International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.13-20
http://dx.doi.org/10.14257/ijsia.2016.10.12.02

A Novel Technique for Detection & Isolation of Blackhole Attack

Shivani Vijan and Sandeep Kumar Arora*

[1,2] Discipline of Electronics and Communication Engineering, Lovely Professional University, Jalandhar, Punjab, India-144411
[1]shivanivijan@gmail.com, [2]sandeep.16930@lpu.co.in

Abstract

All links in mobile ad-hoc networks are wireless and works independently, as there is no fixed infrastructure. In mobile ad-hoc network, network topology may change rapidly. The basic reason is the mobility of nodes, so it requires more security. This paper basically discusses the black hole attack, collaborative black hole attack & the technique to detect and isolate these types of attack. The collaboration of two proposed techniques i.e. fake route request with fake destination ID and multipath routing is implemented that helps in detection of black hole attack. These attacks may lead to the degradation of performance of the network. The algorithm implemented will improve the packet delivery by 25% and delay factor by 50% as compared to the conventional techniques. We also compared the results such as routing overheads, packet loss, energy consumption and throughput.

Keywords*: MANET, Blackhole attack, AODV, Detection, Routing*

1. Introduction

IEEE 802.11 standards for Wireless LAN architecture consists of a basic service set (BSS) without the access point forming a temporary network called ad-hoc network or infrastructure less network. The nodes in the network comprises of such as (PDA's, laptops, smart phones) which are mobile, self-configuring and can act as both routers and packet forwarders in the network. The network comprising of such nodes forms a sub class of ad-hoc networks which is well known as Mobile Ad-hoc Networks (MANET). The self-configuring and self-preserving nature of mobile nodes and dynamic changing topology makes this technology suitable for providing communication in emergency and rescue operations which demands a need of urgent network. In MANET, the nodes maintain a trust and conjoin with each other to forward the packet and convey the information about change of topology. As the nodes are mobile and transmission through medium is wireless so the loss of information packets and how packets are routed from source to destination are two major concerns. [2] So MANET requires a strict routing and security protocols to transfer information throughout the network. From past 20 years, MANET have maintained their remarkable position in commercial domain applications because of the features like mobile nodes, easy and quick installation, no centralized administration (access point) in the network. MANET requires a strict format to provide a secure and methodical communication from source to destination with minimum packet loss [3].

2. Security Issues in MANET

Due to lack of central administration, mobile nodes which are responsible for causing change in network topology, transmission through wireless medium etc. makes the MANET vulnerable to different types of attacks. Intruders are in possession to extract the useful information that is being transmitted. Due to these reasons, MANET require strict

ISSN: 1738-9976 IJSIA

security protocols and excellent cryptographic techniques to make the information and network more secure so that the system can achieve its security goals like authenticity, confidentiality, integrity and non-repudiation. From last few years of development in MANET, security is the domain where researchers are paying more attention and surveying to produce the more secure techniques.

2.1. Attacks in MANET

MANET suffers from variety of attacks that disrupts its functioning. The attacks can be external or internal, active or passive. These attacks are difficult to detect sometimes the cause of the attack is also not known. Routing protocols are required for the efficient routing of the packet from source to destination. Each routing protocol has a security issue associated to it. So, whether its routing or unencrypted message each layer of the TCP/IP model requires the security at its best [4]. The classification of attacks in MANET is as follows: -

2.1.1. Passive Attacks:-In these attacks, the attacker learn and make use of information; keeping the routing protocol undisturbed. Also, the system resources are not affected. The attacker doesn't harm or modify the data. These attacks are in habit of eavesdropping on or monitoring of transmission. These attacks are difficult to detect as there is no involvement of data alteration. These attacks are prevented by the means of encryption. Some examples of passive attacks are as follows:

2.1.1.1. Eavesdropping: -The major drawback of transmission through wireless medium is that any device furnished with transceiver and present within the radio range is capable of hearing the information being transmitted. This calls for the urgent need of encryption techniques. Otherwise, any third party can extract and hears the useful information which is not desired. These attacks can be prevented using spread spectrum techniques.

2.1.1.2 Traffic Analysis and Location Disclosure:-In these types of attacks, the opponent might observe the message patterns, target location, host's identity involved in communication, message frequency and length. Although passive attacks do not directly influence the functionality of the network, but in some applications like military communications, attacks like traffic analysis or eavesdropping leads to information disclosure which can prove costly.

