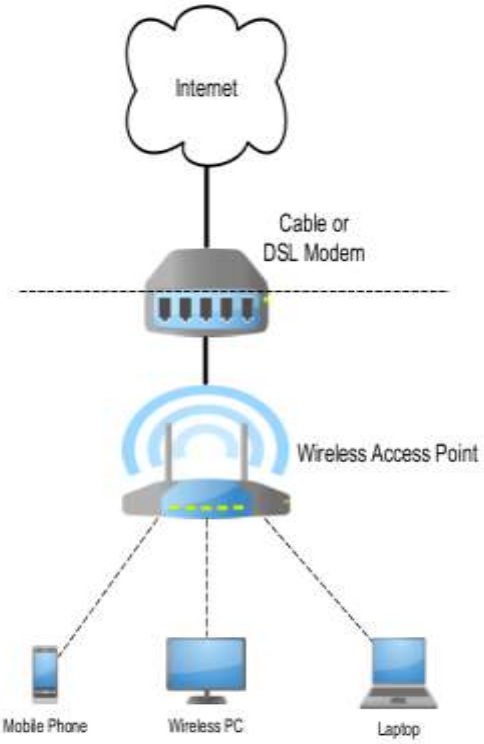

Figure 2 Infrastructure- Based Wireless Networks

Infrastructure-lessnetworks do not rely on an access point [3]. In infrastructure-lessnetwork, mobile nodes communicate with each other without any fixed infrastructure. Infrastructure-less network is shown in figure 3, where nodesarefreeto communicate with each other.

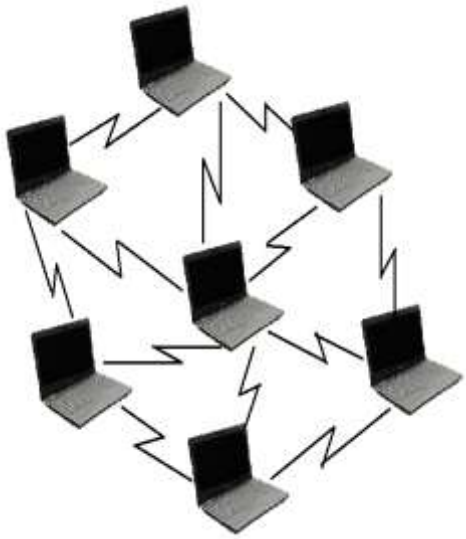

Figure 3Infrastructure-less Network

2. Mobile Adhoc Networks (MANETs)

A Mobile ad-hoc network is a collection of two or more wireless devices having the ability to communicate with each other without the need of any centralized administration [2]. Mobile Adhoc Networks are temporary networks i.e. they are suitable for the areas where it is not possible to set up a fixed infrastructure. They can also be deployed easily in case of emergencies and short-term needs. In MANETs, the network is distributed among nodes, and they will have to act as router also. If one node wants to communicate with another node that is not in its transmission range, then it requires an intermediate node to transmit the data. As shown in figure4, node A wants to communicate with node C. Node A and node C are not in the transmission range of each other. So there is a need for an intermediate node that is in the transmission range of both sender and receiver node. Here node B acts as an intermediate node.

DOI: 10.18535/ijecs/v4i10.26

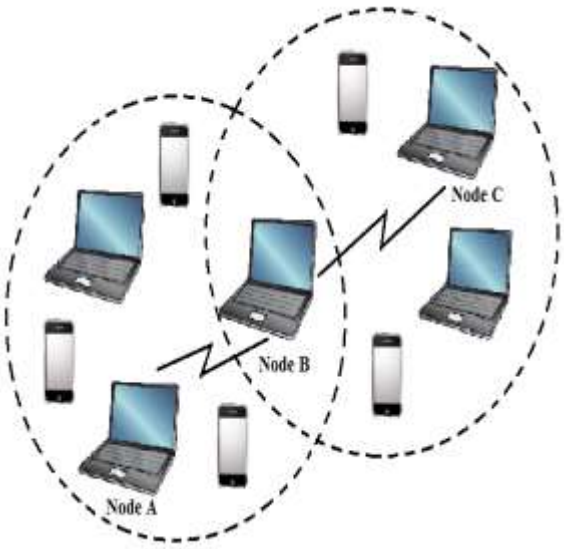

Figure 4 A Mobile Adhoc Network Scenario

As the nodes in mobile ad-hoc networks can change their positions. Thus the topology of MANETs is dynamic in nature. Also in MANETs nodes communicate with each other on the basis of mutual trust. Mobile nodes present within the range of wireless link can overhear and even participate in the network and due to lack of central administration any malicious node can take part in thenetwork.These features make MANETs more vulnerable to be exploited by an attacker inside the network. Characteristics of MANETs are described in Table 1:

