International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Analysis of Mobile Ad-Hoc Networks Under the Attacks

Abhishek Kumar[1], Shweta Kumari[2]

[1, 2]School of Computing Science and Engineering, Galgotias University, Greater Noida, U.P, India

Abstract: ***Mobile Ad-hoc Networks (MANETs) allow mobile hosts to initiate communications with each other over a network without an established infrastructure or a central network authority. Because of this, MANETs have dynamic topologies because nodes can easily join or leave the network at any time. From a security design perspective, MANETs are vulnerable to various types of malicious attacks. As are result, Ad-hoc On-demand Distance Vector (AODV), which is one of the standard MANET protocols, can be attacked by malicious nodes. A black hole attack is one type of malicious attack that can be easily employed against data routing in MANETs. A black hole node replies to route requests rapidly with the shortest path and the highest destination sequence number. The black hole node does not have an active route to a specified destination associated with it and it drops all of the data packets that it receives. In this paper we have discussed some basic MANET routing protocols like Ad-hoc On Demand distance Vector (AODV),Dynamic Source routing (DSR), Optimized Link state Routing (OLSR). Main objective of this paper is to address some basic security concerns in MANET, operations of malicious node and its effect on these routing protocols.***

Keywords: MANET, Routing protocols, malicious node.

1. Introduction

An ad hoc wireless network consists of a collection of independent nodes, all able of transmitting and receiving packets. Such a network can operate in a standalone fashion (with the ability of self-configuration) or can connect to the internet [1]. MANET is more susceptible 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 is more prone to malicious attacks. Minimal configuration time and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency situations, and so forth [2]. In addition, the migration of wireless networks from hot spots to multi-hop ad hoc networks is an important step toward self-organized global routing. The rest of this paper is organized as following; section 2 gives background of MANET routing protocols i.e. reactive, proactive and hybrid, types of attacks are presented in section 3, the analysis along with the simulation results are given in section 4 and finally the conclusion is presented in section 5.

2. Types of Ad Hoc Routing Protocols

Routing is a major area of research in ad hoc networks, as the characteristics of ad hoc networks pose many new challenges by comparison with traditional wired area networks. Existing protocols are likely to be too resource intensive to be suitable for ad hoc use, so many solutions using a variety of methods are being proposed and studied. The Internet Engineering Task Force (IETF) has set up a working group called MANET, with the objective of selecting the most suitable protocols. There are three types of ad hoc network routing protocols, reactive proactive and hybrid protocols. In this paper we study the performance of AODV and DSR as reactive protocols, OLSR as proactive protocol, under malicious node.

2.1 Ad hoc On-Demand Distance Vector (AODV) AODV

[3] is an example of reactive MANET routing protocol, in AODV the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node which then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

2.2 Dynamic Source Routing (DSR)

DSR [4] is another example of reactive MANET routing protocol. The fundamental approach of this protocol during the route creation phase is to launch a route by flooding Route Request packets in the network. The destination node, on getting a Route Request packet, responds by transferring a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received. A destination node, after receiving the first Request packet, replies to the source node through the reverse path the Route Request packet had traversed. Nodes can also be trained about the neighboring routes traversed by data packets if operated in the promiscuous mode. This route cache is also used during the route construction phase.

2.3 Optimized Link State Routing (OLSR)

OLSR [5] is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks. All the nodes in the network do not broadcast the route packets.

Multipoint Relay (MPR) nodes broadcast route packets. These MPR nodes can be selected in the neighbor of source node. Each node in the network keeps a list of MPR nodes. This MPR selector is obtained from HELLO packets sending between in neighbor nodes.

3. Attacks MANET

The security attacks in MANET can be classified into two major categories as usual, namely passive attacks and active attacks [8].

3.1 Passive Attacks

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. The attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect.

3.2. Active Attacks

In an active attack, the attacker tries to break secured systems. This can be done through viruses, worms, or Trojan horses. Active attacks include break protection features, to introduce malicious code, and to steal or modify information. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

4. Simulation Model

We are going to compare the performance of AODV, DSR, and OLSR in terms of delay and throughput in case of black hole attack, but we first give a brief about the model and simulation parameters. This section describes the system model used, the measured parameters, and the results.

4.1. Modeling of a MANET in OPNET

We performed our evaluations using OPNET. We used an IEEE 802.11 MAC layer [10]. The simulation parameters are shown in table I. In this paper two cases were studied with different percentage of malicious nodes. The first case studied the changing in number of nodes without mobility; on the other hand the second case studied the effect of malicious node on MANET routing protocols with mobility with fixed number of nodes.