2.1.2. Active Attacks:-In these types of attacks the attacker seeks to influence the functionality of the network by altering or modifying the message. These attacks are difficult to prevent because attacker can introduce them in the network in variety of ways. Active attacks are so brutal, that they can degrade the whole network performance. [5]

2.1.2.1. Routing Attacks: -whenever the packet is routed in the network, there might be the chances that information is leaked or attacked by the malicious nodes. Most of the routing protocols such as AODV and DSR offer variety of attacks. There are many routing attacks such as blackhole attack, rushing attack, grayhole attack *etc*.

2.1.2.2. Black Hole Attack: -This type of attacks occurs when the route request message is broadcasted in the network and if there is any malicious node present, if receives the request message replies the source node with the reply message and advertise itself to have the shortest route to the destination. In this way a malicious fools the source node and extracts the useful information transmitted in the network. It can be external or internal [1].

2.1.2.3 Internal black hole attack:-In this, the malicious node is present inside the network in between the routes from source to destination. These attacks are difficult to detect so defending them is quite a challenge.

2.1.2.4 External Black Hole Attack:-In these attacks, the malicious node physically stays outside the network and disrupts the entire network by creating congestion in the network.

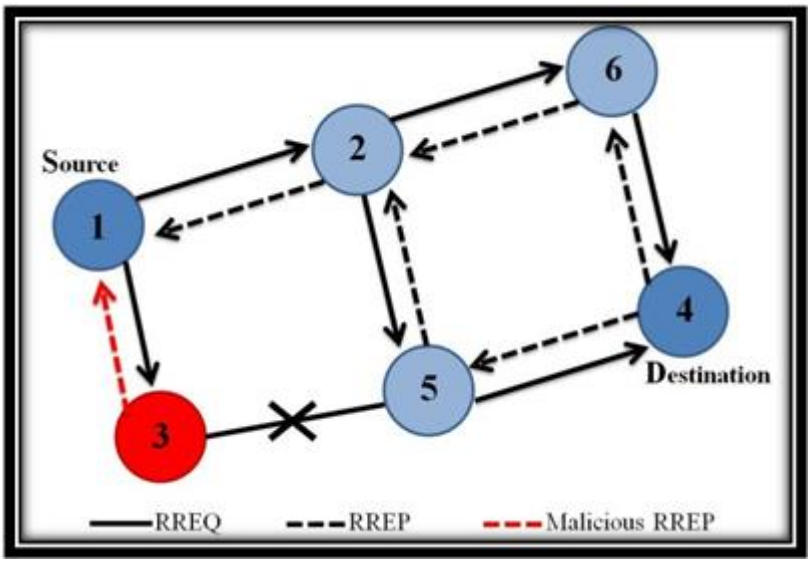

Figure 1. Blackhole in MANET

In Figure 1., we assume that node 1 wants to send the data to node 4. So, it sends RREQ packets to all the nodes. Node 3 which is the malicious node sends the false reply message that I have the path to reach to the destination. So, the packet is forwarded to node 3 which drops the data packet and acts as blackhole node on the way to the destination [6]

3. Research Methodology

In this paper, the technique is proposed which will detect and isolate black hole in minimum amount of time. A threshold value of throughput will be calculated and if the threshold value will be less than the defined threshold value then source will trigger the fake request route packet in the network and in which the malicious node will respond back. All other nodes which are legitimate will not revert back to the source node. This will lead to the detection of malicious nodes in the network. The source node will maintain a blacklist of malicious nodes in the network. The source node will adapt the technique of multipath routing to establish secure and efficient path to the destination.

Dynamic Threshold Algorithm

```
01 double threshold=0.9;
02 initial Proactive defence ();
03 double dynamic (threshold)
04 {double T1, T2;
05 T1=calculate the time of PDR down to threshold;
06 If (PDR< threshold)
07 Initial Proactive defence ();
```

```
08 T2=calculate the time of PDR down to threshold;
09 If (T2 < T1){
10 If (threshold < 0.95)
11 threshold=threshold + 0.01;
12 }
13 Else {
14 If (threshold >0.85)
15 threshold=threshold-0.01;
16 }
17 If (simulation time <800) {
18 return threshold;
19 Dynamic (threshold);
20 If (simulation time <800) {
21 return threshold;
22 Dynamic (threshold);
```

4. Results and Discussion

In proposed work, developed algorithm will focus on the finding of blackhole creating nodes with the help of multiple path selection and detection is done through multiple path detection from nodes connected in the network. This research will provide a stable and effective blackhole prevention mechanism which can be directly applicable to the real-time environment for Mobile Ad-hoc Devices.