Table 1:Characteristics of MANETs [4]

Characteristics	Explanation
Distributed operation	In MANETs there is no centralized administration, and the networkis distributed among nodes. The nodes in the network cooperate with each other during the transmission process.
Multi-hop communication	In MANETs when one node wants to transmit data to another node which is not in its transmission range then it require an intermediate node to forward the data.
Autonomous Terminal	In MANETs, each node has to act as host as well as router.
Dynamic topology	In MANETs nodes are free to move i.e. they can leave and join the network at any time which leads to its dynamic topology.
Scalability	The nodes can move away and join the network at any point of time. Thus, the scalability of the network can be increased anytime by adding new nodes in the network.

MANETs can be deployed in the areas where a wired network may not be possible due to reason of cost or convenience. The network can be deployed easily in the case of emergencies. Some of the applications are discussed below in Table 2.

DOI: 10.18535/ijecs/v4i10.26

Table 2: Applications of MANETs [5]

Area	Application
Military Battlefield	MANETs can be used inthe military to maintain an information network between the soldiers, vehicles, and their headquarters.
Tactical Network	MANETs can be used for emergency services during disaster management because they are easy to establish.
Sensor Nodes	The sensor nodes can be used inside the home for security purpose such as a fire alarm, data tracking of environmental conditions, etc.
Home and Enterprises	Wireless networking is used in home or office, conferences, meeting rooms and personal area networks.

Inspite of so many applications of MANETs there are still some issues and challenges to overcome discussed in Table 3.

Table 3: Challenges in MANETs [6]

Challenges	Explanation
Dynamic topology	Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
Routing Overhead	In wireless adhoc networks, nodes often change their location within network. So it causes unnecessary routing overhead while updating routing table.
Hidden terminal problem	This problem refers to the collision of packets at a receiving node. Due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
Battery constraints	Devices used in these networks have restrictions on the power source to maintain portability, size and weight of the device.
Lack of centralized management	MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large-scale ad-hoc network.
No predefined Boundary	In mobile ad- hoc networks physical boundary of the network cannot be defined. This allows nodes to join and leave the wireless network anytime.

2.1 Security Attacks in MANETs

On the behavior of attacks, it can be classified into two types of attack i.e. Passive attacks and Active attacks [5].

- **Passive attacks:**A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or

accumulates data from it. The passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from the traffic. Different types of passive attacks are like traffic monitoring, eavesdropping etc.

- **Active attacks:** Active attacks cause a modificationofdata, or it can also create a false data stream. Active attacks canalter the normal operation of the network. Various types of active attacks: Wormhole attack, Blackhole attack, Rushing attack, Sinkhole attack, Spoofing attack, etc.

3. ROUTING PROTOCOLS

Routing protocols are a set of rules or standards thatdetermine how nodes in the network communicate or exchange information with each other [7]. Routing protocols in MANETs are classified into three different categories according to their functionality as proactive, reactive and hybrid protocols [8].

