ISSN: 2321-7782 (Online)

Volume 3, Issue 3, March 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Effect of Pause Time on Per-Session Throughput if Black Hole Attack is In-avertible

Sudipta Majumder[1]
Dept. of CSE,DUIET,
Dibrugarh University,
Assam, India.

Bhargab Jyoti Saikia[2]
Dept. of ECE,DUIET,
Dibrugarh University,
Assam, 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 mobile nodes. In this paper, we have found out how the pause rate of mobile ad-hoc network effects black hole attack in the network. Black hole attack is one of the DoS attack. Scenarios of 50 mobile non malicious nodes were taken where each odd numbered nodes transmit packets to the next even numbered node. The taken black hole attack nodes for the purpose of attack are 5, 10 and 14 for different scenarios and the pause rate are 0,3,5 and 7 seconds .

Key Terms - Ad-hoc network, Black hole, Per-Session Throughput, Pause time, Data rate, DoS.

I. INTRODUCTION

In Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that’s why it is sometimes referred to as an “infrastructure less” network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An adhoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Adhoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the 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 new environment.

Security solutions are important issues for MANET, especially for those selecting sensitive applications, 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. Because of these vulnerabilities, MANET are more prone to malicious attacks. The primary focus of this work is to provide a survey on attacks particularly on blackhole attack and worm hole attack that affect the MANET behavior due to any reason.

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.

TABLE I:

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:

2.1. 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.

2.2. 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

2.3. 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.

2.4. 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[13].

2.5. 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.

2.6. Modification Attack

Control massages are used to establish the shortest and true path between two nodes. But malicious nodes want to route packets to the direction that they want, modifying content of the control messages (e.g. RREQ, RREP and RERR). Modification means that the message does not carry out its normal functions. Route information such as hop count, sequence number, life time etc. are carried along with control messages. This information has a big role in establishing a true route. Modifying these fields in the control messages, a malicious node can perform its own attacks. Impersonation is not one of these kinds of attacks; impersonation is only performed by modifying source address to pretend as another node in the network. But changing route information in control messages is performed to mislead the victim or intermediate node and this modification is generally against the replay messages.

2.7. 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 this table, 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.

2.8. 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].

2.9. 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 Attack Scenarios 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. 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 number of nodes with chosen maximum speed up to 5 m/s. The simulation parameters are summarized in table II to V. 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 II:

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
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes	0
Pause time	0 Sec.

TABLE III:

Simulation scenario 2 to 5

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
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes & type	5
Pause time	0 Sec,3 Sec,5 Sec & 7 Sec

TABLE IV:

Simulation scenario 6 to 9

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
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type & mobility	10, Mobile
Pause time	0 Sec,3 Sec,5 Sec & 7 Sec

TABLE V:

Simulation scenario 10 to 13

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
Mobility	10 m/s
Terrain area	800m x 800m
Transmission range	50 m
No. of malicious nodes, type & mobility	15,Mobile
Pause time	0 Sec,3 Sec,5 Sec & 7 Sec

Here an important thing to mention is that the simulation scenarios given in the table III to V have been simulated with various pause times. The pause times considered are 0 sec. 3 sec and 7 sec.

IV. Results And Analysis

With the average per session throughput values for different simulation times, for different simulation scenarios as noted in Table VI, has been plotted. In the simulation scenario all the nodes along with the attack nodes are moving. Here we have plotted the effect black hole attack with 5, 10 and15 black hole nodes. It is very clearly visible is that as the number of black hole attack nodes increase the per session throughput also decreases. The plots vary for the numbers of malicious nodes and mobility of the nodes but patterns remain alike.