4.1 End to End Delay comparison is shown between the Adhoc On Demand Distance Vector (AODV) and Enhanced Adhoc On Demand Distance Vector(EAODV). The delay is defined as average time taken by data packets to arrive the destination and is calculated using:

Delay = sum (arrive time – sent time) / sum (no. of connections)

As shown in Figure 2, after implementing the novel technique for detection and isolation of Blackhole attack, the delay of the network is reduced by 50.51%.

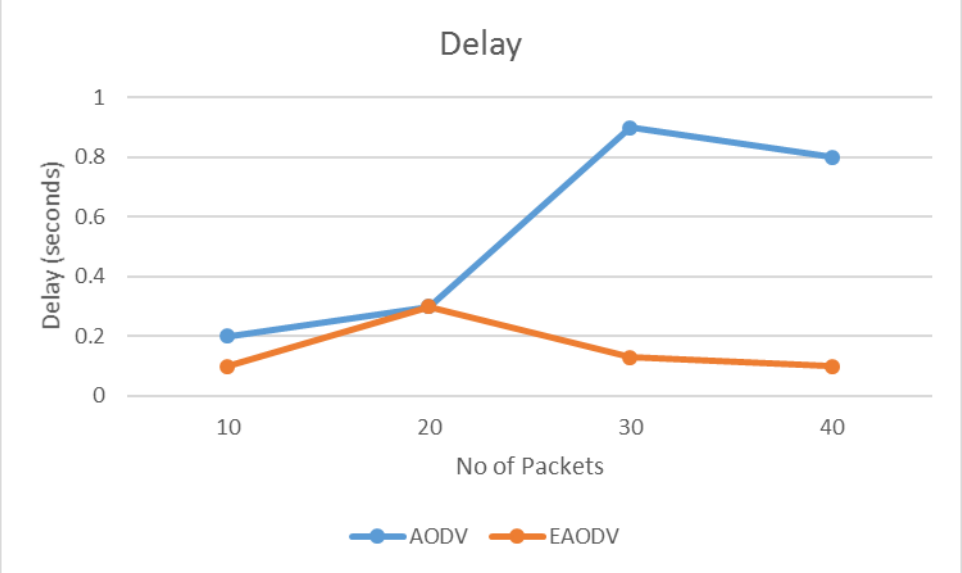

Figure 2. Comparison of Delay

4.2. Packet Loss is defined as total number of packets lost during simulation. Packet loss in the EAODV is less as compared to AODV and is calculated as:

Packet loss = No. of packets sent – No. of packets received

The packet loss is reduced by 60.62% after eliminating the Black hole node as shown in Figure 3.

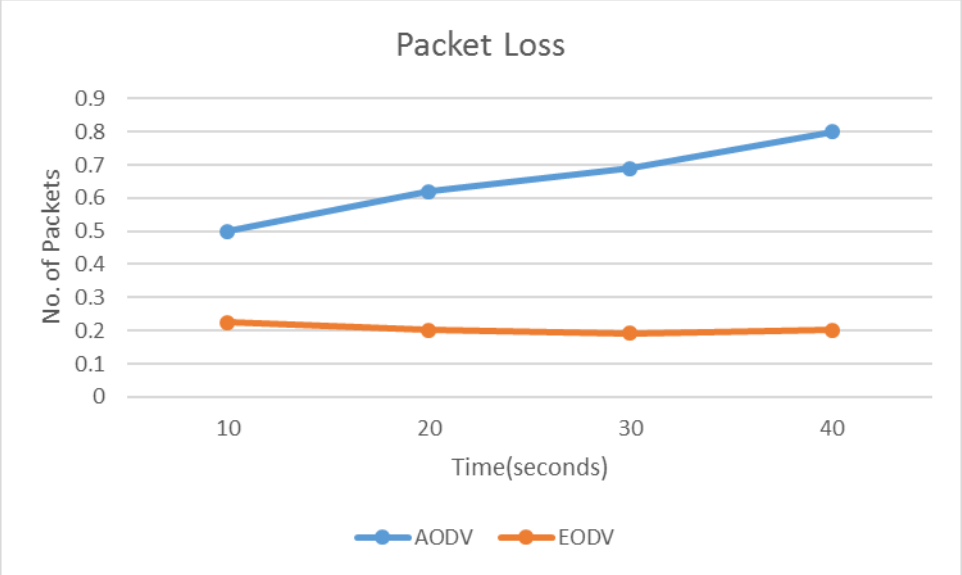

Figure 3. Comparison of Packet Loss

4.3. Throughput of a network is defined as number of data packets transmitted in bits per second. Throughput of the network is increased in comparison to AODV as the number of packets dropped during transmission are less.

