Journal of Theoretical and Applied Information Technology
10th August 2014. Vol. 66 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PERFORMANCE EVALUATION OF DYNAMIC SOURCE ROUTING UNDER BLACK HOLE ATTACK

[1]RAJESHKUMAR.G, [2]Dr.K.R.VALLUVAN
[1]Assistant Professor (Senior Grade), Department of Information Technology, Velalar College of Engineering and Technology, Erode-638 012, Tamil Nadu, India.
[2]Professor and Head, Department of Electronics and Communications Engineering, Velalar College of Engineering and Technology, Erode-638 012,Tamil Nadu, India.
E-mail: [1]grajesh_grk@yahoo.com, [2] krvalluvan@yahoo.co.in

ABSTRACT

Mobile Ad hoc Network (MANET) is a network that does not have a fixed infrastructure and have the ability to manage its network independently. It consists of a collection of “peer” mobile nodes that are capable of communicating with each other. Nodes within each other's radio range, communicate directly via wireless links, while those that are far apart use other nodes as relays in a multi-hop routing fashion. Since mobile ad hoc networks make it possible for the devices to join or leave the domain without required permission, nodes in the domain cannot be completely trusted. This makes MANET susceptible to attacks from malicious nodes. In this work, the impact of black hole attack on MANET is evaluated. In this work, the impact of black hole attack on MANET is evaluated. Simulations were carried out using Dynamic Source Routing (DSR) for network without malicious nodes and with 10% malicious nodes. Simulation results show that the throughput degrades by 45.44 % and the end to end delay increases by 38.3 % due to the presence of malicious nodes in the network.

Keywords*:* *MANET, Dynamic Source Routing (DSR), Routing, Attacks in MANET, Blackhole Attack*

1. INTRODUCTION

Applications Mobile ad-hoc networks (MANET) are self-organized networks made up of mobile nodes without fixed infrastructure. They can be rapidly deployed and reconfigured. Applications for MANETs are diverse: ranging from small static networks that are constrained by power sources, to large scale, mobile, and highly dynamic networks. Success in operations of a mobile ad hoc network depends on cooperation of the nodes in providing services to each other. Since mobile ad hoc networks make it possible for the devices to join or leave the domain without required permission, nodes in the domain cannot be completely trusted. Conventional security approaches do not address all concerns of ad hoc networks since both benign and malicious parties have full admission to communicate with peers. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. In spite of the dynamic nature, mobile users may apply for anytime, anywhere security services as they are in motion from one place to another. Consequently a security solution is required which has both extensive protection and desirable network performance [1].

MANETs differ from conventional cellular networks because all links are wireless and the mobile users communicate with each other without using a base station. Several basic properties of MANETs are described below. An autonomous collection of mobile users composes a MANET, where they communicate over relatively bandwidth constrained wireless links. MANETs use peer-to-peer wireless connections, where the packets from a source node are transmitted via intermediate nodes called relay nodes towards a destination node. A MANET topology dynamically changes as mobile users join, leave, or re-join the network. Sometimes, radio links in a MANET may not be usable due to the node mobility [2].

MANET is a dynamic network due to its node mobility and can be deployed as multi-hop networks [3]. The ability of the network to meet its goals depends directly upon the input fed into the decision process. A big challenge facing MANET researchers is how to generate and capture the factors relevant to the everyday operation of the network. Equally significant in today’s MANET decision algorithms is the lack of consideration given to security factors in the decisions that drive the network's organization and operation. However, the incorporation of security factors must be supported by an organizing structure that facilitates automated decision processes.

Routing is the process of information exchange from one host to the other host in a network [4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself.

1.1. Security in MANETS:

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types as:

- Passive attack
- Active attack

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected.

One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. E.g. Snooping: Snooping is unauthorized access to another person's data.

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network [5-8].

1.2. Black Hole Attack:

Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route Reply (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. By comparing the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the most recent routing information and selects the route contained in that RREP packet.

In case the sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker. Therefore, source and destination nodes became unable to communicate with each other [9].

In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack [10].

The method how malicious node fits in the data routes varies. Figure 1 shows how black hole problem arises. Here node "A" wants to send data packets to node "D" and initiates the route discovery process. So if node "C" is a malicious node, then it will claim that it has active route to the specified destination as soon as it receives Route Request (RREQ) packets.

It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete.

Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost [11].

