AODV vs. OLSR: An Analytical Approach to Study Black Hole Attack

Sanjay Singh
Computer Science and Engineering Department
IET, Alwar

Deepak Choudhary
Computer Science and Engineering Department
IET, Alwar

ABSTRACT
A MANET (Mobile Ad-Hoc Network) is a temporary network consisting of wireless mobile nodes having no centralized administration and access point. An efficient and dynamic routing protocol is needed that can adapt to dynamically changing network topology and should be energy efficient and bandwidth efficient. But these protocols are not suitable due to resource constraints. There is an increasing threat of malicious nodes attacks on the Mobile Ad-hoc Networks (MANET). One of these attacks is Black Hole Attack, which grasps all data packets of network. It's an analogy to the black hole in the universe in which things disappear.

In this paper Ad-Hoc On Demand Distance Vector(AODV) and Optimized Link State Routing((OLSR) protocols are analyzed to validate which protocol is more vulnerable to Black hole attack and how much. The impact of Black hole attack on the performance of Manet is evaluated on the basis of throughput and end to end delay and it was observed that AODV is more susceptible to attack than OLSR. The measurements were carried on Simulating in Network Simulation Tool (NS2).

Keywords
MANET, Black Hole, Routing Protocols

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is a wireless system where nodes are autonomous and decentralized and free to move in and out of network. Nodes in the network may be mobile phone, PDA, MP3 player, personal computer etc. These nodes can act as host/router or both at the same time [1, 2]. The nodes in MANET can arrange themselves in arbitrary topologies based on their connectivity. These nodes have the ability to configure themselves and due to their self-configuration capability, they can be deployed urgently without the need of any infrastructure Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. [6].

In Mobile Ad-Hoc Network Security is the most significant concern for the basic functionality of network. The accessibility of network services, secrecy and integrity of the data can be achieved by assuring that security issues have been meet. MANETs frequently undergo from security attacks because of its features like open medium, frequent changing its topology dynamically, decentralized monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the circumstances for the MANETs against the security threats.

The MANETs function with a decentralized administration where the nodes communicate with each other based on mutual trust. This feature makes MANETs more vulnerable to be exploited by an enemy inside the network. Wireless links also makes the MANETs more vulnerable to attacks, which make it easy for the attacker to go within the network and get access to the current communication [8, 13]. Mobile nodes in the network can overhear or participate in the network. The critical issue in MANET is to ensure secure communication and transmission in presence of increasing security threat. Nowadays, the voice of the day is Security. To ensure secure communication and transmission, the experts must recognize various types of threats and their consequences on the MANETs. MANET may undergo attacks like Black hole attack, Wormhole attack, Sybil attack, flooding attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack etc. [14]. A MANET is open to these kinds of attacks due to the phenomenon that the communication is based on mutual trust among the nodes. There is decentralized network management, no authorization facility, dynamically changing topology and limited resources.

2. REVIEW OF LITERATURE
Black Hole, Wormhole, Jellyfish, DoS, DDos, Impersonation security threats and attacks have been described focusing on their nature and their consequences[12.14.18].Amongst them, Black hole attack is mainly analyzed on Adhoc On Demand Distance Vector(AODV) and shown how it disrupts the performance of MANET. Inadequate attention has been shown towards study of Black hole attack on both Reactive and Proactive protocols and comparing their performance of both protocols against the attack. Inadequate attention has been shown towards study of Black hole attack on both Reactive and Proactive protocols and comparing their performance of both protocols against the attack. To address the behavior and the impact of both protocols against the Black hole attack and analyze AODV and OLSR on different parameters to compare which protocol is less vulnerable is the motive of this paper.

Despite the fact of popularity of MANET, these networks are very much exposed to attacks. MANETs are more vulnerable to security attacks due to wireless links so that attackers can easily enter the network and gain access to the communication [9]. MANETs have been analyzed to know the impact on the network under different attacks. MANETs routing protocols are being exploited by the attackers under flooding attack that is done by the attacker either by victimization RREQ or data flooding [16].

