ELK ASIA PACIFIC JOURNAL OF COMPUTER SCIENCE AND INFORMATION SYSTEM
ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

ELK
Asia Pacific Journals
www.elkjournals.com

ANALYSIS OF WORMHOLE ATTACK IN MANET BY VARYING NUMBER OF NODES

Neha Sharma	Shahjahan Ali
M.Tech Scholar	Assistant Professor
Dept. Of CSE	Dept. of CSE
SRMSCET, Bareilly (UP) India	SRMSCET, Bareilly (UP) India
neha2504sharma@gmail.com	shahjahansrms@gmail.com

Abstract

Mobile adhoc networks are collection of mobile nodes. MANET is very flexible network due to mobility of nodes. But this flexibility comes with the price of security threats. Security in MANET is the vulnerable aspect. There are a number of attacks exist to harm the communication of nodes and harm the data packets as well. Here in this paper we discuss different-different attacks of MANET. Wormhole is one of the famous attacks in MANET. We discuss wormhole in detail and also analyze the effects of number of nodes variation in PDR and Throughput of MANET, under Wormhole attack.

Keywords—*MANET; ADHOC; mitigation*

I. INTRODUCTION

This paper consist different types of attacks and mitigation techniques. Due to mobility in mobile adhoc network it becomes weak in security. Flexibility existence makes MANET an open scenario for attacker. From a long time it had been seen a no. of attacks happened in mobile adhoc network. Thereafter mitigation techniques also developed. In this paper we tried to cover all of the attacks and most suitable mitigation techniques for that.

Different Types of Attacks in MANET

Segregation of MANET attacks can be viewed as following chart below,

Attacks in MANET can be classified on the basis of some special characteristic. Here in this review paper attacks are classified into two categories: active attacks and passive attacks. These two types of attacks are indifferent in nature as the first one attack the network as well as interrupt the network. It also affects the operation [2] where the second one only attacks to steal the information. **(Ref Figure – 1)**

a. Active Attacks

Active attacks not only steal the data but also change it. Attacker can modify the data or can also exchange the data with someone else as dropping some data packets or remove some data packets [3]

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

and so on. Active attacks can be internally or externally done.

1. ***Black-Hole Attack***

In blackhole attack a node behaves like malicious node means it drops the information or it can use another way. It can deliver multiple message of having routing information from source to destination and then nodes in network sends data packets through this malicious node. **(Ref Figure – 2)**

To mitigate the blackhole attack in MANET authentication is used of a true node. Authentication of node is done by having multiple route reply messages. For a clear understanding when a node wants to forward its packet to destination it should have multiple reply of its route request so after verifying a safe route it starts its transmission.

2. ***Flooding Attacks***

Flooding attack, attacks like it name it floods the network. Here it floods the network by route request or data packets. Its main work is to block the network. Fake RREQ's are used as a weapon to flood the network or block the network so the data sending rate will be slow down. It can be done in network in two ways: either by RREQ Flooding or by DATA Flooding. These attacks can make network failures as well as restrict the node to perform their services [4].

The below **Ref figure 3** is an example of RREQ flooding attack where the task of flooder node is to block the network by sending multiple request messages for the node which may be a part of network or maybe not. As in the above example the flooder node L sends RREQ for node R which is not present in that network. By performing this task flooder node disable the way of RREQ for other genuine nodes by having network bandwidth itself.

In **Ref figure 4** DATA flooding is shown where RREQ is send to node K, after getting acknowledgement from node K. Node J starts to sends unusual data to node K repeatedly thus it start blocking the network with the help of data packets.

3. ***Wormhole attack***

In wormhole as soon attacker node have data packet it tunnel that packet to another region in that network as in the figure when node x has any data packet it tunnel that data packet to z.

4. ***Denial of Service Attack***

DOS is an attack where attacker node sends multiple messages to server for authentication of invalid request as server denied its request; this puts the server on wait for verification. Attacker node jams the network by repeating the above step and thus it makes the network disable for genuine user's. genuine users always find the network busy to send their genuine request**. (Ref Figure – 5(A))**

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

B. *Passive Attacks*

Passive attacks in MANET are second type of attack, where only information can be overhear or bypass but the network remains unaffected by this. It just affects the secrecy of your information.

