International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 5, Issue 12 (February 2013), PP. 48-56

DOS Attack Severity on Static and Mobile Adhoc Network

SudiptaMajumder[1], Md. Anwar Hussain[2]
[1]Dept.of CSE, DUIET, Dibrugarh University,Dibrugarh,Assam,India
[2]Dept. of ECE, NERIST,Nirjuli, Arunachal Pradesh, India

Abstract:- A wireless ad-hoc network is a collection of autonomous nodes that communicate with each other by each node acting as router and maintaining connectivity in a decentralized manner. The network topology is dynamic because the connectivity among the nodes may vary with time due to node departure, new arrivals and the possibility of having mobilenodes. In this paper, weexplore the effect on per session throughput of an adhoc network consisting offixed, and mobile non-malicious-nodes, by mobile and fixed malicious nodes making black hole and wormhole attacks and its severity.To simulate black hole attack 5, 10 and 14 malicious nodes were created for different scenarios, and for worm hole attack only one worm hole link was created.The 50 non-malicious nodes fixed, and mobile networks for cases of mobile and fixed malicious nodes attack were simulated in ns-2 where each odd numbered nodetransmits packets to the next even numbered node.

Key Terms:- Ad-hoc network, Black hole, Worm hole, Data rate, per session throughput.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most important areas of research in the recent years because it provides lots of opportunities regarding the services it provides but there are lots challenges to related protocols.[1, 2, 3, 13]. MANET is an emerging technology which enables users to establish communication among various physical devices regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network..A mobile ad hoc network (MANET) is a group of mobile wireless nodes that are set up without the use of any dedicated routers or base stations. Each ad hoc node acts as an end node as well as mobile routers for other nodes. Ad hoc networks can support many applications such as video streaming, military communications and sensor networks. In most ad hoc routing protocols, all the nodes cooperate to deliver and route packets in the network and all the nodes trust one another. However, this assumption is not true if the owner of the node does not belong to the same organization or has malicious intent in disrupting the operations of the ad hoc network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the newenvironment.
It includes: 1. Military Battlefield2. Sensor Networks3. Medical Service4. Personal Area Network.

Security solutions are important issues for MANET, especially for those selecting sensitive applications, and have to meet the following design goals while addressing the above challenges. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. In this paper, we will classify and discuss the different types of attacks from malicious or uncooperative nodes on a reactive routing protocol, the Ad hoc On-Demand Distance Vector (AODV) protocol.
The primary focus of this work is to explore on the attacks particularly blackhole attack and wormhole attack that affect the fixed and mobile adhoc network's throughput performance due to mobile and fixed malicious nodes. We consider here mobile malicious nodes attacking on fixed adhoc network, and fixed malicious nodes attacking on mobile adhoc network.

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc., as explained in [4].Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. These routing protocols are divided into two categories based on management of routing tables. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols, shown in the Table 1 and they are explained below.

Table1: categories of routing protocols

MANET ROUTING PROTOCOLS	
Table Driven Routing Protocols	***On Demand Routing Protocols***
DSDV	AODV
WRP	CBRP
GSR	DSRP
FSR	TORA
HSR	ABR
ZHLS	SSR
CGSR	

In Table Driven Routing Protocols, each node has to keep up-to-date routing tables. To maintain reliable routing tables, every node propagates the update messages to the network when the network topology changes. Because every node has information about network topology, Table Driven Routing Protocols present several problems.

1. Periodically updating the network topology increases bandwidth overhead,
2. Periodically updating route tables keeps the nodes awake and quickly exhaust their batteries,

Many redundant route entries to the specific destination needlessly take place in the routing tables. Destination-Sequenced Distance Vector Routing Protocol (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Fisheye State Routing (FSR), Hierarchical State Routing (HSR), Zone-based Hierarchical Link State Routing Protocol (ZHLS) and Clusterhead Gateway Switch Routing Protocol (CGSR) are Table Driven Routing Protocols[10].