TABLE VI:

Per-session throughput for various scenarios

Malicious Nodes (All Mobile)	Non-Malicious Nodes & their Mobility	Pause Time In Sec	Per session throughput (Bps)
0	50,Mobile	0	9.38E+06
5 Black Hole	50,Mobile	0	8.44E+06
5 Black Hole	50,Mobile	3	8.26E+06
5 Black Hole	50,Mobile	5	8.16E+06
5 Black Hole	50,Mobile	7	7.98E+06
10 Black Hole	50,Mobile	0	6.61E+06
10 Black Hole	50,Mobile	3	6.43E+06
10 Black Hole	50,Mobile	5	6.34E+06
10 Black Hole	50,Mobile	7	6.17E+06
15 Black Hole	50,Mobile	0	8.82E+05
15 Black Hole	50,Mobile	3	8.11E+05
15 Black Hole	50,Mobile	5	7.85E+05
15 Black Hole	50,Mobile	7	7.58E+05

The following figure 1 shows the per-session throughput without any black hole attack. Here the total numbers of nodes are 50 and all of them are mobile. The simulation runs for 80 seconds. The pause time used here is 0 seconds. The simulation was run for 100 times and the average is taken. Similarly same has been done for all other simulation.

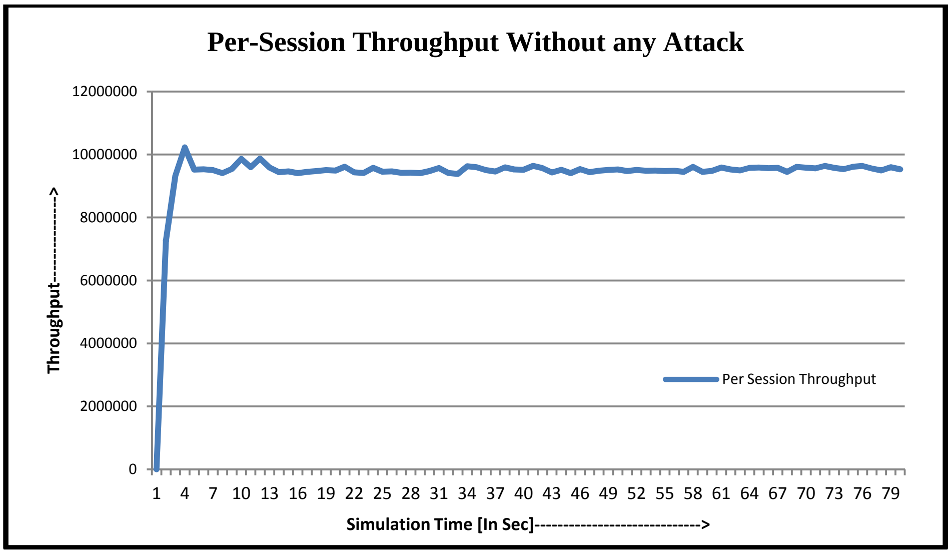

Figure 1: Per-session throughput without any attack

The figure 2 below shows per session throughput under 5 black hole node attack. the total number of non-malicious nodes in the simulation is 50 and that of malicious ones are 5. The simulation for the scenario has been run for for various pause time such as0 sec., 3 sec., 5 sec. and 7 sec. here all the node including malicious and non-malicious are mobile. From the figure, we can clearly see that the throughput decreases as pause time increases. The difference in the average per session throughput for all the pause time is clearly evident in the figure 2.

From the figure 1 and figure 2 it is clearly visible that the per session throughput for 5 black hole node attack with 0 sec pause time has fallen nearly 10% from that with no attack. Similarly, with the introduction of pause time the per session throughput scenario having black hole attack have fallen further. The following table shows the rate of fall of per session through put for scenarios with black hole attack having pause time with respect to scenario having black hole attack with 0 pause time.

TABLE VII:

Percentage fall in Per-session throughput for 5 black hole nodes attacks

Pause time	Percentage fall in Per-session throughput
0 Sec	2.22%
5 Sec	3.32%
7 Sec	5.56%