In any network, the sender wants its data to be sent as soon as possible in a secure environment efficiently The attackers announce in the network of having shortest path and high bandwidth for transmission. The attackers put themselves to strong strategic positions thus making simplest use of location in the network (i.e. shortest path between the nodes). The most arising problems in MANET is that of restricted battery, attackers take the benefit of that and tries to keep the nodes awake till all energy of the attacked node is lost and

therefore the node get in permanent sleep [18]. Several different attacks in MANET like jellyfish attack, modification attack, misrouting attack and Routing Table Overflow are studied and exposed.

In Distributed denial of Service (DDoS), the attacker targets multiple nodes in the network. Such attack is used to enter into large number of machines; these machines are further used to attack the aimed targets. These attacks are used in order to consume the bandwidth of the targets and to block, jam and restrict access of any other machine to the network [4]. In [11] a spatial correlation detection technique is proposed. This method first approximates the abnormality of every origin destination flow. Once estimation is performed after origin destination flow with same destination is compared and spatial correlation comes between their abnormalities. DDoS attacked are often detected by any abrupt modification within the spatial correlation.

A malicious node declares in the network that he is having the shortest path to destination for the packet he intends to intercept in black hole attack.

This hostile node advertises its accessibility of recent routes no matter checking its routing table. In this approach, the node is always ready to reply to the route request and therefore intercept the data packet and retain it [10]. Detection of black hole attack is amongst the critical problems so as to secure the network from such attacks. In [3] a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Black Hole attack.

3. PROBLEM STATEMENT AND MAIN CONTRIBUTION

Aims and objectives of this study work are summarized as follow

- The study center on scrutiny of black hole attack and its consequences in MANET
- Analyzing the consequences of black hole attack in presence of of Network load, throughput and end-to-end delay in MANET
- Simulating the black hole attack using AODV and OLSR.
- Comparing the results AODV and OLSR to analyze which of these two protocols are more vulnerable to Black Hole attack

The ultimate goal of any network is to ensure successful transmission between the devices in the network in a secure environment. Here, the goal is to investigate the impact and vulnerability of both routing protocols under black hole attack in the network.. This paper addresses the followings.

We will discuss the results of black hole attack in this paper? This question is vital as a result of the issue to understand however severe the attack is, what quantity the network is destabilized. This may facilitate the researcher to figure on the isolation of such threats in MANETs. The paper conjointly measures the performance impact of MANETs during a normal operation as well as under black hole attack. Investigation will be carried out which one of these two types of routing protocols is more vulnerable to the Black Hole attack on MANET

4. BLACK HOLE ATTACK

In black hole attack, a malicious node announces itself of having shortest path or to the packet towards destination. The hostile node also announces of its accessibility of existing routes without checking its routing table. thus aggressor node can continuously have the supply in replying to the route request and hence interception can occur In protocols that support flooding, the requesting node receives reply from malicious node before the reply from actual node; thus creating a forged and malicious route. Once the route is created, whether to forward or drop packets it is up to the malicious node[19]..

The method however malicious node fits within data routes varies. In Fig.1, showing Black hole problem, here node "A" need to send knowledge packets to node "D" and initiate the route discovery method. therefore if node "C" could be a malicious node then it'll claim that it has active route to the desired destination as it receives Route Request (RREQ) packets. it'll then send the response to node "A" before the other node. In this way node "A" will consider that this is the active route and thus active route discovery is complete. Node "A" will overlook all other replies and will start sending data packets to node "C". This consumes all the data packets and hence the packets are lost.

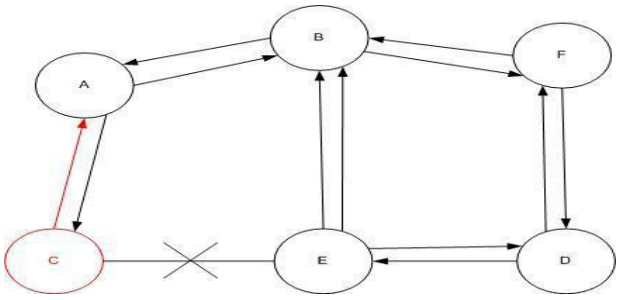


Fig. 1 Black Hole attack in AODV

In Optimized Link State Routing (OLSR) [7] black hole attack, Multi Point Rely (MPR) is selected forcefully by malicious node. The HELLO message is kept continuously in willingness filed by malicious node.. Therefore, malicious node is always selected as MPR by its neighbors.. Thus the malicious node earns a privileged position within the network that it exploits to hold out the denial of service attack