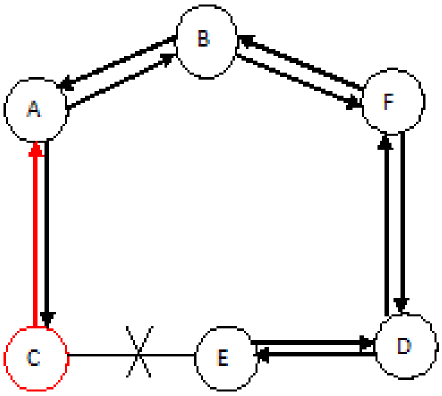

Figure 1: Black Hole Problem

In figure 2, Node A which is a malicious node, can forge a RREP message to the source node S. When source node S receives faked RREP message from node A, it updates its route to the destination node through attacking node. When node A receives the data packets it drops the packets as shown in figure 2.

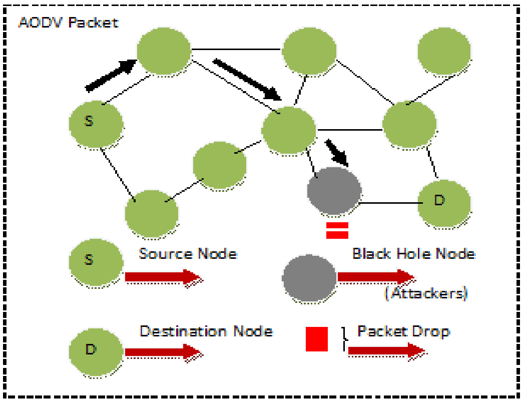

Figure 2: Black Hole Attack Packet Dropping

A Black Hole attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery. A Black Hole node has following two properties

1. The node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is fake, with the intention of intercepting packets.

2. The node consumes the intercepted packets. The malicious node always sends RREP as soon as it receives RREQ without performing standard Ad hoc On-demand Distance Vector (AODV) operations, while keeping the Destination Sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting Black Hole attack [12].

In this paper, the impact of black hole attack on MANET is evaluated. For evaluation DSR is considered. The paper is organized as follows: Section 2 reviews some of the related works available in the literature. Section 3 details the DSR routing and performance metrics used to evaluate the impact of black hole on MANET. Section 4 gives the experimental results and section V concludes the paper.

2. LITERATURE SURVEY:

Saxena and Rana et al [13] provided a behavioral analysis of malicious and selfish nodes in the DSR protocol and how Observation Based Cooperation Enforcement in Mobile Ad hoc (OCEAN) finds it's utility to reduce the effect of these malicious nodes when used over DSR. Experimental results showed that the DSR using OCEAN Protocol decreased the End-to-End delay, but this occurred at an expense of increased time consumption and thus increased power consumption.

Diwaker and Choudhary et al [14] proposed a simple detection algorithm that would detected the black hole attacks before the actual routing mechanism was started by using fake RREQ packets to catch the malicious nodes an algorithm to detect the black hole attacks in MANET has been proposed. The proposed algorithm removed the disadvantages of the Detecting Black hole Attacks DSR (DBA-DSR) algorithm. In DBA-DSR algorithm, the routing overhead and route discovery period increased. But in the proposed algorithm, the routing overhead decreased and route discovery period also decreased.

Bala et al [15] proposed Performance Analysis of MANET under Black hole Attack. They simulate the black hole attack which is one of the possible attacks on AODV routing protocol in MANET by the help of network simulator (NS-2). The simulation results showed the packet loss, throughput, and end-to-end delay with black hole and without black hole on AODV in MANET. It is analysed that the packet loss increases in the network with a black hole node. It is also observed that the throughput and end-to-end delay decreases in the network with a black hole node.

Bhalaji and Shanmugam et al [16] proposed association between nodes to combat black hole attack in DSR based MANET. The work analysed the black hole attack which is one of the possible and commonest attacks in ad hoc networks. In this attack the malicious nodes advertise itself having the shortest path to the destination. The authors approach classified nodes in to three categories based on their behaviour. The extents of association between the nodes are used for the route selection. The authors had conducted extensive experiments using the network simulator-2 to validate our research.

Bindra et al [17] analysed detection and removal of co-operative black hole and gray hole attacks in MANETs. A mechanism to detect and remove the black hole and gray hole attacks is proposed. The solution they proposed tackles these attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. The mechanism is capable of detecting a malicious node. It also maintains a history of the node's previous malicious instances to account for the gray behaviour. Refresh packet, Renew Packet, BHID Packet, Further request and further reply packets are also used in addition to the existing packets (RREQ and RREP). The technique was capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

Jhaveri et al [18] introduced Multiple-route Ad hoc On-demand Distance Vector (MR-AODV), a solution to mitigate Black hole and Gray hole Attacks in AODV based MANETs. Black hole and Gray hole attacks are such attacks that drop significant number of packets by performing packet forwarding misbehaviour and breach the security to cause denial of service in Mobile Ad-hoc Networks (MANETs). In this work, the author discussed the previous work, Reliable Ad hoc On-demand Distance Vector (R-AODV), to detect and isolate multiple Black hole and Gray hole nodes during route discovery process and propose a modified version to improve the performance of MANET. The method analysed the proposed solution and evaluate its performance using Network Simulator-2 (NS-2) under different network parameters.

