DOI: http://dx.doi.org/10.26483/ijarcs.v12i2.6701

ISSN No. 0976-5697

Volume 12, No. 2, March-April 2021

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IMPLEMENTATION PAPER ON COUNTERING OF BLACKHOLE AND SINK HOLE ATTACK ON MANET WITH DSR PROTOCOL

Amanpreet Kaur
Department of Computer Science& Engineering , RIMT University,
MandiGobindgarh,Punjab , India

Dr Ashish Oberoi
HOD Department of Computer Science& Engineering ,
RIMT University, MandiGobindgarh,Punjab , India

Er Jasdeep Singh
Department of Computer Science& Engineering,RIMT
University, MandiGobindgarh,Punjab , India

Abstract: Many applications of Wireless Mobile Communication are used in military, defense etc .however this type of network have many constraints mainly including power constrains, less range of communication & insecure transmission channel which makes it more vulnerable to attacks .such as sinkhole and black hole attack which hampers the communication by attacking on data traffic and communication links on which packets are routed. The attack which operates by falsely claiming a fresh route to destination is a kind of denial of service is known as Sink hole attack. On the other hand black hole attack, intentionally dropped the incoming packets through malicious node in between the intermediately nodes. In this research paper we can examine and investigate the impact of sink hole and black hole attack on the performance of MANET network using DSR protocol in terms of throughput ,packet delivery ratio over the network.

Keyword- Sinkhole attack, black hole attack, MANET, DSR routing protocol, OPNET tool.

I . Introduction

Mobile adhoc networks playing an important role in wireless communication. It is collection of autonomous nodes. Network Topology can be determines by its each node .mobile adhoc network doesn't have any pre exciting infrastructure and centralized control support. it can applied in disaster rescue management ,military surveillance and robot network[1]. Communication between two nodes depends upon which are exist between in source and destination and relies on distributed cooperation of nodes. Many nodes can be gain and loss in manet simultaneously and nodes are pushed into resource constraints such as storage, energy capacity and bandwidth.manet are thus more emotional attack to a network. To calculate the performance of any routing protocol , various performance metrics such as, end to end delay, and PDR packet delivery ratio and throughput & packet loss are used.Manet can be classified into two major groups: internal and external .In internal attack a compromised node of same network is originated .Nodes such as Internal nodes can be drop, formulate, modify, eavesdrop or misroute data packets. Routing process is not participating in the External attack howeverinterrupts network operations like flooding, dos, or cut off nodes from network[11]. where a malicious node can read all packets by falsely claiming a fresh route to the target. is a kind of denial of service is known as Sink hole attack.In Sink Hole Attack the node can drop the data coming from the source .So it will difficult to know whose node will read the data.

II.Sinkhole Attack

Sinkhole attack is a possible threat to meant environment, as it grasps the dynamic property. A sinkhole node channelizes all the traffic from a network through a compromised the traffic and exploits the information .Sinkhole attack objective is to keeping itself updated and attractive is achieved. Sinkhole nodes draw other nodes attraction towards it by routing packets propagated. In sinkhole attack data packets are sent throughout the network with high quality and fictitious[2]. The whole traffic in sinkhole attack is diverted into to all surrounding node so that original data packets ignored. where a malicious node can read all packets by falsely claiming a fresh route to the targetis a kind of denial of service known as Sink hole attack. In this Sink Hole Attack analysis the node coming from the sourcecan drop the data .So it will find difficult to analysis which node will read the data .

Blackhole attack

In Black hole attack, a malicious node waits for a route discovery process to begins from its neighbors .Once its neighbor broadcasted RREQ packet, malicious node sends a false RREP packet immediately with a greater sequence number[3]. So, the RREP packet received from other node is ignored by the source source node consider that the malicious node is having a fresh route almost the destination

node[8-9]. It does not allow forwarding any packet anywhere and also takes all the routes almost it .

III. Problems of sinkhole attack and blackhole attack

In sinkhole attack a malicious node tries to broadcast fake routing address to its neighbor so to attract data to itself and make fake image and let them know itself on the way to definite nodes[4]. In this way it attempts to draw all network traffic to itself. After thatit drops the packet silently and sometime also it adjust the data packet which increase network above, decreases boosting power consumption; finally put away the network. . In this type of black hole attack, where a malicious node claim to have the fresh and shortest route to the destination. Even if no such route exists[10]. As a result, the data can drop or later by the malicious node..