5. PROPOSED METHOD

The packet end-to-end delay, network, network load and network throughput are chosen as performance metrics for the analysis of black hole attack.. The packet end-to-end delay is defined as the average time to traverse in the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the delay of networks as well as buffer queues, transmission time and delay as a result of routing activities.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits/sec or pack/sec. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

The tool used for the simulation study is NS2.35 modeler. NS2 is a network and application based software used for network management and analysis. NS2 models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. NS2 provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WI-MAX, Wi-Fi, UMTS, analysis and designing of MANET protocols.

In this study we employed NS2 for modeling the network nodes, selecting its statistics and then running its simulation to obtain the result for the analysis In Fig. 2, the scenario consisting of 30 mobile nodes for a simulation setup has been depicted. There are 12 different scenarios that have been developed and the mobility of nodes has been set to 10 m/s with simulation time at 1000 seconds. This time is taken so that the simulation get stable, in the first 300 seconds simulation is varying subsequently start getting stable for rest of the time. Simulation area taken is 1000 x 1000 meters, which enough for 15 and 30 nodes to move freely without being crowded. Second reason is if we take area more than the one taken, the distance between each node will increase that will introduce extra delay due to the long distance between the nodes. Packet Inter-Arrival Time (sec) and packet size (bits) is taken exponential (1) is exponential (i.e.1024) respectively.

The data rates for mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random point mobility was selected with the constant speed of 10 meter/seconds and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only.

Our aim was to verify the protocol which shows less vulnerability in presence of black hole attack. AODV and OLSR routing protocols were chosen as reactive and proactive protocols respectively. In each case AODV and OLSR, buffer size of malicious node is lower to a level which increase packet drop. Table.1 shows Architectural experiments.

Table.1 Simulation Parameters

SIMULATION PARAMETERS	
Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m * m)	1000 *1000
Number of Nodes	15 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random

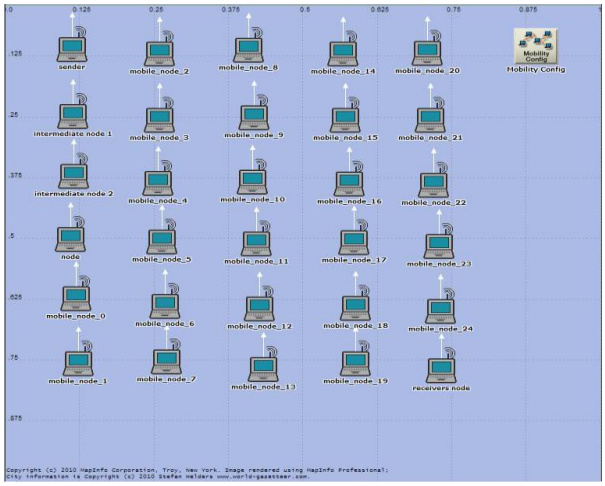


Fig. 2 Proposed Experimental Setup

6. RESULTS

In case of with and without black hole attack, packet end-to-end delay depends upon the routing protocol and number of nodes. Fig. 3 shows that delay is high for AODV and OLSR for 15 nodes (in case of no black hole attack). During black hole attack, RREQs and RREPs are not required as the malicious node sends its RREQs in advance to sender node without waiting for reply from destination node with less delay. Due to reactive nature and route search, AODV has high delay in comparison with OLSR.