- Proactive Protocols
- Reactive Protocols
- Hybrid Protocols

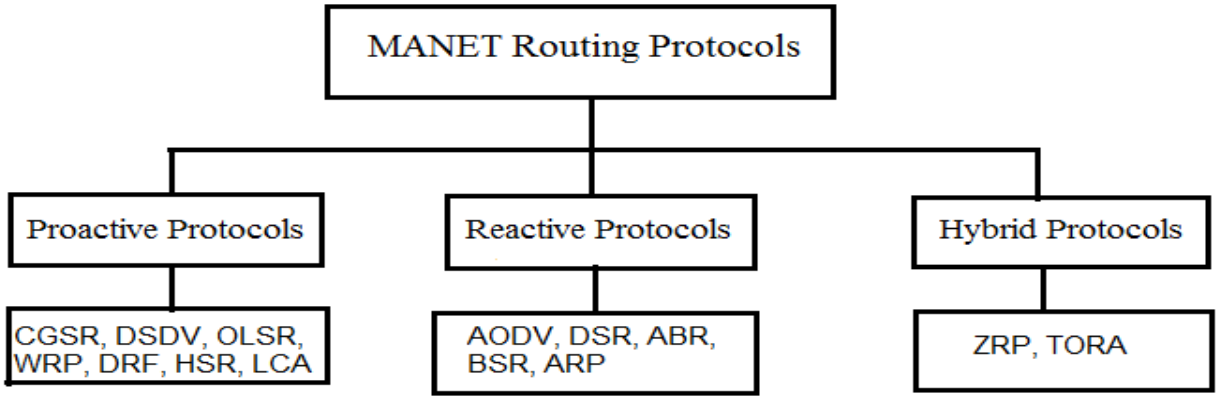

Figure 5 Classification of Routing Protocols

(a) Proactive Protocol: In proactive routing protocol, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network. These protocols are also called table driven protocols [9].

(b) Reactive protocols: Reactive protocols are also called as On Demand drivenprotocols [9]. They are called so because they do not initiate the route discovery process by itself until they are requested.Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR), Associativity Based Routing (ABR), Bootstrap router (BSR) etc.

Examples of proactive protocols are: Destination sequenced distance vector (DSDV), Optimised Link State Routing Protocol (OLSR), Cluster Gateway Switch Routing Protocol (CGSR), Wireless Routing Protocol (WRP), Hierarchical State Routing (HSR) etc.

(c) Hybrid Protocols: Hybrid protocols are the protocols that combine the features of reactive and proactive routing protocols [10]. The Zone Routing Protocol (ZRP) is an example of hybridrouting protocol in which network is divided into zones. To maintain routing information within each zone proactive approach is used. If source node and destination node are in different zonesthen reactive approach (initiates a new route discovery process) is used.

DOI: 10.18535/ijecs/v4i10.26

3.1 Adhoc on Demand Distance Vector

The Ad hoc On-Demand Distance Vector (AODV) protocol enables dynamic, self-
starting, multi hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain those routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. AODV protocol has three phases: route discovery phase, route reply phase and route maintenance phase [11]. Figure 6 shows the route discovery process in AODV protocol. Source node S broadcasts RREQ packet to its neighbor node. Neighboring nodes will again broadcast the packet until it reaches the desired destination. Destination node receives multiple copies of same RREQ packet through different routes i.e. from node 2, node 3 and node 6. Now it will select a routewith a highest sequence number and less number of hop counts.Then it will unicast RREP packet over the shortest path i.e Node D – Node 3- Node S.