IV. DSR

The on-demand routing protocols(DSR) which executes the path-finding process when a path is required by a node[12]. Dynamic source routing protocol (DSR) is a representative on- demand protocol designed to reduce the bandwidth consumed by control packets in ad hoc wireless networks [13].

Our proposed method is stated on the situation of dynamic source routing protocol. This research is mainly focuses on performance of the sinkhole attacker on dynamic source routing (DSR) protocol positively.

Packet drop

Packet drop is calculated as the difference between the numbers of packets sent by the source node to that of the number of packets received by the target node[14]. As sinkhole as well as black hole is a malicious node it may drop the packets that are being collected by it. Hence the packet drop will increase in the existence of sinkhole attack.

Packet delivery ratio

PDR is the ratio of number of packets collected at target node to that of number of packets sent by source node. It is disclose in percentage. As sinkhole as well as black hole will drop and hold the packets of the network the packet delivery ratio (PDR) of the network will reduce[5]. The packets which are not expressed are either dropped or may be forwarded to some other node in the network.

Network throughput:

Throughput is the total number of packets received by the target node over a period of time and the metric used to calculate the throughput is kbps[6]`. The reason is sinkhole as well as black hole has connection to more packets on the network and sinkholeas well as blackhole will not allow the packets to reach the target and hence the throughput decreases [7].

V. Simulation results analysis

To study the effect of sinkhole attack on DSR protocol, the consecutive network parameters like throughput, packet drop and packet delivery ratio are evaluate without the sinkhole on the network and with the sinkhole nodes perform on MANET.