In the case of 30 nodes the delay is 5 percent more as compared to the case of 15 nodes. This increase in delay is due to the additional nodes in the topology through which the data passes to the destination node. As the number of nodes increases the delay increased. The overall impact of delay on AODV and OLSR is same as it was observed in 15 nodes. However increase in the numbers of nodes also increases the difference of delay in AODV in case (of Black Hole attack) with comparison to a simple AODV scenario

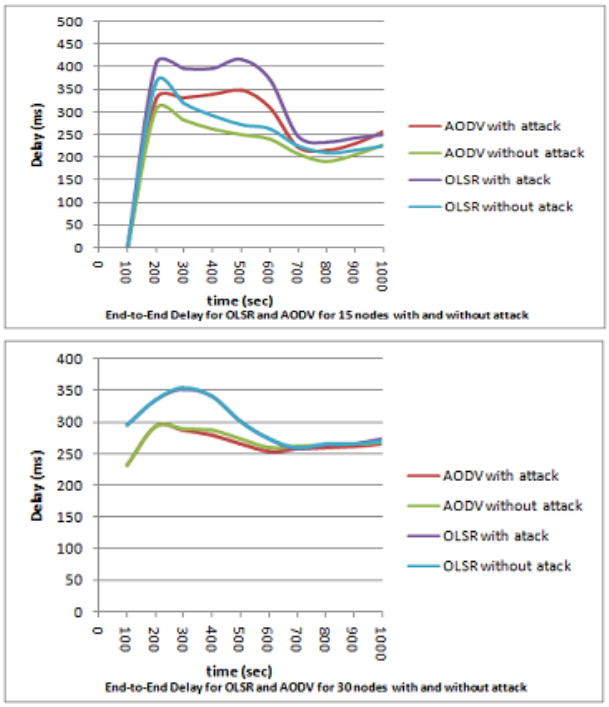
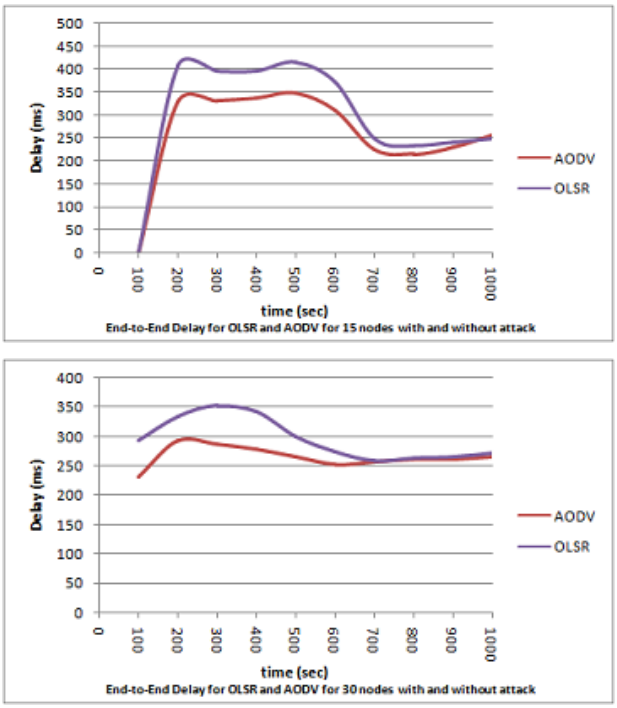


Fig. 3 End-to-end delay for OLSR and AODV (with vs. without attack)

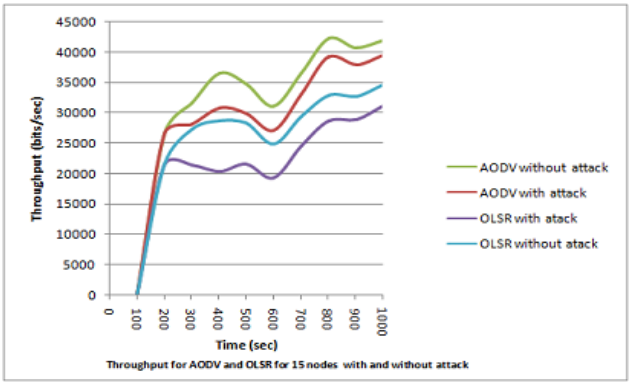
Fig. 3 and Fig. 4 show the average packet end-to-end delay in presence of a malicious node only. Fig. 3 shows that OLSR has slightly higher delay than to AODV (for 15 and 30 nodes) respectively. This is consistent if the numbers of nodes are less. However with the increase in number of node an increase in the delay of AODV has been observed as shown in Fig.4, for 30 nodes. In terms of delay the performance of OLSR improves with the increase in number of nodes because of its table driven nature. It maintains up to date routing information from each node to every other node in the network.