Throughput = Maximum no of data packets transmitted / Round trip time

Round trip time is time taken to arrive the packet at destination and time for the reception of acknowledgement from the destination to source. The new throughput of the network is increased by 32.76% after the detection and isolation of Black hole node as shown in Figure 4.

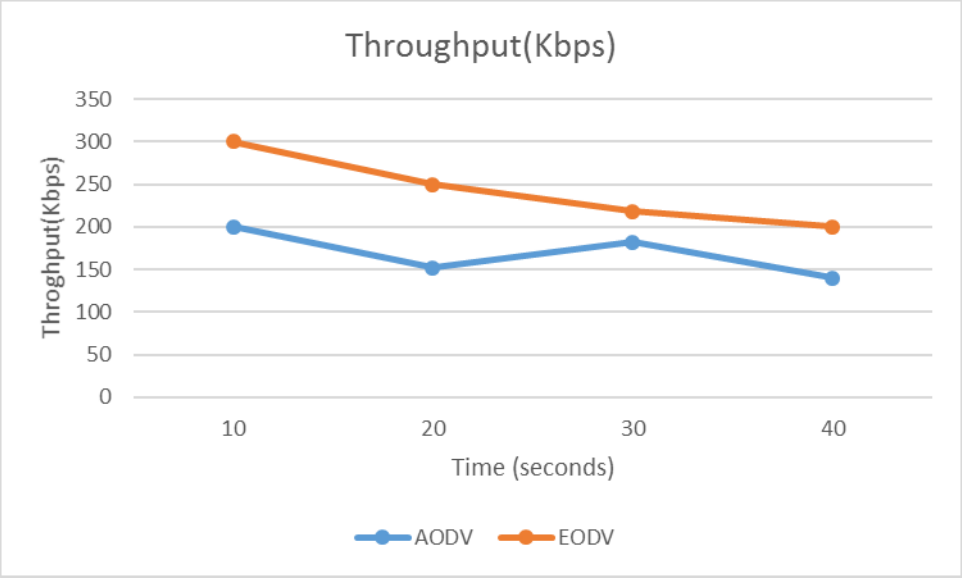

Figure 4. Comparison of Throughput

4.4. Energy Consumption in MANET is the total amount of energy spent while transmission of data packet from each node in a multi hop communication. Most of the energy is consumed while transmission of data packets to a Black hole node and in changing the routing path. The energy consumption for EAODV protocol is reduced by approximate 60.84% as shown in Figure 5, makes the network more efficient.

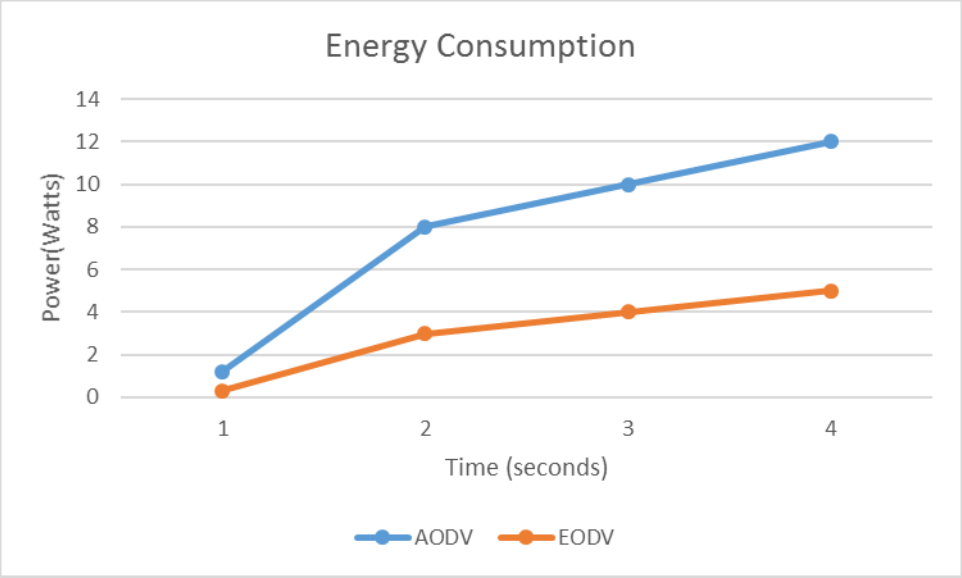

Figure 5. Comparison of Energy Consumption

4.5. As shown in Figure 6. Packet Delivery Ratio in Mobile Ad hoc Networks is the ratio of number of delivered data packets to the destination. This illustrates the level of delivered data to destination. It can be calculated as:

PDR = sum (No. of packets receive)/ sum (No. of packets sent)

After the implementations of the novel technique, the packet delivery ratio is increased by 25% approximate.