II. ON-DEMAND ROUTING PROTOCOLS

These protocols take a lazy approach to routing [5] compared to Table Driven Routing Protocols. On-Demand Routing Protocols are not maintained periodically, route tables are created when required. When the source node wants to connect to the destination node, it propagates the route request packet to its neighbors. Just as neighbors of the source node receive the broadcasted request packet, they forward the packet to their neighbors and this action is happen until the destination is found.

Afterward, the destination node sends a replay packet to the source node in the shortest path. The route remains in the route tables of the nodes through shortest path until the route is no longer needed [10].
Cluster based Routing Protocols (CBRP), Ad-Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing Protocol (DSRP), Temporally Ordered Routing Algorithm (TORA), Associatively Based Routing (ABR), Signal Stability Routing (SSR) are On-Demand Routing protocols.

Since MANETs are networks with no fixed infrastructure and network functions are carried out by all available nodes, which are mobile and have constrained power resources. Consequently MANETs have increased sensitivity to node misbehavior in mobile ad hoc networks [11]. The first is external attackers, in which unauthenticated nodes can replay old routing information or inject false routing information to partition the network or increase the network load. The second type of attack is internal attack which comes from compromised nodes inside the network. Internal attacks are generally much harder to detect as compared to external attacks. Various types of attacks that can usually be seen are as follows:

A. Passive Eavesdropping

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications[15].

B.Selective Existence (Selfish Nodes)

This malicious node which is also known as *selfish node* and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviors are known as *selective existence attacks.* [7]. For instance, selfish nodes do not even send any

HELLO messages and drop all packets even if they are sent to itself, as long as it does not start the transmission. When a selfish node wants to start a connection with another node, it performs a route discovery and then sends necessary packets. When the node no longer needs to use the network, it returns to the "silent mode" After a while, neighboring nodes invalidate their own route entries to this node and selfish node becomes invisible on the network

C. Gray Hole Attack (Routing Misbehavior)

Gray hole attack is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message.

Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds in its purpose.

D.Black Hole Attack

The difference of Black Hole Attack compared to Gray Hole Attack is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checkingits routing table, immediately sends a false RREP message giving a route to destination through itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets through the malicious node. Malicious node attacks all RREQ messages from other source nodes also and takes over all routes. Therefore all packets are sent to a point when they are not forwarded anywhere[14].

E.Impersonation

Due to lack of authentication in ad-hoc networks, only MAC or IP addresses uniquely identify hosts. These addresses are not adequate to authenticate the sender node. Therefore non-repudiation is not provided for ad-hoc network protocols. MAC and IP spoofing are the simplest methods to pretend as another node or hide in the network. Malicious nodes achieve impersonation only by changing the source IP address in the control message. Another reason for impersonation is to persuade nodes to change their routing tables pretending to be a friendly node, such as attacks against routing table.

F.Attacks against the Routing Tables

Every node has its own routing table to find other nodes easily in the network. At the same time, this routing table draws the network topology for each node for a period (max. 3 seconds, duration of ACTIVE_ROUTE_TIMEOUT is constant in AODV protocol). If a malicious node attacks against thistable, attacked nodes do not find any route to other nodes that it wants to connect. This attack is always performed by fabricating a new control message. Therefore it is also named fabricating attack. There are many attacks against routing tables. Each one is done by fabricating false control messages[14].

G. Sleep Deprivation Torture Attack (Battery Exhaustion)

Many techniques are used to maximize the battery life and mobile nodes prefer to stay at the sleep mode, when they are not used. Sleep Deprivation Torture is one of the serious types of Denial of Service Attacks, which affects only nodes, especially handheld devices that have limited resources. In a period time, attacker can propagate some control messages through the network, in which other nodes are also affected. Other nodes pass to the operation mode from the sleep mode and start processing these unnecessary packets until their batteries completely run out [6].