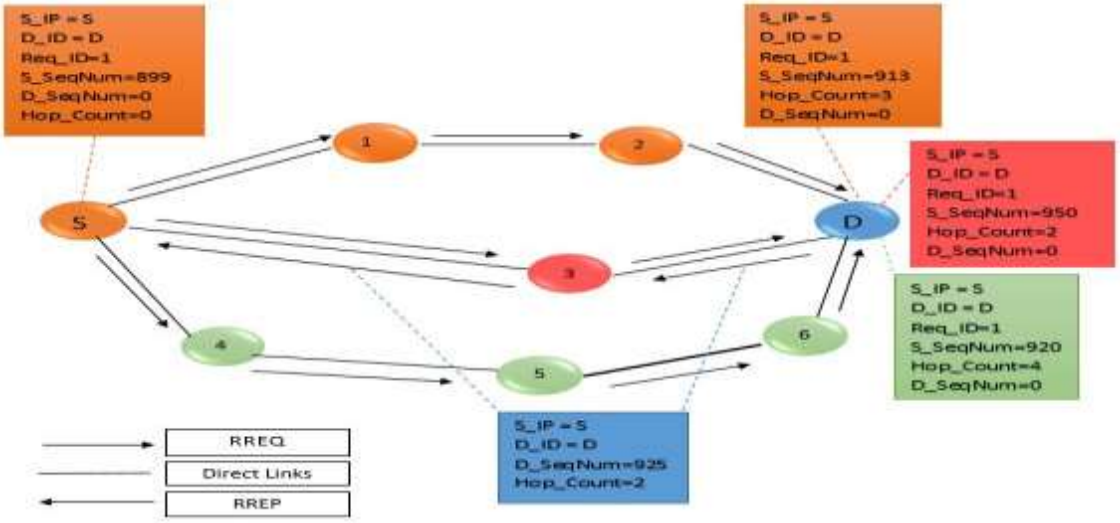

Figure 6 Route Discovery in AODV Routing Protocol

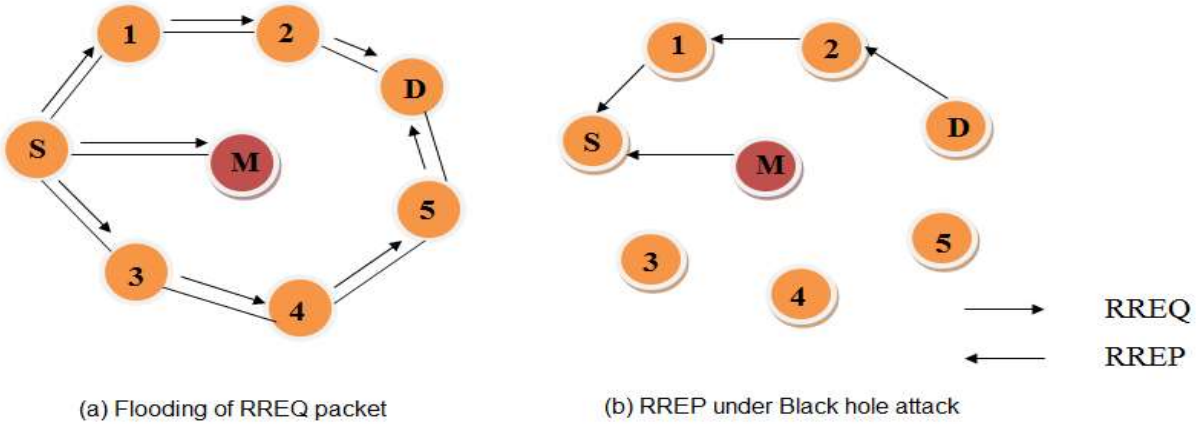

Figure 8(a) Flooding of RREQ packet (b) RREP under Blackhole Attack

DOI: 10.18535/ijecs/v4i10.26

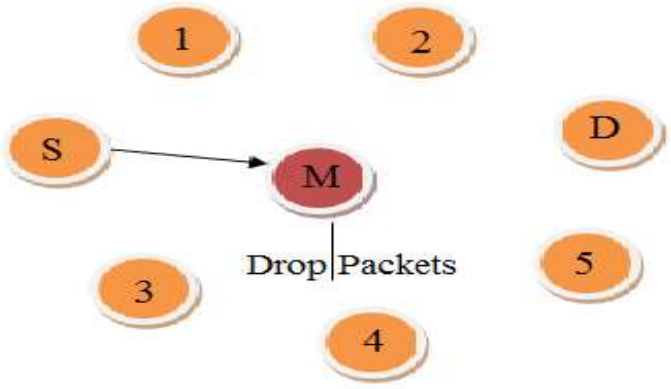

Figure 9 Blackhole attack

Figure 8 and figure 9 shows blackhole attack over AODV routing protocol. Source node S floods the RREQ packets all over the network. In response to that request packet, destination node will make route reply. As the network is under blackhole attack the malicious node M will generate a fake reply packet with freshroute having a highest destination sequence number and less number of hop counts. The source node S considers this node as a legitimate node having a freshroute, and starts routing packets to malicious node. As shown in figure 9 Malicious node M drops all the packets as it receives them.

5. Proposed Technique

In proposed prevention technique it is assumed that blackhole nodes in the network are known. List blackhole nodes id's and initialized them by tcl commands. Once blackhole nodes aredetected they are not considered during route construction.To start a transmission process from source node to destination, source nodestarts a route discovery process. In order to find a secure route each intermediate node has to be parsed for the presence of blackhole node id. If the blackhole node id appears in the path, one hasto simply dump that path and start a new route discovery phase from the previous node.