1. Eavesdropping

Eavesdroppers [6] are the third party which acts as an attacker and they can overhear information or data packets in the network. Attacker nodes just eavesdrop confidential information does not make any harm to network but later on that information can be used by any malicious or selfish node for any kind of maliciousness. **(Ref Figure – 5 (B))**

2. Traffic Monitoring

Traffic Monitoring attacks are used to identify information so it can be used to trigger other types of attacks.

II. PROPOSED WORKING MODEL

The aim of our paper is to analyze behavior of MANET. In this paper we analyze effect of nodes in wormhole attack. We are focusing on the behavior of MANET's parameters as throughput and Packet delivery rate (PDR). After steady change in number of nodes what happened in throughput and in PDR. Wormhole attack is implemented in this paper and it has certain rate of dropping data packets. So eventually it is also has an effect on throughput and on PDR. So we have to check the effect of nodes variation on parameters.

III. SIMULATION SETUP AND RESULTS DISCUSSION

a. Simulation Setup

To simulate the scenario, we used NS2.35 on UBUNTU 16.04 LTS. The simulation parameters are given below in **(Ref Table – 1).**

Performance Metrics

These two Metrics are used to analyses the scenario by varying number of nodes in MANET:

i. *Throughput* – Throughput is the amount of data transferred successfully from source to destination.

ii. *Packet delivery rate* – PDR is a ratio of packet received to packet originated.

b. Result Discussion

Performance of scenario can be analysed with the help of xgraph an utility under NS2.35. Following figures shows variation in throughput and in pdr by varying the numbe of nodes.

Ref Figure 6 shows Throughput graph. In this scenario we plot the Throughput at three variances when node is 16, 20 then 25. From the graph it is clear when nodes are less then throughput is less and as the number of nodes increased throughput also increased.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

Ref Figure 7 shows throughput graph. In this graph we can see that PDR is decreasing and being constant after some time as the network having wormhole attack so packet drops also take place which gradually support LESS packet delivery rate.

IV. CONCLUSION

This paper has result on the basis of two parameters throughput and PDR. We analyzed performance of Wormhole Attack with AODV routing protocol. The distinct of this paper is that analysis of wormhole attack under different nodes is done. And the result shows that throughput is increased with number of nodes and if any detection technique would be applied with wormhole attack then other parameters like end to end delay, packet delivery rate should be increased as well.

ACKNOWLEDGEMENT

The authors want to thank their family members for supporting and encouraging for her work. A special thanks to Mr. Shahjahan Ali for his guidance and support.

REFERENCES

[1] Neha Kamdar, Vinita Sharma,Poorva Kakani, "Study of Various Attacks in MANET and Elaborative Disscussion of RREQ Flooding Attack and Its Solution," IJCSIT, vol. 7(1) , pp. 104-107,2016.

[2] Gagandeep, Aashima, Pawan kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A- Review", IJEAT, vol. 1, 2015.

[3] K. Raj Kumar, S. Prasanna, "Complete Analysis of Various Attacks in MANET", International Journal of Pure and Applied Mathematics, vol. 119, 2018.

[4] Daniel S. Yeung, Shuyuan Jin, Xizhao Wang , "Covariance Matrix Modelling and Detecting Various Flooding Attacks", IEEE,Vol. 37, 2007.

[5] Roshani Verma, Roopesh Sharma , " New Approach through Detection and Prevention of Wormhole Attack in MANET", ICECA, 2017.

[6] B. Wu, J. Wu and M. Cardei, " A Survey on Attacks and Countermeasures in Mobile Adhoc Networks", Springer, 2006.

[7] Ashish Bagwari, Raman Jee, Pankaj Joshi, Sourabh Bisht, "Performance of AODV Routing Protocol with increasing the MANET nodes and it's effects on Qos of Mobile Adhoc Networks", IEEE, 2012.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

LIST OF FIGURES

Fig.1. Classification of MANET Attacks [1]