From Fig. 5, (for 15 nodes), it could be observed that the throughput for OLSR is high compared to that of AODV Also, throughput of OLSR is higher under no attack compared to under attack. This occurs due to less routing and forwarding. In this case the data is discarded instead of forwarding by malicious node affecting throughput.



Fig,4 End to End Delay 30 Nodes AODV vs OLSR(with attack)

The same is also observed with AODV, where throughput is higher under without attack with respect to under attack as malicious node discards packets. Likewise in Fig. 5 (for 30 nodes), due to high number of nodes, throughput is high however the trend for throughput is same in 15 number of nodes with and without attack..



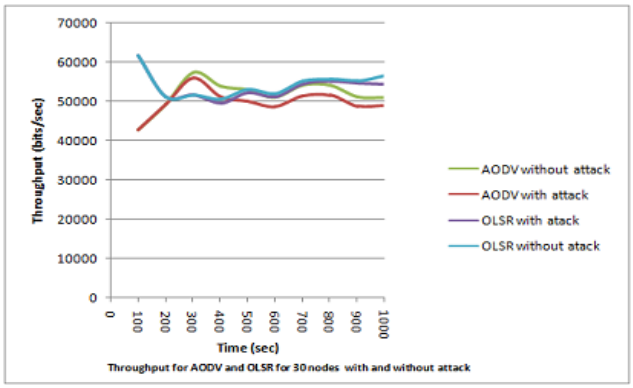


Fig. 5 Throughput for OLSR and AODV (with vs. without attack)

Fig. 6 shows the throughput of AODV and OLSR in the presence of a single malicious node. It is obvious from both figures that OLSR by far outperforms AODV in case of both 15 and 30 sources. Before routing the traffic, OLSR makes sure about the availability of routing path. It has been seen that difference in throughput is less when high number of sources are compared with less number of sources, since congestion is more in high number of sources. Over all, OLSR lowers the delay by ensuring consistent routing paths. Since throughput is defined as the ratio of total data received from source by the time receiver receives the last packet. A lower delay results in higher throughput. Because of route reply, the overall throughput of AODV is low. The malicious node sends its route reply immediately as well as discards all the data sent to him. The network throughput is significantly lower.

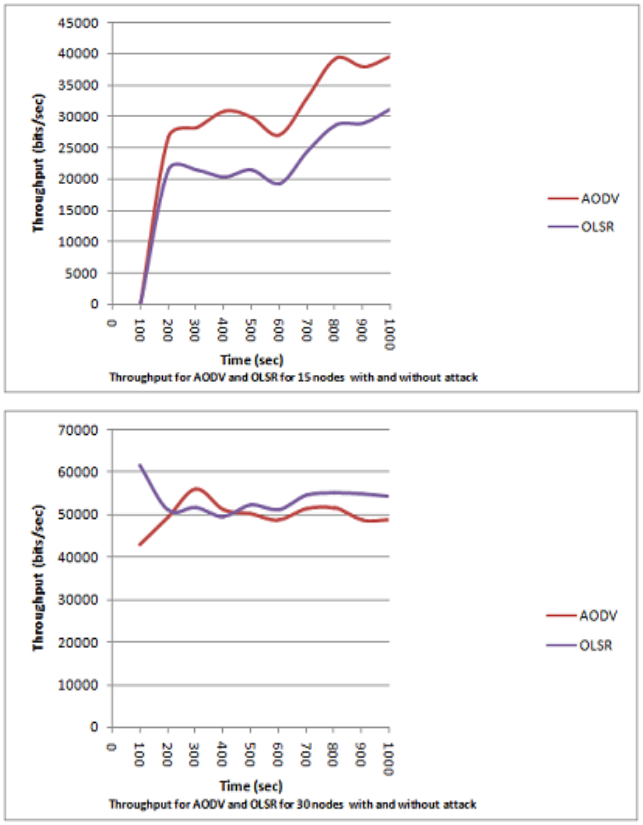


Fig. 6 Throughput for AODV vs. OLSR (with attack)