H.Worm hole attack

The *wormhole attack* [6] is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node *X* located within transmission range of legitimate nodes *A* and *B*, *A*and*B*are not themselves within transmission range of each other. Intruder node *X* merely tunnels control traffic between *A* and *B* (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that *X* is virtually invisible

III. IMPLEMENTING ATTACKSCENARIOS ON AODV ROUTING PROTOCOLS

For the simulations, we use ns-2 (v-2.32) network simulator. ns-2 provides faithful implementations of the different network protocols. At the physical and data link layer, we used the IEEE 802.11 algorithm. The channel used is Wireless Channel. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 2 Mbps and then 3 Mbps. The connection pattern is generated using *cbrgen*and the mobility model is generated using *setdest utility. Setdest*generates random positions of the nodes in the network with specified mobility and pause time. The terrain area is 800m X 800m with 50 numbers of nodes with chosen maximum speed up to10 m/s. The simulation parameters are summarized in table 2. Each data point represents an average of 100 runs. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols. The various simulation scenarios are as follows:

Table 2: Simulation Scenario 1

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes& mobility	50, Mobile
Routing protocol	AODV
Traffic model	CBR
Data Rate	2 Mbps& 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes & type	0

Table 3: Simulation Scenario 2

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes & mobility	50 , fixed
Routing protocol	AODV
Traffic model	CBR
Data Rate	2 Mbps & 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes & type	0

Table 4: Simulation Scenario 3

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes & mobility	50 , fixed
Routing protocol	AODV
Traffic model	CBR
Data Rate	2 Mbps & 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type& mobility	5, 10 & 14 mobile Black hole

Table 5: Simulation Scenario 4

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes & mobility	50 , fixed
Routing protocol	AODV
Traffic model	CBR

Data Rate	2 Mbps & 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type & mobility	1 worm hole link, mobile

Table 6: Simulation Scenario 5

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes & mobility	50 , moving
Routing protocol	AODV
Traffic model	CBR
Data Rate	2 Mbps & 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type & mobility	5, 10 & 14 fixed Black hole

Table 7: Simulation Scenario 6

Parameter	***Value***
Simulator	NS 2.32
Simulation time	80 Sec
Number of nodes & mobility	50 , moving
Routing protocol	AODV
Traffic model	CBR
Data Rate	2 Mbps & 3 Mbps
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type & mobility	1 worm hole link, fixed

IV. RESULTS AND DISCUSSIONS

The average per sessionthroughput values for different simulation times, and for different simulation scenarios such as all the nodes are moving except the malicious ones at the data rate of 2 Mbps and 3 mbps,all the nodes are fixed except the malicious ones at the data rate of 2 Mbps and 3 mbps, are obtained for 100 simulation runs.Similarly, we also have simulated for all node moving ie. both malicious and non-malicious nodes moving as well as all nodes fixed. We have shown below plots of average per session throughput, average over 100 simulation runs, in Figs. 1for scenarios without malicious nodes and DR 2 Mbps. This is done in order to show that with the introduction of malicious nodes in the network, throughput falls as shown in Figs. 3 to 6. For finding out the average per session throughput, simulations were run 100 times for each scenario. The plots for DR 3 Mbps are similar and skipped for lack of space.

Table 8: Per-Session Throughput for Various Scenarios

Malicious Nodes & their mobility	***Non-Malicious Nodes & their mobility***	***Data Rate (DR) (Mbps)***	***Av. Per session throughput (Bps)***
0	50, mobile	2	4.15e+06
0	50, mobile	3	7.46 e+06
0	50, fixed	2	9.50 e+05
0	50, fixed	3	1.62 e+06
5, Bh,mobile	50, fixed	2	6.98 e+05
10, Bh,mobile	50, fixed	2	5.02 e+05
14, Bh,mobile	50, fixed	2	3.45 e+05
5, Bh,mobile	50, fixed	3	9.60 e+05