Woungang et al [19] proposed a novel scheme for Detecting Black hole Attacks (DBA-DSR) in MANETs. The DBA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes. Simulation results are provided, showing that the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics; when black hole nodes are present in the network.

Detecting malicious packet dropping is important in ad hoc networks to combat a variety of security attacks such as blackhole, greyhole, and wormhole attacks. Hayajneh et al [20] consider the detection of malicious packet drops in the presence of collisions and channel errors and describe a method to distinguish between these types. The author presented a simple analytical model for packet loss that helps a monitoring node to detect malicious packet dropping attacks. The model is analysed and evaluated using simulations. The results show that it is possible to detect malicious packet drops in the presence of collisions and channel errors.

3. PERFORMANCE Of DSR:

In This Paper, the impact of black hole attack is observed in MANET. The experimental setup consists of 30 nodes distributed over two square kilometres and DSR protocol is used for routing. Two experiments are conducted: first without malicious nodes and the second with 10% of the nodes being malicious.

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.
- Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, Scan attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D [21].

The performance of the network is evaluated using throughput and end to end delay. Throughput is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.

It is defined as,

Throughput= N/1000

Where N is the number of bits received successfully by all destinations [22].

End to End delay is the average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. It is defined as,

Avg. EED=S/N

Where S is the sum of the time spent to deliver packets for eachdestination, and N is the number of packets received by the all destination nodes [23].

4. RESULTS AND DISCUSSION

In this paper, the impact of black hole attack in MANET is evaluated. The experimental setup consists of 30 nodes distributed over two square kilometres. DSR routing protocol is used. Two experiments are conducted: first without malicious nodes and second with 10% of the nodes being malicious. Figure 3 and 4 depicts the throughput and end to end delay of the network with and without malicious nodes. Table 1 and 2 tabulate the same.

Table 1: Throughput in bits/sec

Simulation time in second	Throughput in bits/sec	
	DSR	DSR with Blackhole attack
30	42792	29110
60	57716	32472
90	57160	31036
150	43150	27382
192	47846	23252
240	44914	30469
300	49825	29592
360	52309	26633
462	57929	37177
468	49968	23000
540	57396	22237
600	52564	39708

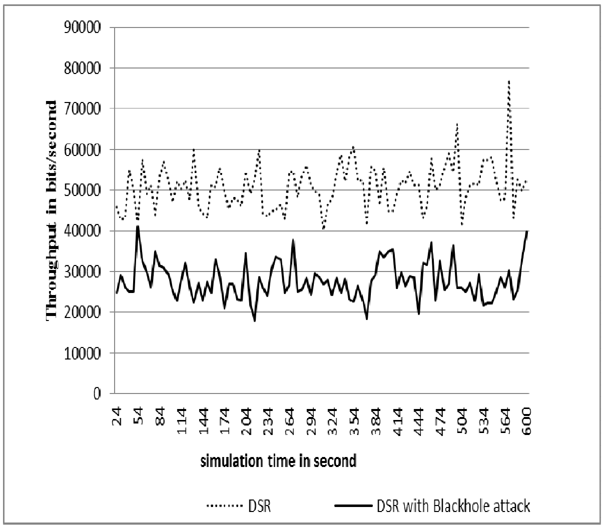

Figure: 3: Throughput in bits/second

From figure 3 it is seen that the throughput is decreased by 45.44 % due to the blackhole attack for DSR.