4.2 Table Simulation Parameters

Parameter	Value
MANET Area	1 Km2
Total number of nodes	20 : 120
percentage of malicious nodes	0% : 30%
Movement Pattern	Random Waypoint
Node Speed	0 : 10 m/s
Application	FTP
Size of Packet	1Mbytes
Inter-request time	Exponential 360 sec
Simulation time	240 seconds
Transmission range	250 m
Data rate	11 Mbps
Transmission power	0.005 W

5. Performance Metrics

There are different types of parameters for the performance evaluation of MANET routing protocols, which have different behaviors of the overall network performance. We will evaluate two metrics for the comparison of our study on the overall network performance. These metrics are delay and throughput. These parameters are mainly used in most of the previous works [11], [12], [13], [14], [15], [16].

According to [10], the two measured metrics are defined as following:

Delay represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay includes medium access delay at the source MAC, reception of all the fragments individually.

Throughput is the bit rate sent to the higher layer. It represents the rate of data successfully received from other stations. Throughput is expressed as bits per sec.

6. Simulation Results

First we compare the performance in terms of delay and throughput of AODV, DSR, OLSR versus number of nodes as shown in figures 1 to 6 then versus speed as shown in figures 9 to 12 with different percentage of malicious nodes.

From figures 1 to 3 it is clear that the delays increase with increasing the number of nodes as the packet dropped in such case increaseNoting that in case of DSR, for nodes more than 60 nodes the curves is not valid due to limitation in simulation.

Figures 4 to 6 show the throughput versus different number of nodes with different percentage of malicious nodes using different ad hoc routing protocols; it also shows that the throughput increases with increasing the number of nodes and decreases with increasing the percentage of malicious nodes in case of AODV, OLSR and DSR, Noting that in case of DSR, for nodes more than 60 nodes the curves is not valid due to limitation in simulation.

DSR uses more bandwidth because of source routing that increases the size of the header in data packets. its route maintenance is accomplished through route caches, the entries in route caches are updated as nodes learn new routes, multiple routes can be stored, Route requests tend to flood the network and generally reach all the nodes of the network, also there is a risk of many collisions between route requests by neighboring nodes as there is a need for random delays before forwarding RREQ, and a similar problem for the RREP (Route Reply storm problem), in case

links are not bidirectional, also DSR replies to all requests reaching destination from a single request cycle.

In case of AODV it uses sequence numbers which avoid using stale information about routes, avoid loops (no source routing), avoid the counting to infinity problem, also in AODV destination replies only once to request arriving first and ignore the rest, and when faced with two choices, the fresher route is always chosen (destination sequence number), and If any routing table entry not used recently, this entry will be expired.

In case of OLSR, MPR reduces flooding of broadcasts by reducing the same broadcast in some regions in the network, OLSR is a proactive protocol then the routing table must have routes for all available hosts in the network. And these are also explain why OLSR and AODV have the best overall performance and the highest throughput while increasing the number of nodes while DSR had lowest throughput as shown in figures 5 to 8 .