10, Bh,mobile	50, fixed	3	6.65 e+05
14, Bh,mobile	50, fixed	3	4.30 e+05
1Wh link, mobile	50, fixed	2	3.49 e+05
1Wh link, mobile	50, fixed	3	9.76 e+05
5, Bh,fixed	50, mobile	2	3.77 e+06
10, Bh,fixed	50, mobile	2	3.01 e+06
14, Bh,fixed	50, mobile	2	2.72 e+06
5, Bh,fixed	50, mobile	3	6.78 e+06
10, Bh,fixed	50, mobile	3	3.20 e+06
14, Bh,fixed	50, mobile	3	3.01 e+06
1Wh link, fixed	50, mobile	2	4.13 e+06
1Wh link, fixed	50, mobile	3	5.04 e+06

From Table 8, it is seen that average per session throughput is higher when non-malicious nodes are moving and malicious nodes are fixed, for both blackhole and wormhole attacks. The corresponding histogram for average per-session throughput plot over 100 simulation run is shown in Figs. 11 to 26.We plot the histogram to identify the different attack patterns and hence a signature for each pattern. The attack patterns that we observe are different for each of black hole attack and worm hole attack. And the plots vary over the number of malicious nodes but patterns remain alike. The histograms shown in the figures are self-explanatory and clearly showing the signature of each attack type. Histogram plots for both data rate 2 Mbps and 3 Mbps are shown for all scenarios. After doing careful study of the graphs above, we find that for a given fixed number of non-malicious nodes and malicious nodes, the per session throughput, for a scenario of non-malicious nodes being mobile and malicious nodes being fixed, are always greater than that for a scenario of non-malicious nodes being fixed and malicious nodes being mobile. This means the effect of malicious nodes, such as black hole and worm hole, are severe in case of static node scenario then mobile node scenarios. The above statements are justified by the table 8.

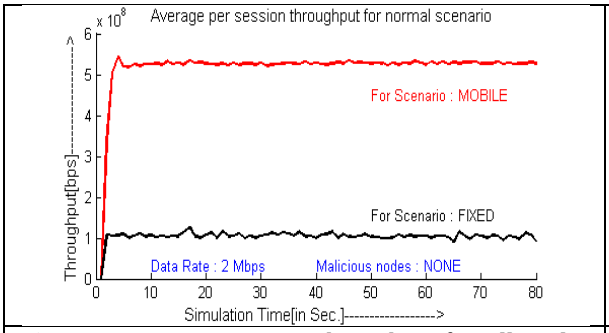


Fig1: Average Per Session Throughput for All Nodes Moving and fixedData rate (DR) 2 Mbps, Average over 100 simulation runs

Fig. 2: Average per session throughput with all fixed nodes at different data rates

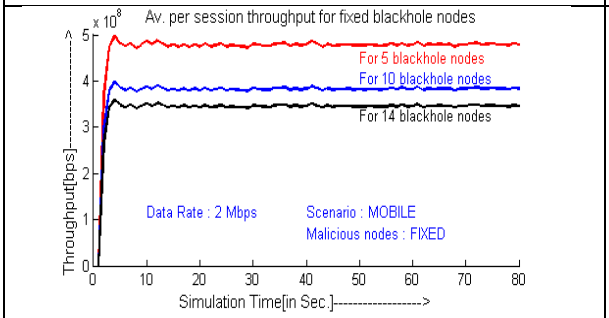


Fig. 3: Average per session throughput with fixed, 10& 14 mobileBlackhole nodes in mobile cenario.DR 2 Mbps, Average over 100 simulation runs

Fig. 4: Average per session throughput withmobile 5,10& 14Blackhole nodes in fixed scenario.DR 2 Mbps, Average over 100 simulation run

After doing careful study of the graphs above, we find that for a given fixed number of non-malicious nodes and malicious nodes, the per session throughput, for a scenario of non-malicious nodes being mobile and malicious nodes being fixed, are always greater than that for a scenario of non-malicious nodes being fixed and malicious nodes being mobile. This means the effect of malicious nodes, such as black hole and worm hole, are severe in case of static node scenario then mobile node scenarios. The above statements are justified by the table 8.