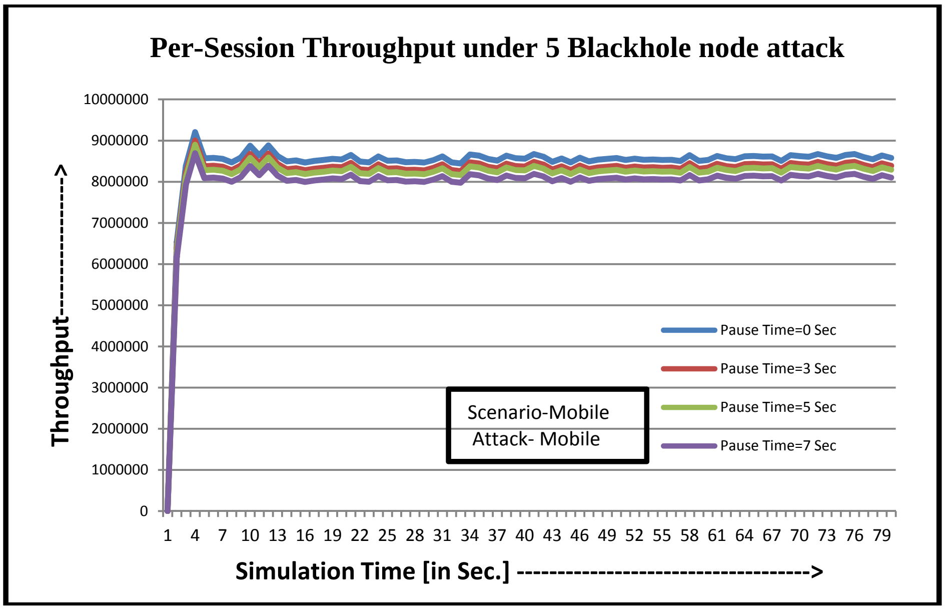

Figure 2: Per-session throughput with Black hole (5 nodes) attack

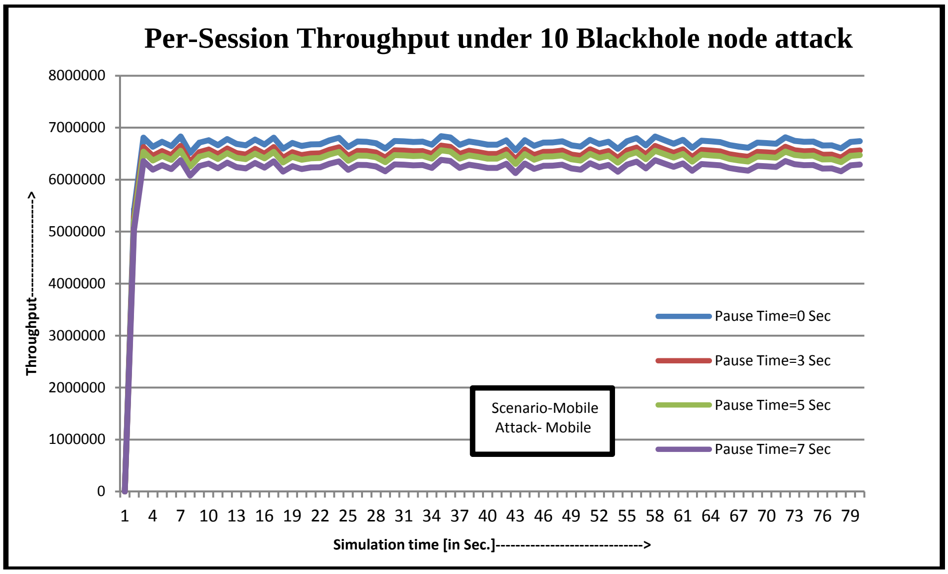

Figure 3: Per-session throughput with Black hole (10 nodes) attack

Similarly, the figure 3 and 4 shows the impact of 5 and 6 black hole nodes attack on the scenario having varying pause time. In both the simulation scenarios, the per-session throughput decreases with the addition of the black hole attacks. Here, the impact of impact of black hole attack is severe because the numbers of black hole nodes have increased to 10 and 15 respectively. Besides, the impact of introduction of the pause time is easily visible in the plots. that is, as the pause time increases the effect of black hole attack also increases. The following table VI shows the percentage fall of per-session throughput for scenarios with pause time under black hole attack with respect to scenario with no pause time under black hole attack.