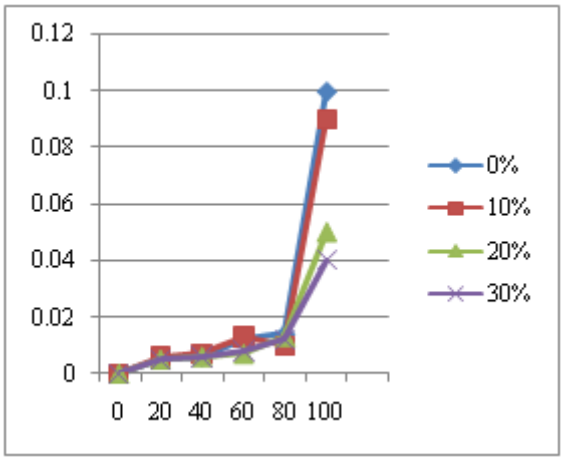

Figure 1: For AODV, delay vs no. of nodes

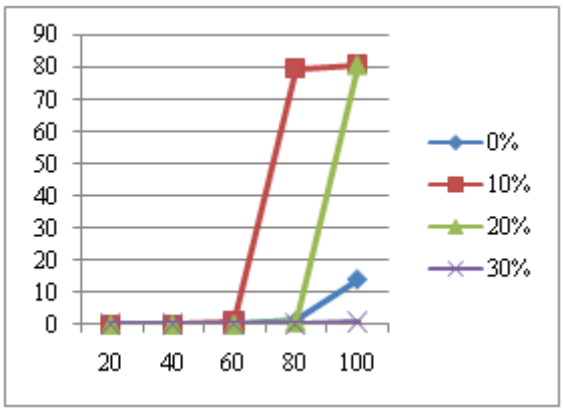

Figure 2: For DSR no of nodes vs dealy

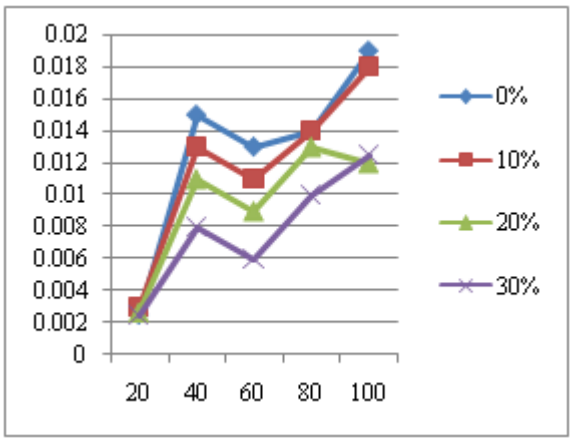

Figure 3: For OLSR, no of nodes vs delay

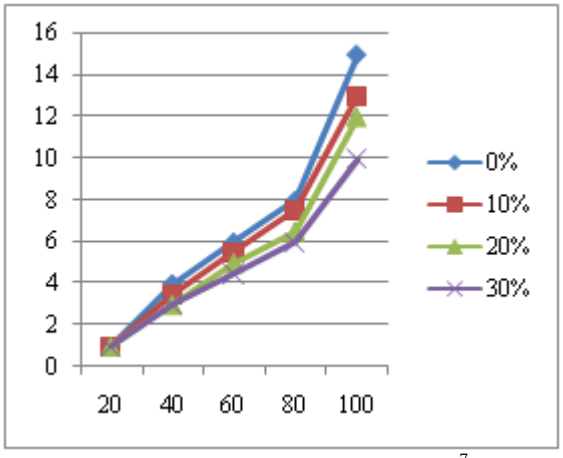

Figure 4: Number of nodes vs throughput(10^7) in AODV

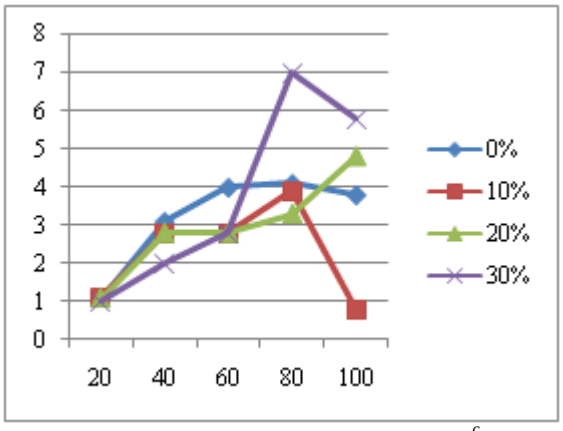

Figure 5: Number of nodes vs throughput(10^6) in DSR

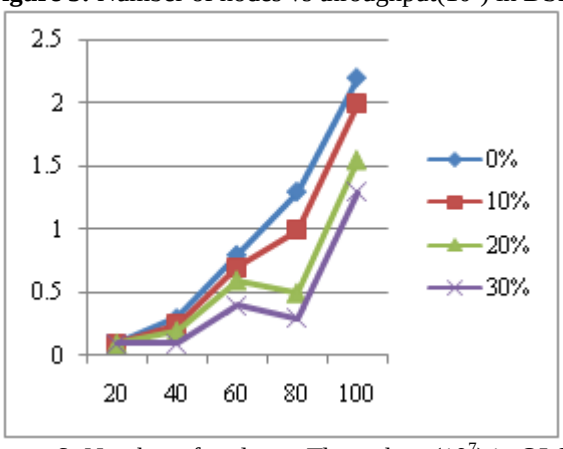

Figure 6: Number of nodes vs Throughput(10^7) in OLSR

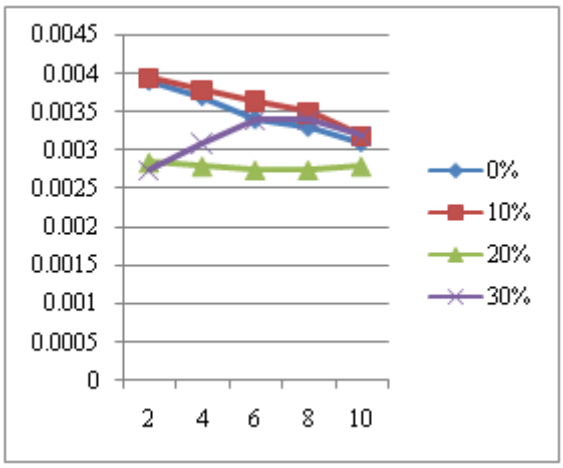

Figure 7: Speed (m/s) vs delay in AODV

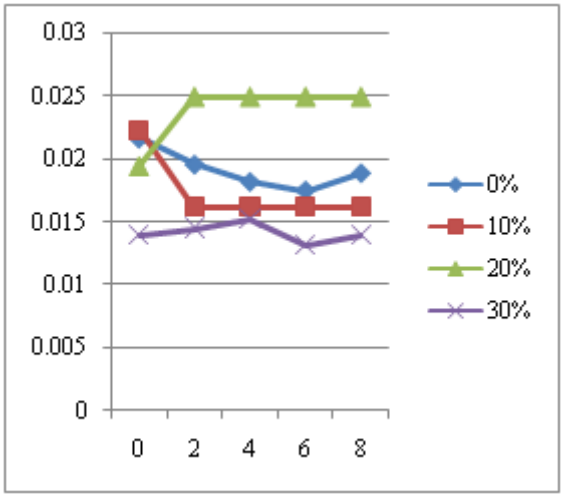

Figure 8: Speed (m/s) vs Delay in DSR

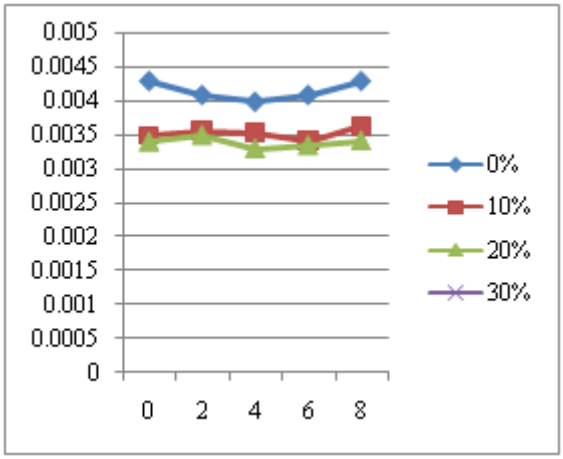

Figure 9: Speed (m/s) vs Delay in OLSR

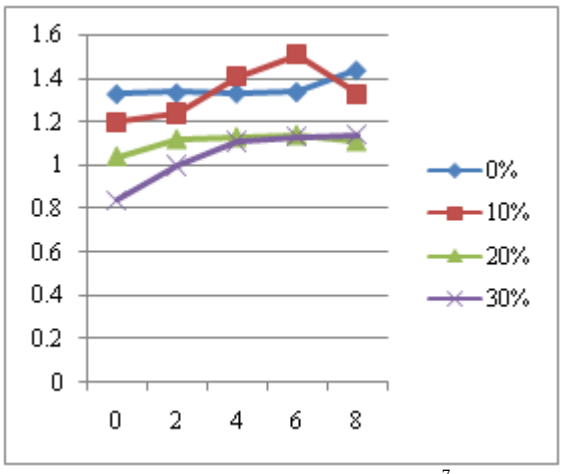

Figure 10: Speed (m/s) vs Throughput(10^7) in AODV

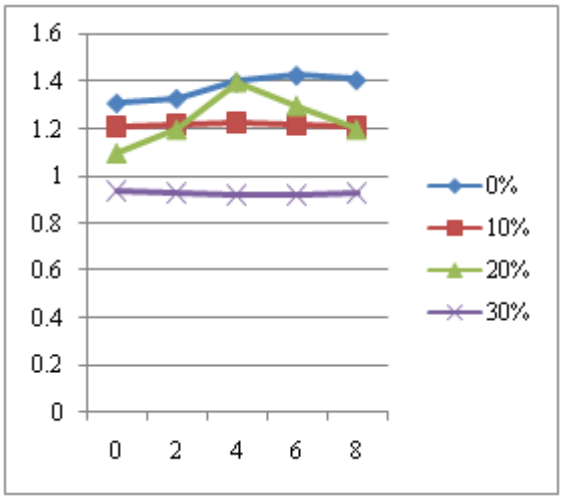

Figure 11: Speed (m/s) vs Throughput(10^7) in DSR

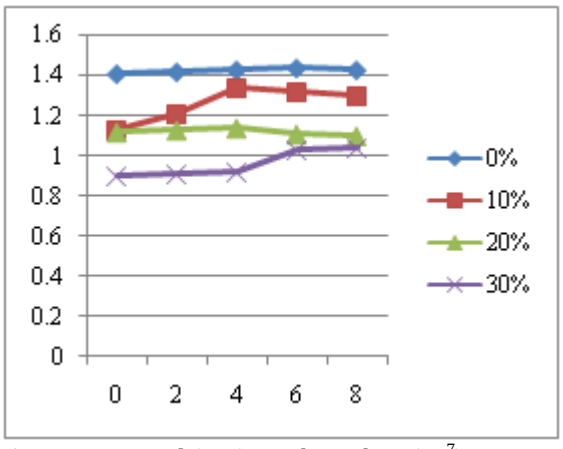

Figure 12: Speed (m/s) vs Throughput(10^7) in OLSR

7. Related Work

A Performance analysis of AODV, DSR and OLSR Routing Protocols in Static Scenarios is undertaken in [12], in [17] a performance analysis of AODV and OLSR in Mobile Ad hoc Networks using NS2 simulator is given. It concludes that the average end to end delay of packet delivery was higher in OLSR as compared to AODV. In [18] using NS2 simulator and it concludes that in stressful situation, the average delay of AODV protocol.