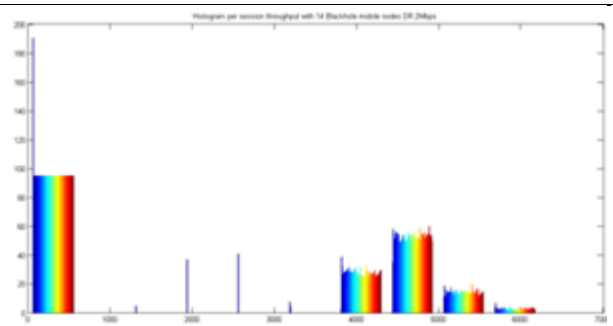


Fig. 5: Histogram for per session throughput with 5 mobile BH nodes DR 2 Mbps

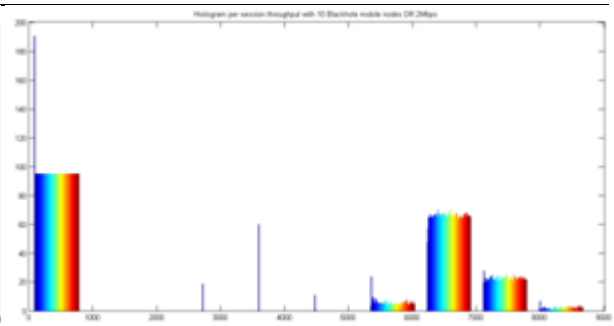


Fig. 6: Histogram for per session throughput with 10 mobile BH nodes DR 2 Mbps

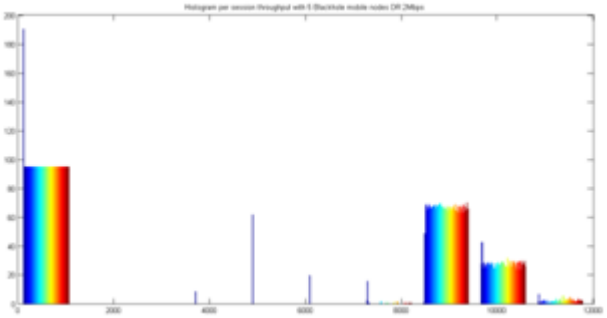
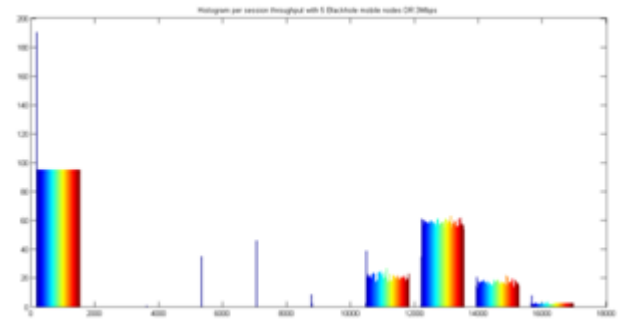


Fig. 7: Histogram for per session throughput with 14 mobile BH nodes DR **2** Mbps