DOI: 10.18535/ijecs/v4i10.26

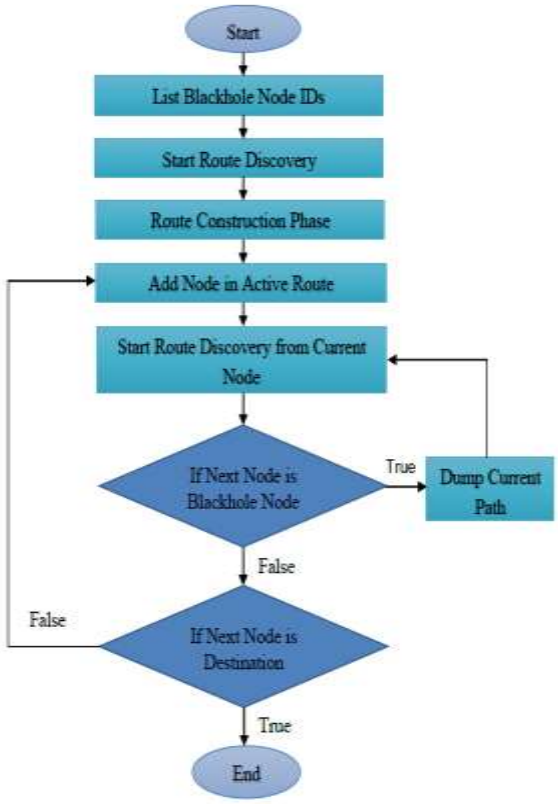

Figure 10 Mechanism to Prevent Blackhole Attack

5. Simulation Environment

The simulation study shows that how a particular protocol will behave when deployed in real scenario. Simulation over various parameters is donein order to analyze its performance and effectiveness. The simulation environment and the parameters consideredfor research work is shown in Table 2.

Table 2: Simulation Experiment

Experiments	No. of nodes	Traffic Pattern	Metrics
Simulation of AODV and DSR without Blackhole attack	10 30 60 100	FTP	• Packet Delivery Ratio • AverageEnd To End Delay • AverageThroug-hput
Simulation of AODV and DSR under Blackhole attack			
Simulation of AODV and DSR under Prevention scheme.			

5. Results and Discussions

The performance of both protocols AODV and DSR are analyzed under three conditions i.e without blackhole attack, with blackhole attack and under prevention scheme