In [19] the simulation study of this thesis consisted of three routing protocols AODV, DSR and OLSR deployed over MANET using FTP traffic analyzing their behavior with respect to three parameters, delay, network load and throughput with different number of nodes. In [20] the research describes the performance of the three routing protocols (AODV,) in different network situations, specially varying the size of the networks.

8. Conclusion

In this paper, we compare the performance of MANET routing protocols like AODV, DSR, OLSR under attack. It has been concluded that OLSR and AODV are more immune to black hole attack than DSR Also, it has been detected that increasing the speed yield to minimize the effect of black hole attack. In general, it's important to realize that DSR should be avoided for large number of nodes, and AODV and OLSR are recommended. More over OLSR offered the highest throughput. As future work different routing protocols can be studied with different types of attacks such as DoS, Wormhole attack in the presence of real time application such as VOIP.

Reference

[1] Sajjad Ali , Asad Ali ,"Performance Analysis of AODV, DSR and OLSR in MANET", Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Master's Degree Thesis,Sweden 2009.

[2] Naga .V. Yedida, Rajesh Reddy Challa, "Performance Comparison of AODV, DSR and OLSR Routing Protocols in Static Scenarios", Center for Advanced Computer Sciences. E-mail: xy4835,rxc2763@louisiana.edu.

[3] S. Gowrishankar, T.G. Basavaraju, M. Singh, Subir Kumar Sarkar, "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks", Proceedings of the 24th South East Asia Regional Computer Conference, November 18-19, 2007, Bangkok, Thailand, Special Issue of the International Journal of the Computer, the Internet and Management, Vol.15 No. SP4, November, 2007.

[4] N Vetrivelan, Dr. A V Reddy ,"Performance Analysis of Three Routing Protocols for Varying MANET Size ",Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol. II IMECS 2008, 19-21 , Hong Kong, March 2008.

[5] Asar Ali, Zeeshan Akbar," Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications", Blekinge Institute of technology, Master's Degree Thesis, October2009.

[6] Singh Annapurna, Mishra Shailendra, "Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

[7] S. Gowrishankar, T.G. Basavaraju, M. Singh, Subir Kumar Sarkar, "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks", Proceedings of the 24th South East Asia Regional Computer Conference, Bangkok, Thailand, Nov., 18-19, 2007, pp. 8.1 – 8.6.

[8] Hsun Tseng , Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks on MANET " , international conference on black hole attack in MANET , Human-centric Computing and Information Sciences 2011, 1:4Springer 11/2011

[9] Teerawat Issariyakul and Ekram Hossain "Introduction to Network Simulator : NS2" ISBN: 978-0-387-71759-3, Publisher- Springer, 2009 .