Fig, 8: Histogram for per session throughput with 5 mobile BH nodes DR 3 Mbps

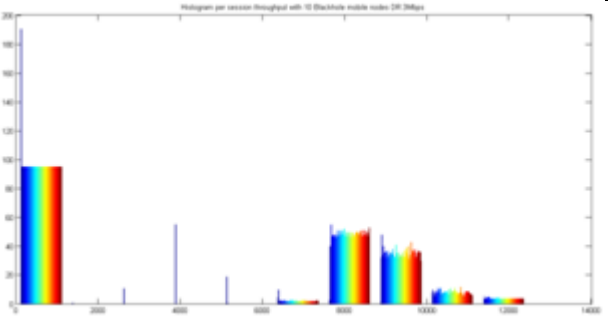


Fig. 9: Histogram for per session throughput with 10 mobile BH nodes DR 3 Mbps

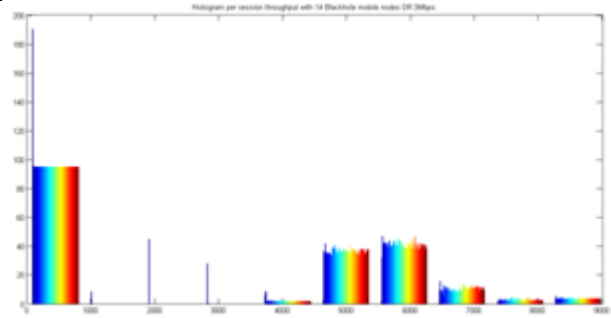


Fig. 10: Histogram for per session throughput with 14 mobile BH nodes DR 3 Mbps

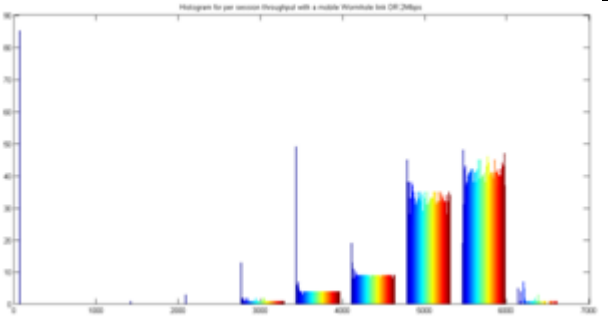


Fig. 11: Histogram for per session throughput with a mobile WH link DR 2 Mbps

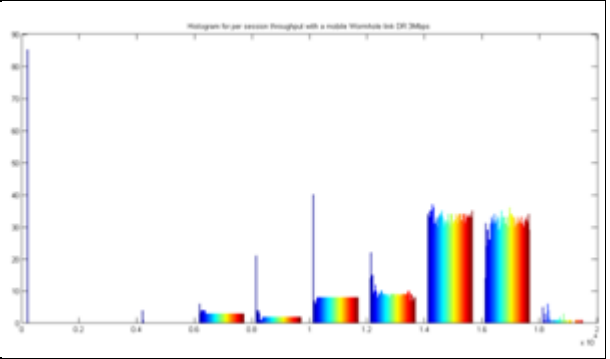


Fig. 14: Histogram for per session throughput with a mobile WH link DR 3Mbps

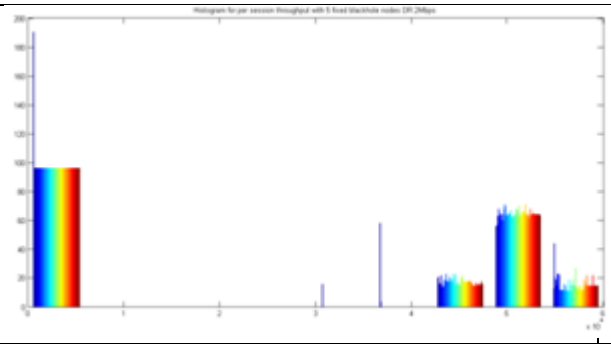


Fig. 15: Histogram for per session throughput with 5 fixed BH nodes DR 2 Mbps

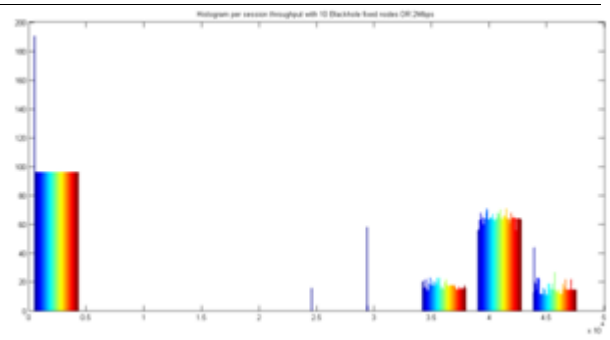


Fig. 16: Histogram for per session throughput with 10 fixed BH nodes DR 2 Mbps

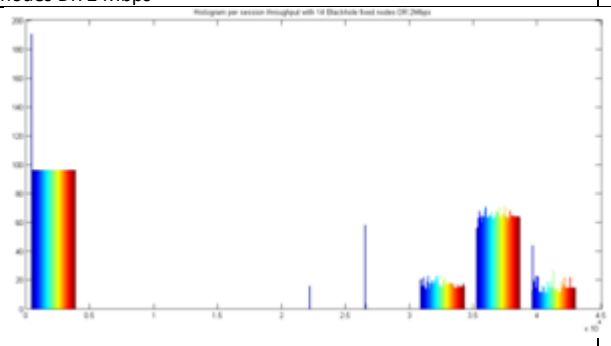


Fig. 17: Histogram for per session throughput with 14 fixed BH nodes DR 2 Mbps

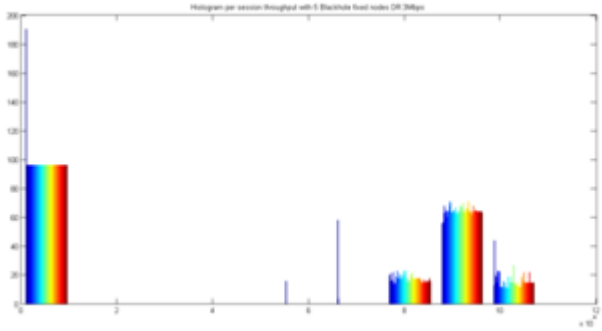


Fig. 18: Histogram for per session throughput with 5 fixed BH nodes DR 3 Mbps

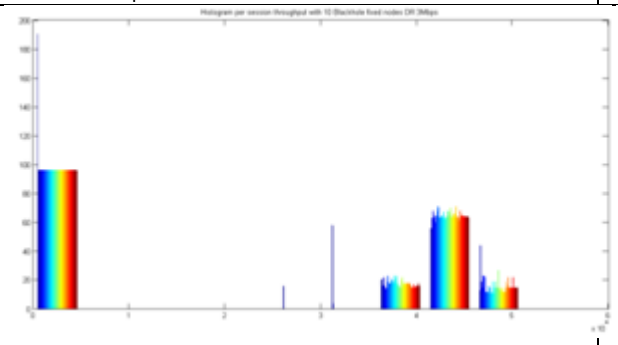


Fig. 19: Histogram for per session throughput with 10 fixed BH nodes DR 3 Mbps

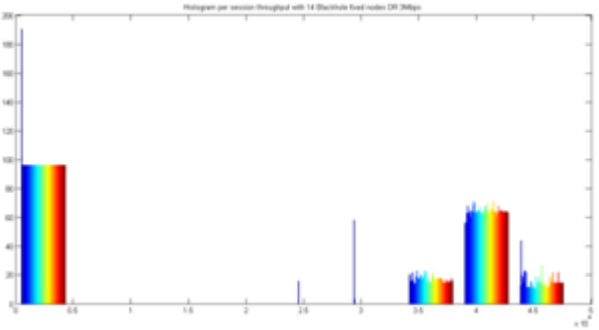


Fig. 20: Histogram for per session throughput with 14 fixed BH nodes DR 3 Mbps

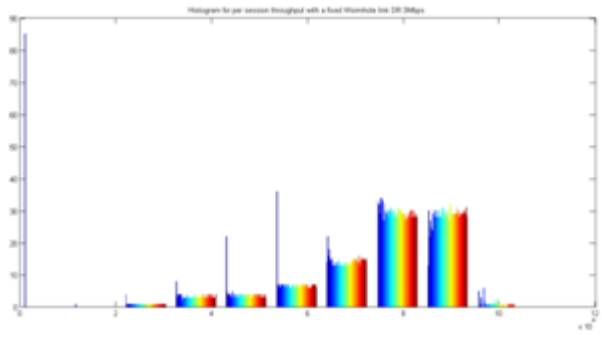


Fig. 21: Histogram for per session throughput with a fixed WH link DR 2 Mbps

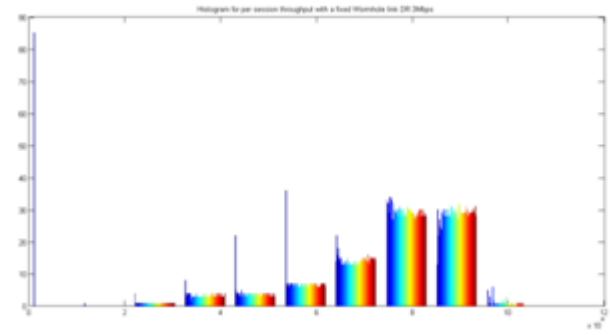


Fig. 22: Histogram for per session throughput with a fixed WH link DR 3 Mbps