5.1 Performanceevaluation of AODV routing protocol

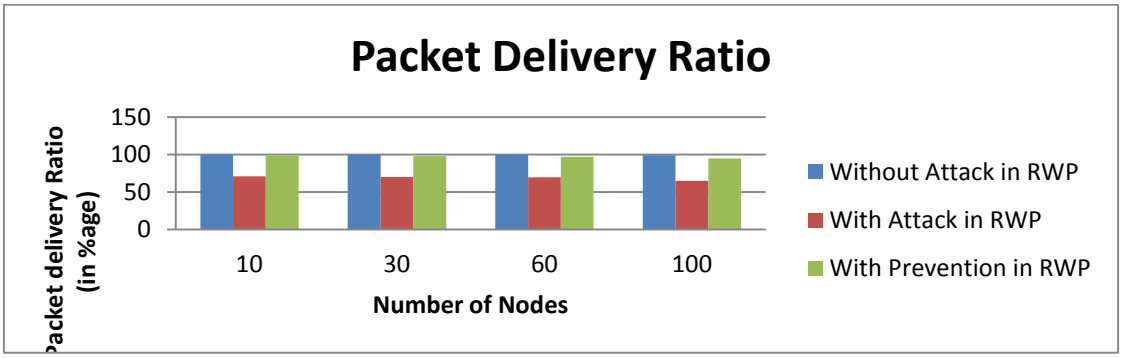

Figure 11 Packet Delivery Ratio in AODV Routing Protocol

DOI: 10.18535/ijecs/v4i10.26

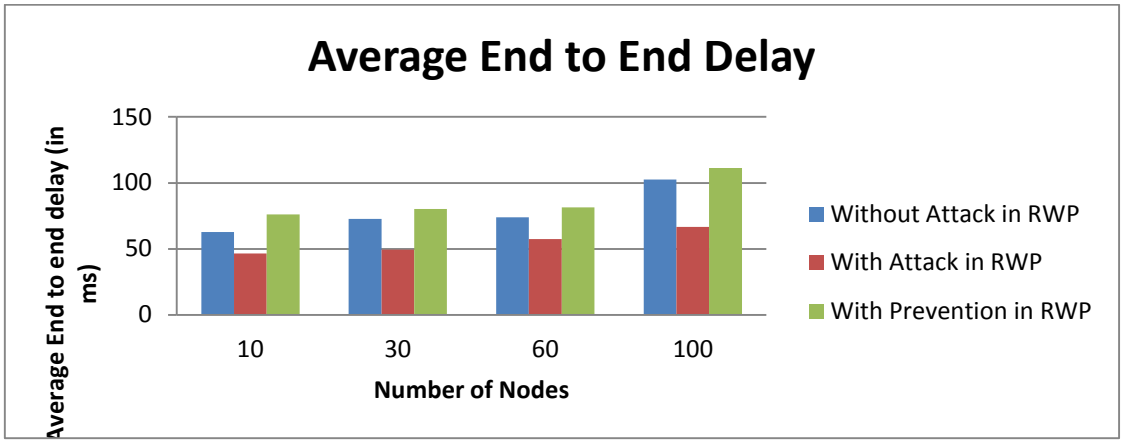

Figure 12 Average End to end Delay in AODV Routing Protocol

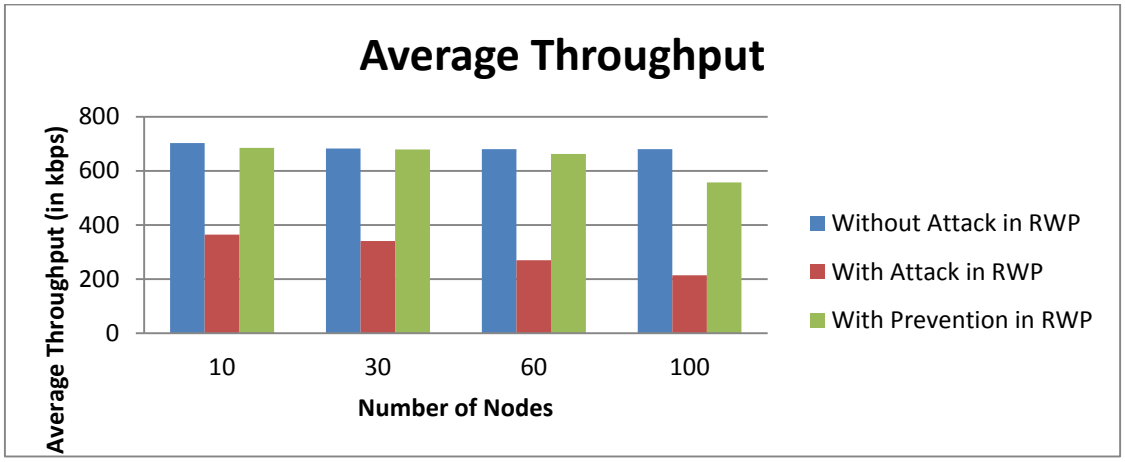

Figure 13 Average Throughputin AODV Routing Protocol

5.2 Performance evaluation of DSR RoutingProtocol

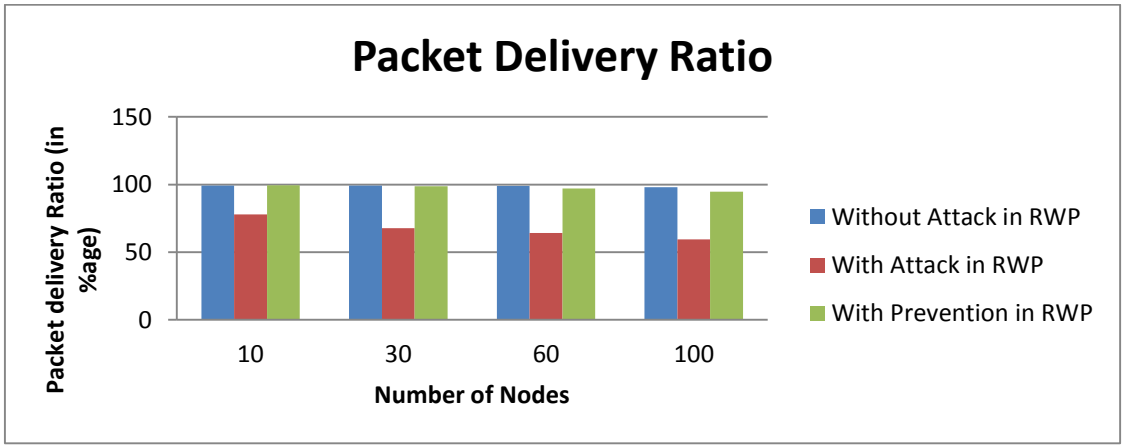

Figure 14 Packet Delivery Ratio in DSR Routing Protocol

DOI: 10.18535/ijecs/v4i10.26

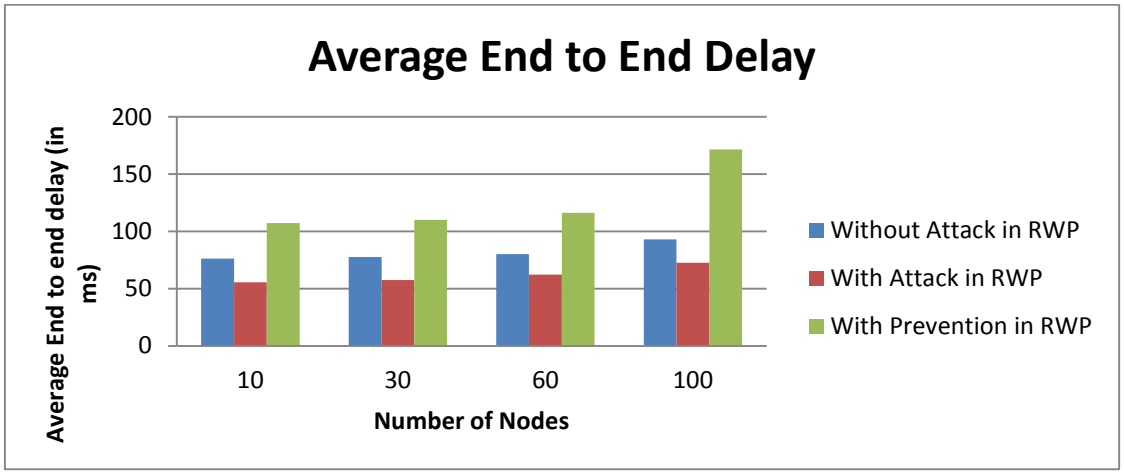

Figure 15 Average End to End Delayin AODV Routing Protocol

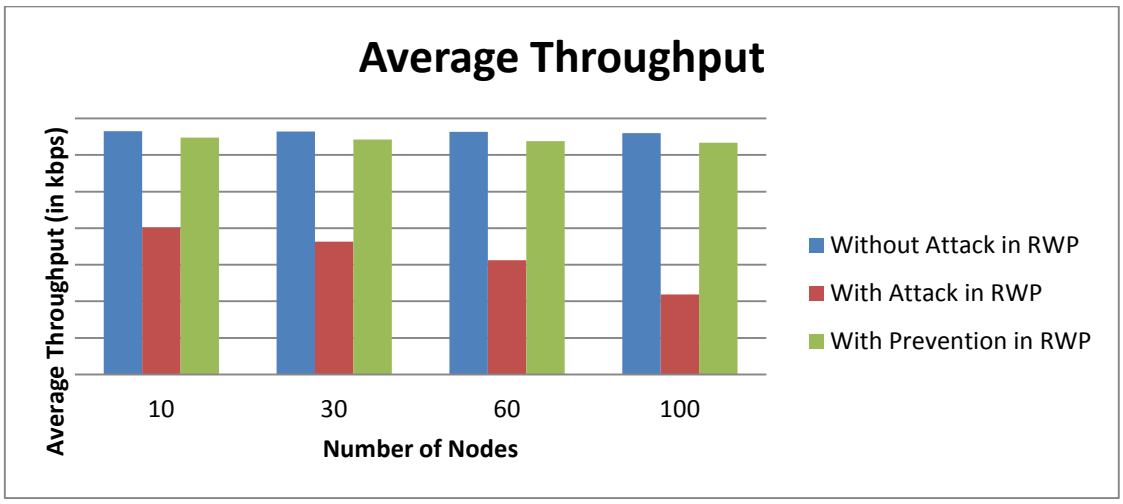

Figure 16 Average Throughput in DSR Routing Protocol

In section 5.1 and 5.2 both AODV and DSR MANET routing protocols are analyzed under different performance metrics. The results are analyzed as follow:

(a) Packet Delivery Ratio : It can be defined as the ratio of total number of data packets delivered to the destination, to the total number of data packets generated by the source. It is calculated as

P = (number of packets received) / (number of packets sent) * 100

AODV is more effective compared to DSR. Unlike DSR, it does not store any route. Italways uses fresh routes for communication and is best suitable for highly dynamic networks. PDR is less in case of DSR routing protocol because for every new communication process, firstly, it checks its route cache for any pre-existing routes and if there is a route in cache it starts transmitting packets otherwise it will start a new route discovery process.

(b) Average end to end Delay : It is average delay time incurred when data packets are send from source to destination. It is calculated as

$$D = \sum_{i=0}^{n} \mathbf{di}\,/n$$

Where d_i is a time for end-to-end delay of i_{th}data packet.