[10] Patel, M.; Sharma, S., "Detection of malicious attack in MANET a behavioral approach," Advance computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.388,393, 22-23 Feb. 2013

[11] Singh, P.K.; Sharma, G., "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," Trust, Security and Privacy in Computing and Communications (Trust Com), 2012 IEEE 11th International Conference on , vol., no., pp.902,906, 25-27 June 2012

[12] Patel, M.; Sharma, S.; Sharan, D., "Detection and Prevention of Flooding Attack UsingSVM," Communication Systems and Network Technologies (CSNT), 2013 International Conference on, vol., no., pp.533, 537, 6-8 April 2013.

[13] Gambhir, S.; Sharma, S., "PPN: Prime product number based malicious node detection scheme for MANETs," Advance Computing Conference (IACC), 2013 IEEE 3rd International, vol., no., pp.335, 340, 22-23 Feb. 2013.

[14] Tan, S.; Keecheon Kim, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs," ICT Convergence (ICTC), 2013 International Conference on , vol., no., pp.1027,1032, 14-16 Oct. 2013.

[15] Junhai Luo; Mingyu Fan; Danxia Ye, "Black hole attack prevention based on authentication mechanism," Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on, vol., no., pp.173, 177, 19-21 Nov. 2008.

[16] Sanjeev Sharma, Rajshree, Ravi prakash pandey and vivek shukla, "Bluff-Probe based black hole node detection and prevention "IEEE international advance computing conference , march 2009.

[17] Harb, L.M.T.; Tantawy, M.; Elsoudani, M., "Performance of mobile ad hoc networks under attack," Computer Applications Technology (ICCAT), 2013 International Conference on, vol., no., pp.1, 8, 20-22 Jan. 2013.

[18] C.K Toh," Ad hoc mobile wireless networks, protocols and systems" ISBN 978-81-317-1510-9, chapter 3 sec 3.7.8 pp-37. Publisher- PEARSON, 10 th impression 2012.

[19] Charles E. Perkins, "ad hoc networking" ISBN-978-81-317-2096-7, Published- 2008, Chapter- 1,3,5,6,7.

[20] C.K. Toh, "Ad hoc mobile wireless networks protocol and scientist" INBS- 978-81-317-1510-9, Published-2013, chapter – 4,5,7,8,10,11,15.

[21] Theodore S. Rappaport, "wireless communication" ISBN-978-81-317-3186-4, Published- 2013, chapter-1,2,3,10,11.

[22] Rutvij H. jhawari, et al ,"MANET routing protocol and wormhole attack against AODV" international journal

of computer science and network security, VOL. 10 No. 4, April 2010.
[23] Sanjay Sharma et al, " Bluff-probe based black hole node detection and prevention.", IEEE International advance computing conference 6-7 march 2009, 978-1-4244-1888-6, 2008 IEEE.
[24] Golak Panda et al, "prevention of black hole attack in AODV protocol for mobile ad hoc network by key authentication", international journal of computer science and information technology and security, ISSN-2249-9555 vol.2 no.3 june 2012.
[25] Rajib Das et al , "security measure for black hole attack in MANET : An Aproach", international journal for computer science and network security, vol. 3 no 4 may 2012.
[26] R. Stoleru, H.Wu, H. Chenji, "secure neighbor discovery in mobile ad hoc network"IEEE internation conference on Mobile ad hoc and sensor system, 978-0-7695-4469-4/11, 2011.
[27] Jain ming chain et al, "defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." IEEE system journal, ISSN-1932-8184, IEEE 2012.
[28] Zhao min , Zhau Jiliu, "cooperative black hole attack prevention for mobile ad hoc network" , international sumposium on information engineering and electronic commerce, 978-0-7695-3686, IEEE 2009.
[29] M.Gayatri Wahane, Ashsok Kanthe, "technique for detectioin of cooperative black hole in MANET", international conference on advance in engineering and technology. ISSN- 2278-0661,pp-59-76, 2014.
[30] Harris Simaremare, Rifi Fitri Sari, "performance evaluation of AODV variants on DDOS, black hole and malicious attacks", international journal of computer science and network security,VOL.11 NO6 june 2011.
[31] Shraddha Raut and SD Chere, "Detection and removal of balck hole in mobile ad hocnetwork(MANET)" International journal of electrical and electronics engineering (IJEEE) vol-1 iss-4, 2012.
[32] Collin Mulliner, "Vulnerable Analysis and attacks on NFC- enabled mobile phones", international conference on availability , reliability and security., 978-0-7695-3564-7, IEEE 2009.
[33] Lamyaa M.T. et al, "performance of mobile ad hoc network under attack" 978-1-4673-5285, IEEE 2013.