Since there is no centralized security mechanism, the networks are exposed to internal as well as external attacks. With the importance of MANET comparative to its huge potential it's still several challenges left to overcome. MANET's security is one of the vital features for its deployment. We have analyzed the performance and challenges of black hole attack in mobile Ad-Hoc networks. The MANET is simulated and its behavior is analyzed under black hole attack for matrices like End-to-End delay and Throughput . The results obtained from simulation are analyzed deeply in order to draw the final conclusion.

7. CONCLUSION AND FUTURE WORK

The black hole attack is analyzed for AODV and OLSR under four different scenarios for end-to-end delay and throughput. It is essential for a protocol that it should be redundant and efficient in term of security in a network. An investigation on the vulnerability of two protocols OLSR and AODV have been studied.

It was observed that when there is higher number of nodes and more route requests, it affect the network performance more. As compared to OLSR, throughput of AODV is affected twice. The malicious node affects AODV less as compared to OLSR with respect to network load. From view point of impact of black hole attack in MANET, it was observed that AODV is affected more than OLSR. This leads to conclusion that AODV is more vulnerable than OLSR under black hole attack.

An effort has been created to debate and analyze the impact of black hole attack in MANETs using AODV and OLSR protocols. There's a requirement to research black hole attack in different MANETs routing protocols like DSR, TORA and GRP. Different sorts of attacks like wormhole, DOS, Jellyfish and Sybil attacks are required to be studied as compared with black hole attack. they may be categorized on the basis of what proportion they have an effect on the performance of the network. Black hole attack can even attack the opposite means around i.e. as Sleep Deprivation attack. A study on the detection of this behavior of black hole attack and elimination strategy for such behavior is presently into consideration.

8. REFERENCES

[1] Rakhi Purohit, Hari Singh Choudhary, Vikas Choudhary " Performance Evaluation of Ad Hoc Routing protocols with NS2 " IJCSET, January 2012, Vol 2, Issue 1, 787-791

[2] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks", Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[3] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[4] Akshay Kansra, Ankur Sehgal, " Improvement of Black Hole Detection Technique in Wireless Sensor Network",IJEDR, Vol. 4,Isue 3, ISSN:2321-9939.

[5] C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: April. 10, 2010]

[6] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[7] T. Clausen, P.Jacquet , "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, 2003.

[8] P. V. Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 2002.

[9] Jasmeen Kaur, Tanupreet Singh, "Enhanced Proactive Secret Sharing Scheme to Prevent Black Hole Attacks in MANETs", International Journal of Computer Applications (0975-8887), Volume 119-No 10, June 2015.

[10] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265,

[11] Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[12] V. Mahajan, M. Natue and A. Sethi, "Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[13] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks", University of Cincinnati, IEEE Communication Magazine, Oct, 2002.

[14] Konagala Pavani andDamodaram Avula, "Performance of Mobile Adhoc Networks in Presence of Attacks", International Conference on Information Secuity and Artificial Intelligence (ISAI 2012), 2012 vol.56 (2012), IACSIT Press Singapore.

[15] Anjali Joy and Sijo Cherian, "Black Hole Attack and its Mitigation Techniques in OLSR and AODV", IJCSET , ISSN:2229-2245, Vol 4 No. 06, 2013

[16] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-Hoc Networks", ACM Southeast Regional Conf. 2004.

[17] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless Ad-Hoc networks", Cincinnati Univ.,OH, USA; IEEE Communications Magazine, , Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.

[18] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks", In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer Science, California Univ., Santa Barbara, CA, USA. pp.78- 87, ISSN: 1092-1648, Nov. 2002.

[19] S.Sharma, Rajshree, R.P.Pandey, V.Shukla, "Bluff-Probe Based Black Hole Node Detection and Prevention", IEEE International Advance Computing Conference (IACC 2009), pp. 458-462, March, 2009.