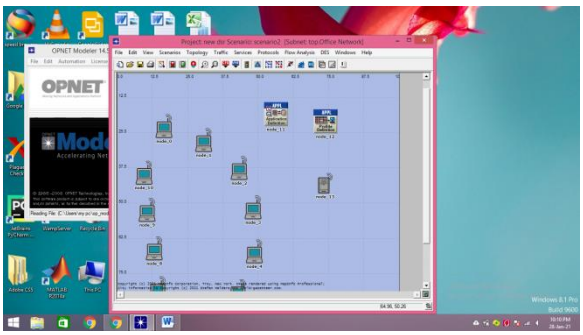

Fig 1 Manet with DSR Protocol

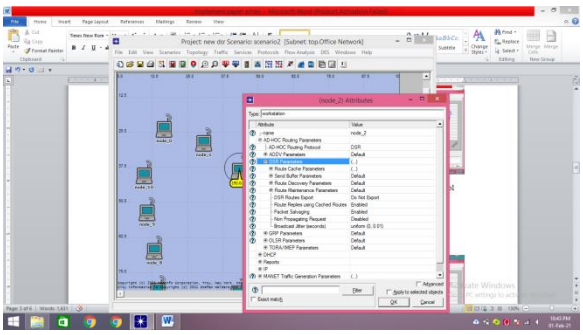

Fig 2 Manet network with DSR Protocol

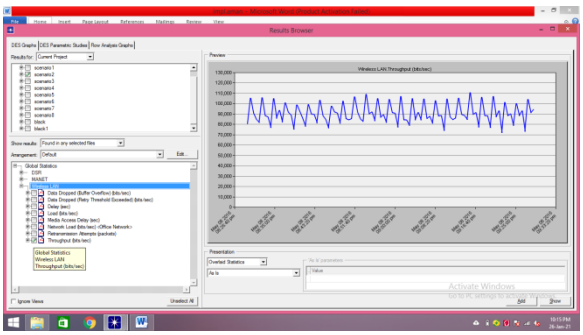

Fig 3Throughput bit/sec with DSR protocol

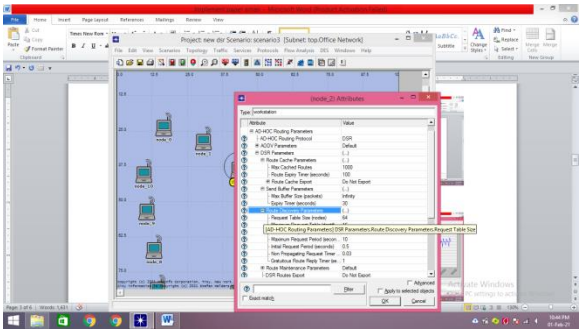

Fig 4 Manet Network (DSR) with Black hole attack

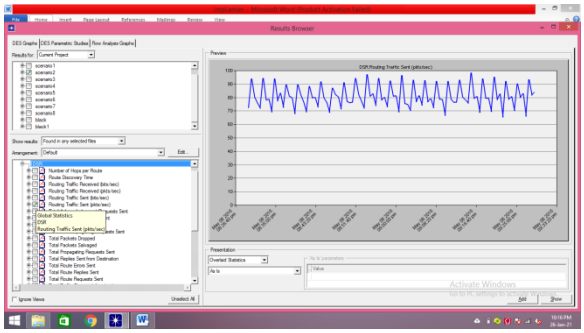

Fig 8 Traffic sent with DSR protocol

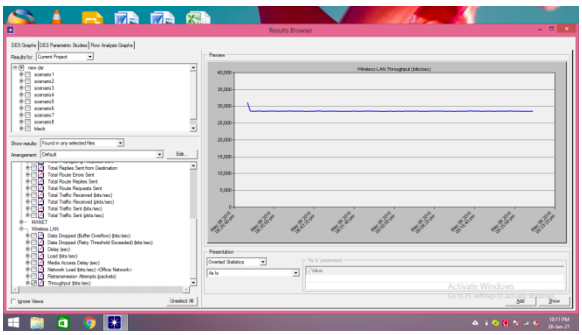

Fig.5Throughput bit/sec withblack hole attack

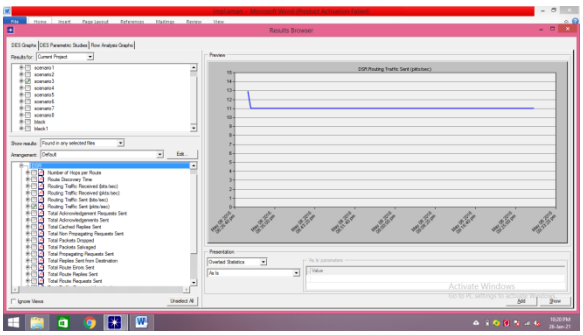

Fig 9 Traffic sent with Sink hole attack

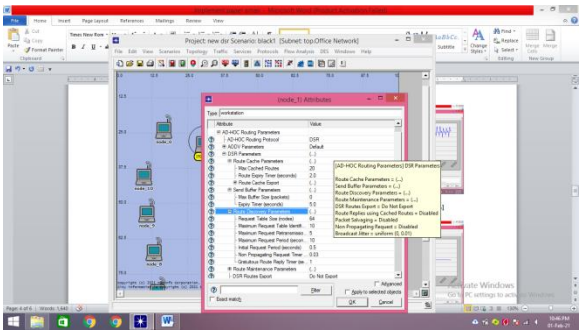

Fig 6 Manet Network (DSR) with Sink hole