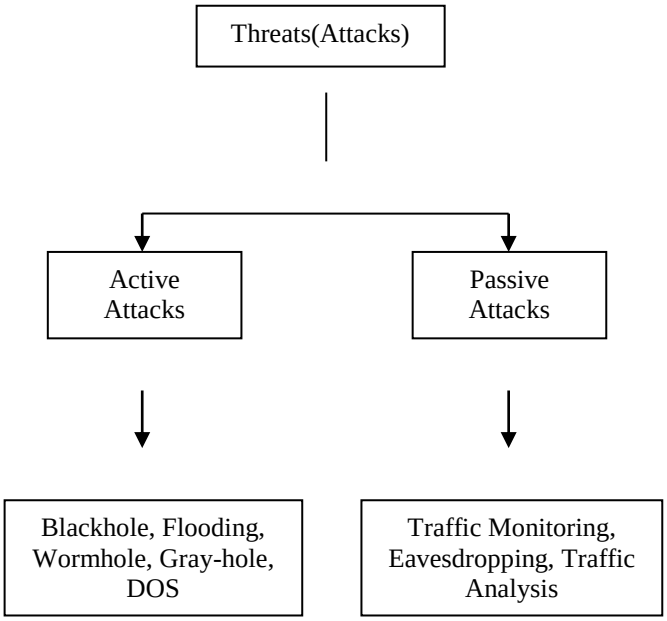
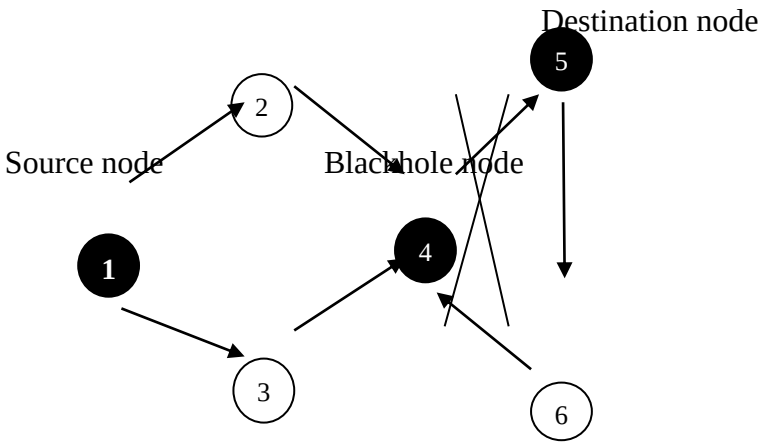


Figure- 2. Black-Hole Attack [3]



ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

Figure - 3. Flooding Attack by RREQ Flooding [1]

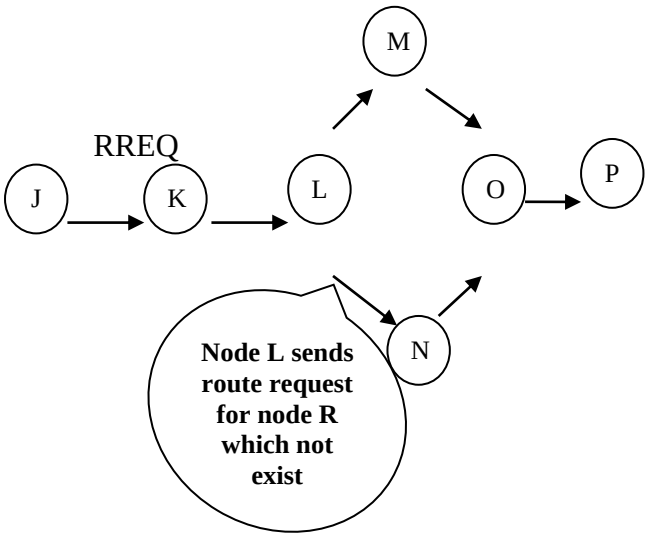
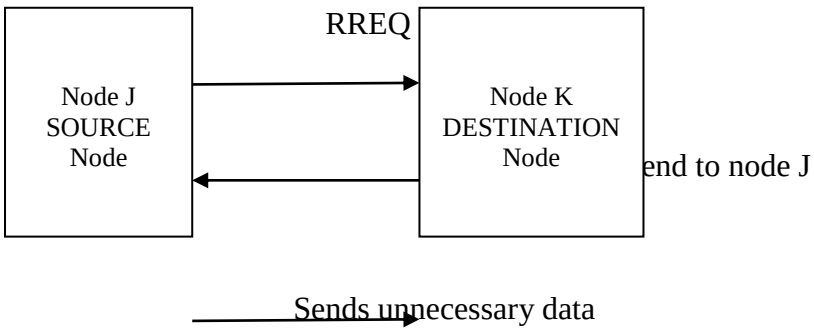