In this paper, we have analyzed the security threats such as black hole attack and worm hole attack on an ad-hoc network. Here we have simulated and analyzed the black hole and worm hole attack under various scenarios such as all the non- malicious nodes are moving and malicious nodes are fixed, all the non-malicious nodes are fixed and malicious nodes are moving, and source and destination communicating at data rates of 2 Mbps and 3 Mbps.

We find that for a given fixed number of non-malicious nodes and malicious nodes, the per session throughput, for a scenario of non-malicious nodes being mobile and malicious nodes being fixed , are always

greater than that for a scenario of non-malicious nodes being fixed and malicious nodes being mobile. This means *the effect of malicious nodes, such as black hole and worm hole, are severe in case of static node scenario to mobile node scenarios*. Besides this, we have also found that irrespective of the nodes moving or not, the black hole and wormhole attack have *definite attack patterns* which are visualized by the histogram plotsof the results of scenarios and may considered as signature of the respective attack pattern.

REFERENCES

[1]. C.C. Chiang, H.-K. Wu, W. Liu and M. Gerla, "Routing in clustered multihop, mobilewireless networks with fading channel", in: The IEEE Singapore International Conference on Networks (1997) pp. 197-211

[2]. B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, Jamalipour , "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[3]. Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," in Proc. Workshop on Real-World Wireless Sensor Networks, REALWSN'5, Stockholm, June 2005.pp.1