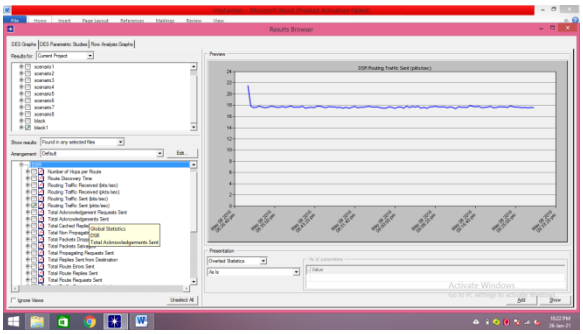

Fig 10 Traffic sent with Black hole attack

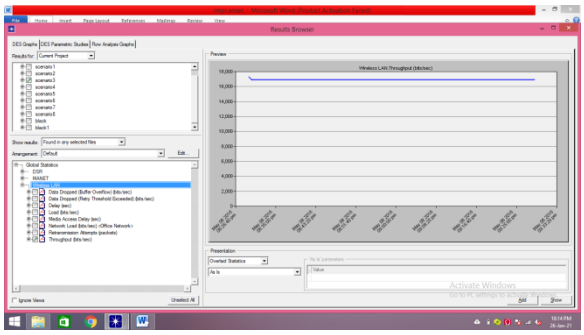

Fig 7 Throughput bit/sec with Sink hole attack

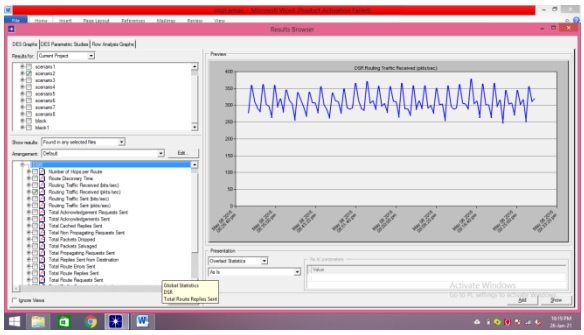

Fig 11 Traffic Received with DSR Protocol

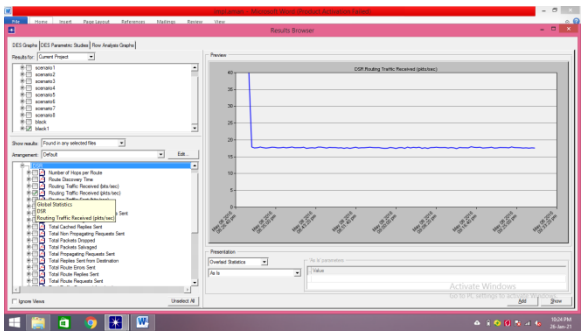

Fig 12 Traffic Received with Black hole attack

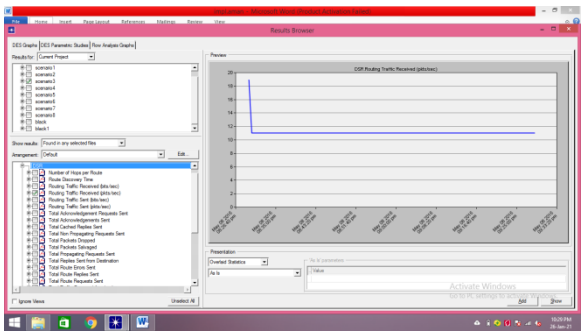

Fig 13 Traffic Received with Sink hole attack

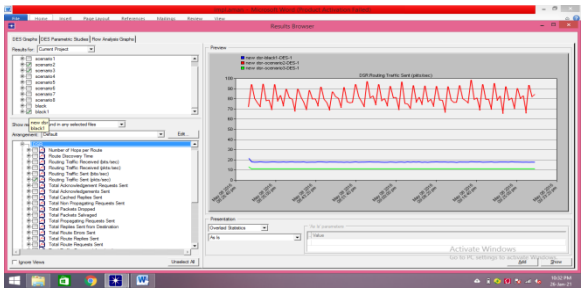

Fig14 Comparison between Traffic sent with manet network,Blackhole,Sinkhole attack

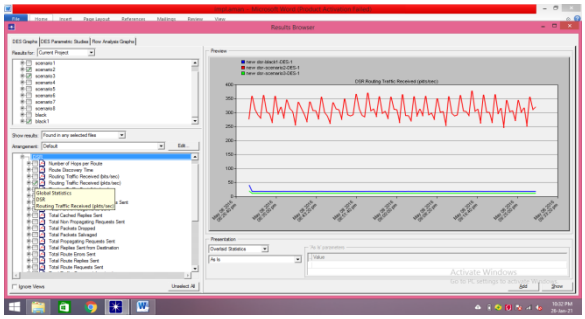

Fig15 Comparison between Traffic Received with manet network,Blackhole,Sinkholeattack