Figure- 4. Flooding Attack by DATA Flooding [1]



ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

Figure- 5 (A). Wormhole Attack [5]

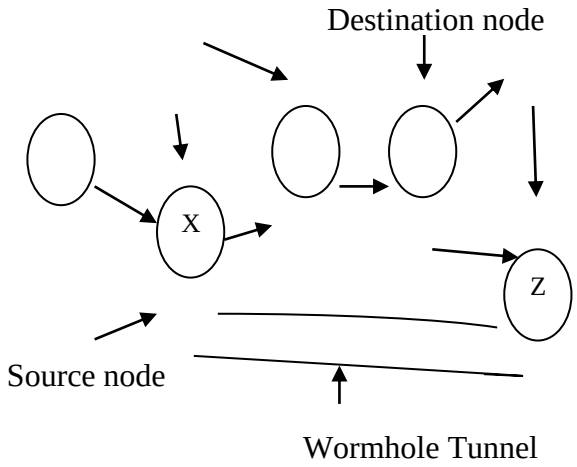


Figure- 5 (B). Eavesdropping Attack [3]

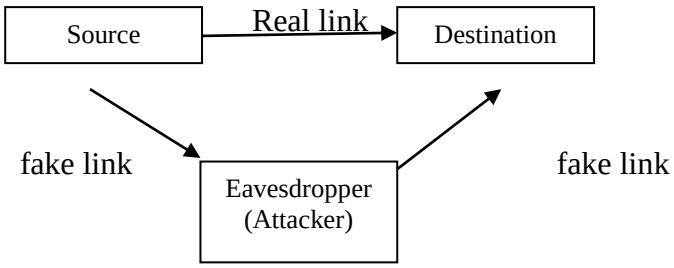
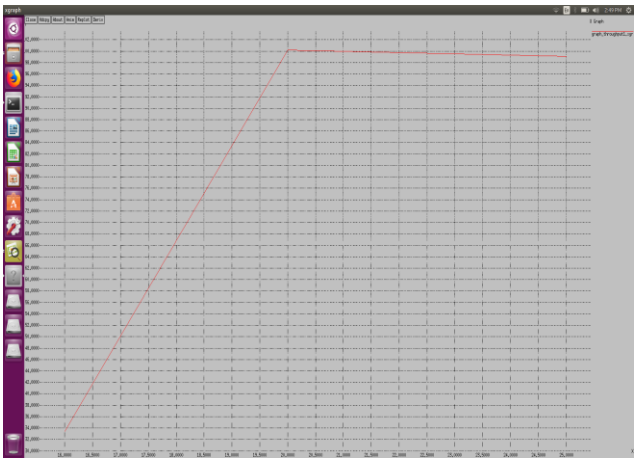
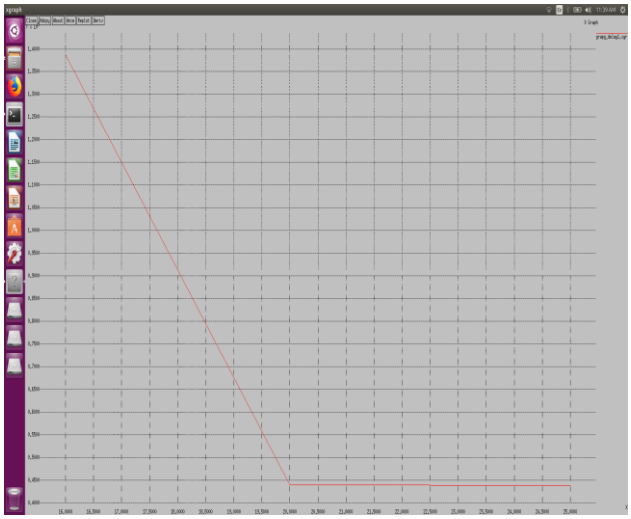


Figure- 6. XGRAPH of Throughput



ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 5 Issue 1 (2019)

Figure- 7. XGRAPH of Packet Delivery Rate



LIST OF TABLE:-

TABLE 1- SIMULATION PARAMETERS

PARAMETER	VALUE
Numbers of nodes	16,20,25,30…..
Size of area	500X500
Traffic Type	CBR
Protocol	AODV
Standard ADHOC Speed	20 m/s
Attack	WORMHOLE