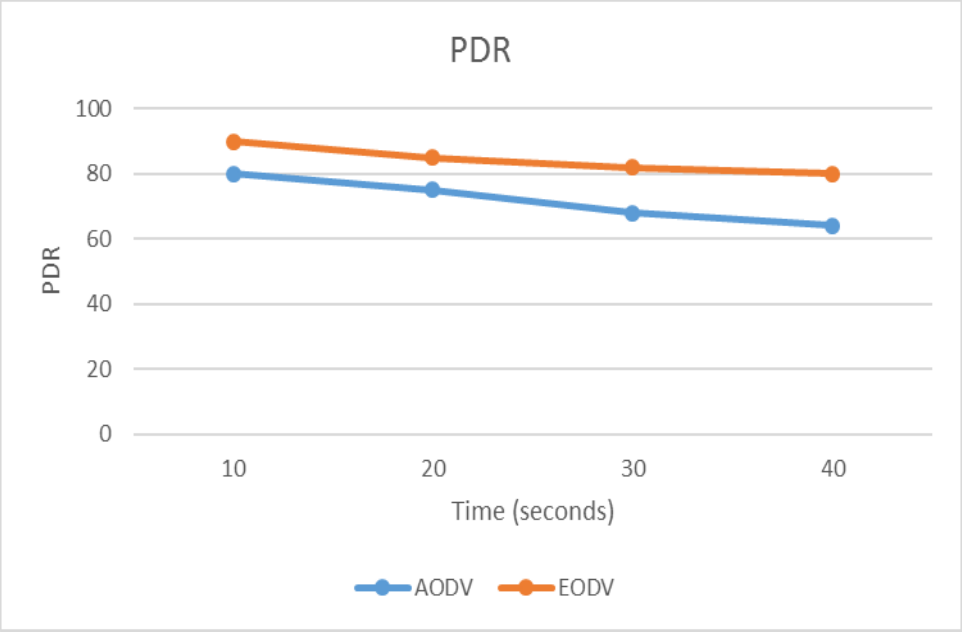

Figure 6. Comparision of PDR

5. Conclusion

As the mobile ad hoc network is self-configuring and self-preserving in nature and due to its abruptly changing topology it mainly suffers from routing attacks. Due to the presence of any blackhole node between the transmission path, all the data packets are lost or even dropped during the transmission, which leads to the following problems such as increase in routing overhead, increase in energy consumption and also a significant increase in packet loss. A novel technique based on threshold value is proposed which is helpful for the detection and isolation of blackhole attack. In future, blackhole attack can be detected and isolated for multipath routing.

References

[1] Bo Sun Yong, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference, **(2003)**, pp. 490-495.
[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Journal of Communication Network, vol.3, no.4, **(2004)**, pp. 60-66.
[3] E M Royer, CK Toh," A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, vol.6, no.2, **(2012)**, pp.46-55.
[4] Brijesh Soni, Biplab Kumar Sarkar, Arjun Rajput, "Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails," Proceedings of All India Seminar on Biomedical Engineering, **(2012)**, pp.285-292.
[5] F.Tseng, L. Chou and H.Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", Journal on Human-Centric Computing and Information Sciences,vol.1, no.4, **(2011)**,pp. 1-16.
[6] Sandeep Kumar Arora, Gujot Singh Gaba," Improvement in data routing on the basis of stability", Indian Journal of Science and Technology, vol.9, no.3, **(2016)**, pp.1-6.

Authors

Shivani Vijan, is currently pursuing M. TECH in Electronics and Communication Engineering with Spl. in Wireless Communication Systems at Lovely Professional University, India. Her research interests include Adhoc Networks and Cryptography.

Sandeep Kumar Arora, is currently pursuing Ph. D. in Electronics & Electrical Engineering with Spl. in *Design of Secure Initiation Protocol in VANET*. He is working as an Asst. Prof. in Lovely Professional University since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Adhoc Networks Communications and Cryptography. He is a member of IEEE and also the author of more than one dozen research papers indexed in Scopus.