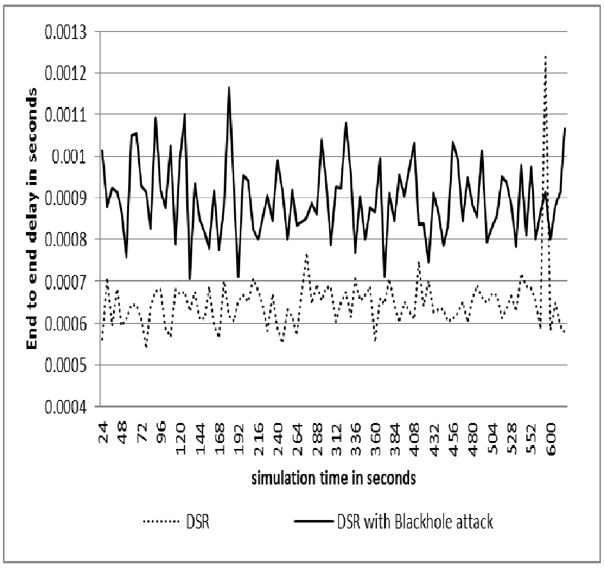

Figure: 4: End to end delay in second

Table 2: End to end delay in second

Simulation time in second	End to End Delay in second	
	DSR	DSR with Blackhole attack
30	0.000709256	0.000880386
60	0.000643642	0.001049396
120	0.000669134	0.000992199
150	0.000612195	0.000816237
210	0.000706501	0.000825522
276	0.0007693	0.00085211
300	0.000685665	0.00094475
360	0.00055428	0.000867656
402	0.000628739	0.000970933
462	0.000626187	0.000993193
528	0.000665689	0.000884104
588	0.000594035	0.000914873
600	0.000578656	0.001065744

From figure 4 it is seen that the end to end delay is increased by 38.3 % for DSR when the network has blackhole attack.

Figure 5 to 7 show the results obtained for Average Cache Replies, average number of hops and average route discovery time.

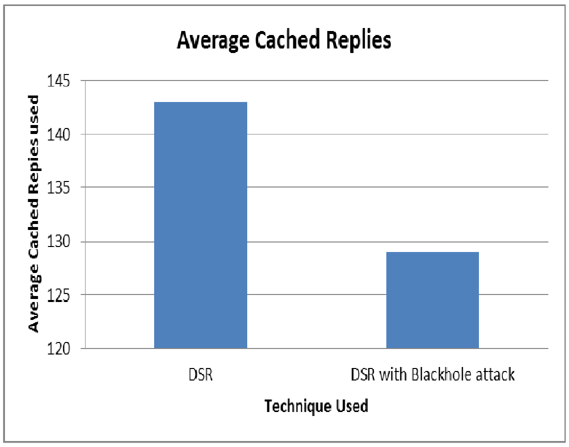

Figure 5: Average Cached Replies used

In figure 5, it is seen that the due to black hole attack, the average cached replies used decreases by 10.42%

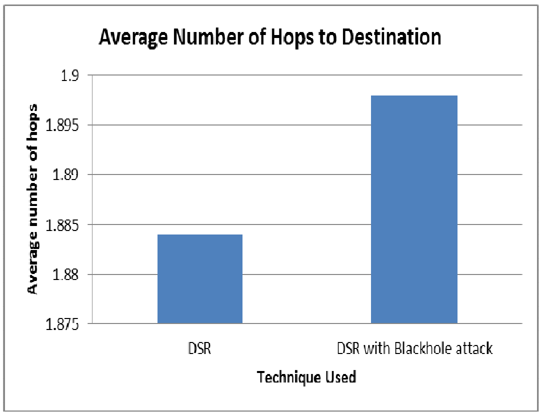

Figure 6: Average Numbers of Hops to Destination

From figure 6, it is observed that the blackhole attack increases average number of hops to destination.

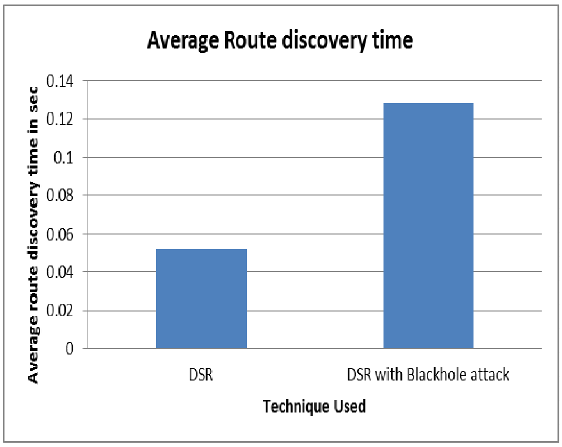

Figure 7: Average route discovery time

The average route discovery time drastically increases due to blackhole attack as seen in figure 7.

5. CONCLUSION

Success in operations of a mobile ad hoc network depends on cooperation of the nodes in providing services to each other. Since mobile ad hoc networks make it possible for the devices to join or leave the domain without required permission, node in the domain cannot be completely trusted. In this work, the impact of black hole attack in MANET is evaluated. The experimental setup consists of 30 nodes distributed over two square kilometres. DSR routing protocol is used. Two experiments have been conducted: first without malicious nodes and second with 10% of the nodes being malicious.

Simulation results show that the throughput degrades by 45.44 %, the end to end delay increases by 38.3 % and average cached replies used degrades by 10.42 % due to black hole attack. The number of hops required to reach destination is increased in malicious network and also the route discovery time is more. Further work is required to investigate methods to mitigate the impact of blackhole attack.