TABLE VIII:
Percentage fall in Per-session throughput for 10 & 15 black hole nodes attacks

Number of black hole nodes	Pause time In Sec.	Percentage fall in Per-session throughput
10	3	2.67%
10	5	4.00%
10	7	6.67%
15	3	8.00%
15	5	11.00%
15	7	14.00%

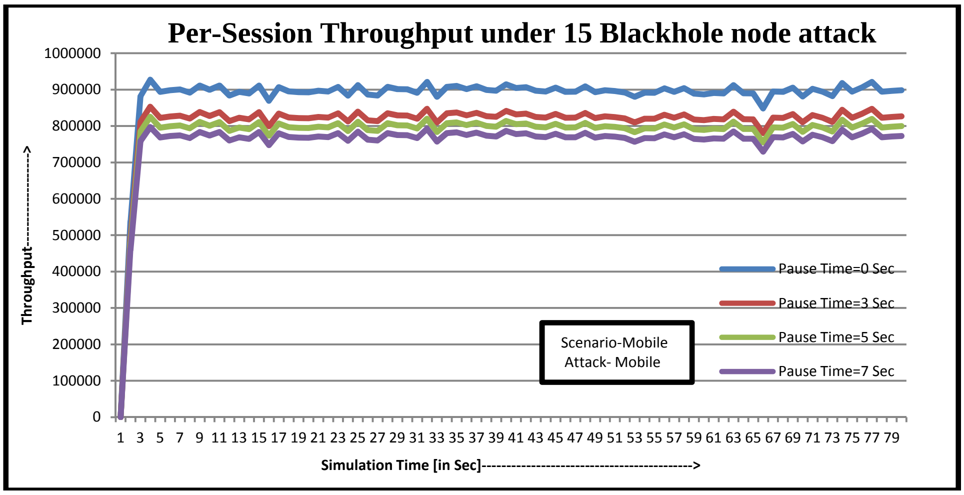

Figure 4: Per-session throughput with Black hole (15 nodes) attack

From the table VIII and figures above it is clearly evident that per-session throughput for scenarios decreases with the introduction of more number of black hole nodes and the severity of the black hole attack increase as the pause time of the mobile nodes increases.

V. Conclusion

In this paper, we have studied the severity of black hole attack and its response to the pause rates of non-malicious mobile nodes. Here in the simulation scenario, we have all the nodes mobile irrespective of its behavior. But the non-malicious nodes are introduced with certain pause rates. This results increased black hole behavior by the malicious nodes. Further, as the black holes were increased in the particular simulation scenario, the percentage drop in per-session throughput increased. In other words, we can say that *as the numbers of black hole nodes increases in a simulation scenario, the severity of its behavior also increases with increase of pause time of the non-malicious nodes*.

References

1. C.C. Chiang, H.-K. Wu, W. Liu and M. Gerla, Routing in clustered multihop, mobile wireless 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.
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. 2-5
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 andTechnology, 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 Southeast Con Journal, “Performance analysis of ad-hoc networks under black hole attacks”.Proceedings IEEE Volume, Issue, 22-25 March 2007

9. F. J. Ros and P. M. Ruiz, “Implementing a New ManetUnicast Routing Protocol in NS2”, December, 2004, 25July 2005.

10. The ns Manual (formerly ns Notes and Documentation).

11. C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel” Journal cluster computing, volume 1 issue1,1998,USA) pp. 1-3

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

13. S.Majumder, A.Hussain,”how to increase per-session throughput in distress hours if black hole attack is in-avertible”, ISSN(online):2319-2801, Asian Academic Research Associates , Vol1,Issue 12, August 2013,IF-2.015 by ISRA-JIF .

AUTHOR(S) PROFILE

Mr. Sudipta Majumder has received his M.Tech Degree in Information technology and B.Tech in Computer Science And Engineering from North Eastern Regional Institute Of Science And Technology(NERIST), Itanagar, AP, India. He is currently working in the Department of Computer Science and Engineering in Dibrugarh University institute of engineering technology (DUIET), Dibrugarh University, Assam.

Mr. Bhargabjyoti Saikia has received his M.Tech Degree in Information technology from North Eastern Regional Institute of Science and Technology(NERIST), Itanagar, AP, India. And his B.Tech from Biju Patnaik University. He is currently working in the department of Electronics and communication in Dibrugarh University Institute of Engineering Technology (DUIET), Dibrugarh University, Assam.