Average end to end delay increases with increase in number of nodes in both AODV and DSR routing protocol. It is less in case of AODV routing protocol because whenever there is need to send

packet from source to destination, it will start a new route discovery process. While in case of DSR, it first searches its cache rather then a new route discovery process and due to dynamic topology if route changes then cached route become invalid.

(c) Average Throughput : It is defined as a amount of data delivered per unit from source to destination. It is calculated as:

Average Throughput =
(Received packet size/ (stop time-start time))*(8/1000)

As PDR increases average throughput also increases. It is more in case of AODV routing Protocol.

6. Conclusion

Adhoc network is self organized network that consist of mobile nodes which communicate with each other over wireless links. These networksare not protected against malicious nodes due to the simplicity of the routing protocols. Blackhole attack is one of a major attack, in which malicious node falsely claim fresh and shortest path from source to destination. If these malicious nodes work co-operatively then the damage caused by them will be serious. AODV routing protocol is more effective than DSR in all scenarios. Unlike DSR, it does not store stale routes.

As a future scope of work, the same technique can be implemented with different traffic patterns like HTTP traffic, telnet traffic and real time traffic and also can be implemented over different protocols like ABR, DSDV, WRP, etc. under other different mobility models (Random Walk Model, Reference Point Group Model etc).The prevention technique can also be enhanced by adding a detection method to it .

References

[1].Loo, J., Khan, S., and Al-khwildi, A. N. (2012). *Mobile AdHoc Network- Current Status and Future Trends.* New York: CRC Press Taylor & Francis Group

[2].Medadian, M., Mebadi, A., and Shahri, E. (2009). Combat with Black hole Attack in AODV Routing Protocol. *Proceedings of the 2009 Malaysia International Conference on Communication* , 530-535. Malaysia.

[3].Singh, P. K., and Sharma, G. (2012). Efficient Prevention of Blackhole Problem in AODV Routing Protocol in MANET. *11th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom).3*, 902-906. Liverpool: IEEE.

[4]. Mishra, A., Jaswal, R., and Sharma, S. (2014). A Novel approach for Detecting and Eliminating Cooperative Blackhole attack using Advanced DRI Table in Adhoc Network. *International Journel of Computer Science And Mobile Computing, 2* (12), 217-220.

[5].Kanthe, A. M., Simmunic, D., and Parsad, R. (2012). Effects of Malicious Attacks on Mobile Adhoc Networks. *IEEE International Conference on Computational Intelligence &Computing Research(ICCIC)* 1-5. Coimbatore: IEEE.

[6]. Tseng, F. H., Chou, L. D., and Chao, H. C. (2011). A survey of Black hole attack in Wireless Mobile Adhoc Networks. *Human Centric Computing and Informational Sciences* , 1-16.

[7].Srivastav, A., and Chandar, N. (2013). Overview of Routing Protocols in MANETs and Enhancement in Reactive Protocols. *International Journal of Advanced Research in Computer Science and Software Engineering, 3* (2), 251-259.

[8]. Aware, A. A., and Bhandari, K. (2014). Prevention of Black hole Attack on AODV in MANET using hash function. *3rd International Conference on Reliability, Infocom Technologies and Optimization(ICRITO)(Trends and Future Directions,2014)* 1-6. Noida: IEEE.

[9].Sam, S., and Chacko, N. M. (2013). A survey on various privacy and security features adopted in MANETs Routing Protocol. *International Multiconference on Automation Computing, Communication, Control and Compressed Sensing* 508-513. Kottayam: IEEE.

[10].Sharma, P. S., Shukla, R., and Pandey, R. P. (2009). Bluff-Probe Based Black hole node Detection and Prevention. *IEEE International Conference on Advanced Computing* 458-461. Patiala: IEEE.

[11].Perkins, C. E. (2015, March 15). *Ad hoc On demand Distance Vector (AODV) Routing*. Retrieved March 15, 2015, from https://www.ietf.org: https://www.ietf.org/rfc/rfc3561.txt

[12].Johnson, D. (2015, March 15). *The Dynamic Source Routing (DSR) for Mobile Adhoc Network*. Retrieved March 15, 2015, from https://www.ietf.org: https://www.ietf.org/rfc/rfc4728.txt

[13].Das, R., and Purkayastha, B. S. (2012). Security Measure For Black Hole Attack in Manets: An Approach. *International Journel of Engineering Science and Technology, 3*, 28