REFRENCES:

[1] Ismail, Z., & Hassan, R. (2011, October). A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET. In *Communications (APCC), 2011 17th Asia-Pacific Conference on*(pp. 637-642). IEEE.

[2] Mohamed, Y., & Abdullah, A. (2008). Security Mechanism for MANETs. *Journal of Engineering and Science Technology*, 231-242.

[3] Kim, S. C., & Chung, J. M. (2008). Message complexity analysis of mobile ad hoc network addresses auto configuration protocols. *Mobile Computing, IEEE Transactions on*, *7*(3), 358-371.

[4] Shrivastava, A., Shanmogavel, A. R., Mistry, A., Chander, N., Patlolla, P., &Yadlapalli, V. (2005). Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols.

[5] Johnson, D. B., Maltz, D. A., &Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, *5*, 139-172.

[6] Rai, A. K., Tewari, R. R., &Upadhyay, S. K. (2010). Different types of attacks on integrated MANET-Internet communication. *International Journal of Computer Science and Security*, *4*(3), 265-274.

[7] Nandy, R., & Roy, D. B. (2011). Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme. *Int. J. Advanced Networking and Applications*, *3*(01), 1035-1043.

[8] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*, 32-37.

[9] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2007). Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. *IJ Network Security*, *5*(3), 338-346.

[10] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97). ACM.

[11] Ullah, I., &Rehman, S. U. (2010). Analysis of Black Hole attack on MANETs Using different MANET routing protocols. *School of Computing Blekinge Institute of Technology, Sweden.*

[12] Gurjar, A. A., &Dande, A. A. Black Hole Attack in Manet's: A Review Study.

[13] Saxena, A., &Rana, J. L. (2010). Analysis of Selfish and Malicious Nodes on DSR Based Ocean Protocol in MANET. *International Journal of Computing Science and Communication Technologies*, *3*(1), 570-575

[14] Chander Diwaker &Sunita Choudhary (2013). DETECTION OF BLACKHOLE ATTACK IN DSR BASED MANET International Association of Scientific Innovation and Research (IASIR) (An Association Unifying the Sciences, Engineering, and Applied Research)

[15] Bala, A., Bansal, M., & Singh, J. (2009, December). Performance analysis of MANET under blackhole attack. In *Networks and Communications, 2009. NETCOM'09. First International Conference on* (pp. 141-145). IEEE.

[16] Bhalaji, N., &Shanmugam, A. (2009, April). Association between nodes to Combat Blackhole attack in DSR based MANET. In *Wireless and Optical Communications Networks, 2009. WOCN'09. IFIP International Conference on*(pp. 1-5). IEEE.

[17] Singh Bindra, G., Kapoor, A., Narang, A., &Agrawal, A. (2012, September). Detection and removal of co-operative blackhole and grayhole attacks in MANETs. In *System Engineering and Technology (ICSET), 2012 International Conference on* (pp. 1-5). IEEE.

[18] Jhaveri, R. (2013, January). MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs. In *Accepted and To be published In: Proceeding of International Conference on Advanced Computing & Communication Technologies (ACCT 2013), CPS (IEEE Computer Society).*

[19] Woungang, I., Dhurandher, S. K., Peddi, R. D., &Obaidat, M. S. (2012, May). Detecting blackhole attacks on DSR-based mobile ad hoc networks. In*Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on* (pp. 1-5). IEEE.

[20] Hayajneh, T., Krishnamurthy, P., Tipper, D., & Kim, T. (2009, June). Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In *Communications, 2009. ICC'09. IEEE International Conference on* (pp. 1-6). IEEE.

[21] Malany, A. B., Dhulipala, V. S., &Chandrasekaran, R. M. (2009). Throughput and Delay Comparison of MANET Routing Protocols. *Int. J. Open Problems Compt. Math*, *2*(3), 462-468.

[22] PankajRoha Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV) Vol. 1, Issue II, Mar. 2013 ISSN 2320-6802

[23] B.N. Singh, Bhim Singh, Ambrish Chandra, and Kamal Al-Haddad, “Digital Implementation of an Advanced Static VAR Compensator for Voltage Profile Improvement, Power Factor Correction and Balancing of Unbalanced Reactive Loads”, *Electric Power Energy Research*, Vol. 54, No. 2, 2000, pp. 101-111.

[24] J.B. Ekanayake and N. Jenkins, “A Three-Level Advanced Static VAR Compensator”, *IEEE Transactions on Power Systems*, Vol. 11, No. 1, January 1996, pp. 540-545.