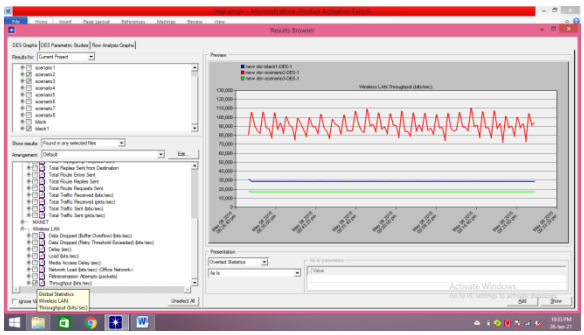

Fig16 Comparison between throughput bit/sec with manet network,Black hole,Sinkholeattack

VI. Conclusion

Due to significant using and development of many applications & computing activities base on MANET network,the security is going to be crucialCan as there are no of risks associated with it. In this paper ,the impact of sinkhole and black hole attack is analyzed on MANET network using DSR protocol. The performance is measured to check the impact of these attacks in terms of throughput, PDR as a parameter. We have seen that there will be drastically decrease in performance of network.so,blackhole attack as well as sinkhole attack reflects significant degradation on the performance of network.In future a more improvedmechanisms should be developed to detect &prevent such attacks .This work will also implemented to analyze the impact on performance of other reactive routing protocol such as AODV.

VII. REFERENCES:

[1] A Review study on the use of Manet for Wireless Devices Kaur, Jaspreet and Singh, Alankrita, A Review Study on the Use of MANET for Wireless Devices (April 10, 2020).

[2]. Lanka Chris SejaphalaThe Design of a Defense Mechanism to Mitigate Sinkhole Attack in Software Defined Wireless Sensor Cognitive Radio Networks April 2020.

[3]. MahuwaGoswami, Prashant Sharma, AnkitaBhargava Black Hole Attack Detection in MANETs using Trust Based Technique ISSN: 2278-3075, Volume-9 Issue-4, February 2020.

[4]. Mohammed AlGhazaliHamza Khalil Omnia Omer Hassan2,Comparative Analysis in MANET Performance evaluation for routing protocol jan 2020.

[5]. HarjeetKaur, ManjuBala, VarshaSahni ,” Study of Blackhole Attack Using different Routing Protocol in Manets,”IEEE,Vol-2,Issue 7,july 2013,pp.3031-3039.

[6]. Mrs.Padma, Mr.R.Suresh,” Literature Survey on latest research issues in MANET ,”International Journal of Advanced Research in Computer Engg& Technology,Vol-2,Issue 7,july 2013,pp.2384-2388.

[7].S.Kannan,T.Maragatham,S.Karthik,V.P.Arunchalam,” A Study of Attacks,Attack Detection and Prevention Methods in Proactive &Reactive Routing Protocols ,” 2011,pp.178-183.

[8].G.Vijaya Kumar, Y.VasudevaReddyr, Dr.M.Nagendra ,”Currnet Research Work on Routing Protocols for

MANETS:A Literature Survey", International Journal on Computer Science & Engg,Vol.2,Issue3, 2010,pp.706-713.

[9]. Anjaly Joy, SijoCherian," Black Hole Attack & its Mitigation Techniques in AODV and OLSR Based Manets", International journal of Computer Science & EnggTeChnology.Vol.4,issue6, june 2013,pp.740-745.

[10]. Om Shree ,FrancisJ.Ogwu," A Proposal for Mitigating Multiple Black-Hole Attack In Wireless Mesh Networks" ,Wireless Sensor Network.Vol.5 .2013,pp76-83.

[11] P,.Jacquet, P.Muhlethaler, T.Clausen, A.Laouiti, A.Qayyum, L.Viennot," OptimiZed Link State Routing Protocol for Ad Hoc Network".

[12] G.Vijaya Kumar, Y.VasudevaReddyr, Dr.M.Nagendra ,"Currnet Research Work on Routing Protocols for MANETS:A Literature Survey", International Journal on Computer Science & Engg,Vol.2,Issue3, 2010,pp.706-713.

[13] H.Deng.W.Li and D.P. Aggarwal , Routing security in wireless AD Hoc network,IEEE Communication Magazine,2002, pp 70-75.

[14]Singh Jasdeep and Sharma Sukhwinder (2014), "A SURVEY ON ROUTING PROTOCOL IN MANET", Journal Of International Academic Research For Multidisciplinary, pp 341-342, ISSN: 2320-5083, Volume 2.