[4]. I. Stamouli, P. G. Argyroudis, and H. Tewari, "Real-time Intrusion Detection for Ad hoc Networks". Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), 2005. pp. 1-2

[5]. J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu,"Adaptive security for multi-layer ad-hoc networks," in Special Issue of Wireless Communications and Mobile Computing.WileyInterscience Press, Aug. 2002

[6]. S. Sharma and R. Gupta, "Simulation study of blackhole attack in the mobile ad-hoc networks," Journal of Engineering Science and Technology, Vol. 4, No. 2 (2009) pp. 243-250.

[7]. L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. IEEE Network Magazine, 13(6):24–30, 1999. [8] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks".Proceedings IEEE Volume, Issue, 22-25 March 2007 .

[8]. F. J. Ros and P. M. Ruiz, "Implementing a New ManetUnicast Routing Protocol in NS2", December, 2004, 25 July 2005.

[9]. The ns Manual (formerly ns Notes and Documentation).

[10]. S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps.,Vancouver, Canada, Aug. 18–21, 2002.," pp. 1-5

[11]. Mike, Evangelos, Tao Wan,"Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks", in proceeding of ADHOC-NOW,2003 pp.2-4

[12]. Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil,"Black Hole Attack Injection in Ad hoc Networks",5th Latin-American Symposium on Dependable Computing, LADC 2011, São José dos Campos, Brazil, 01/2011 pp.1-2

[13]. Jiejun Kong, Xiaoyan Hong, Mario Gerla, "A New Set Of Passive Routing Attacks In Mobile Ad Hoc Networks", IEEE Military Communications Conference (MILCOM'03), October 13-16, 2003. Boston,pp.1-5