ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

# Resisting Black hole Attack in MANET

R.Siva Subbiah[1], Dr. K.E.Kannammal[2]

Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Sri Shakthi Nagar, L&T By - Pass, Chinniyampalayam Post, Coimbatore, Tamilnadu, India.

Head of the Department, Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Sri Shakthi Nagar, L&T By - Pass, Chinniyampalayam Post, Coimbatore, Tamilnadu, India.

**ABSTRACT:** Mobile Ad-Hoc Networks (MANET) a fast growing network scheme and it provides lots of features to communication strategies and routing protocols. Theses routing protocols are introduced to avoid the attacker nodes and provides the efficient communication between source and destination. The attacks in the network scenarios are: DOS, Wormhole attack and Blackhole attacks. In this system, a new routing protocol strategy is defined by means of Route Request and Route Response Strategies with the help of Blackhole Resisting Mechanism (BRM). Source Node sends Route Request to the nearby node. The nearby node checks the request and sends the Route Response to Source Node back within a proper interval. The proper and relevant response from the neighbor node indicates it as a proper node as well as the neighbor node sequence Number will get incremented by 1. The node is proper then only the count will be incremented otherwise it consists attack content. This kind of nodes are properly blocked from the present scenario and the source checks for the alternate or other neighbor nodes to proceed for further communications. As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology. Along with these routing strategies we introduce a novel crypto algorithm to dictate the data security. Once the data is transmitted from source it carries only cipher data not an actual content, so no one in mid part can attack the data or retrieve it for their use. This kind of mechanisms provides strengthen to the routing principles to avoid attacking and provide trust worthy routing schemes.

**KEYWORDS:** Attack Prevention, MANET, BlackHole Attack, DoS attack, Routing Protocol.

## I. INTRODUCTION

A Mobile Ad Hoc Network [MANET] is a decentralized infrastructure less system in which hubs coordinate to forward information from a source to a goal. Every hub in MANET demonstrations both as a switch and as a host. A few directing conventions have been intended for MANETs to improve arrange steering execution. The significant issues required in outlining a directing convention for MANET are hub portability, data transmission obliged and mistake inclined remote channel, asset compelled hubs, and dynamic changing of the system topology. MANET steering conventions can be named proactive or responsive directing conventions. In proactive steering conventions, every hub keeps up at least one table containing directing data to each other hub in the system.

While in responsive steering conventions, courses are made at whatever point a source requires to send information to a goal hub which implies that these conventions are started by a source on-request. In this paper, we concentrate on the AODV convention which is one of the broadly concentrated receptive conventions, considered by the IETF for institutionalization. Ordinary MANET steering conventions accept that all hubs participate without vindictively upsetting the operation of the convention and don't give safeguard against malevolent aggressors.

Be that as it may, the presence of malignant hubs can't be disregarded in PC systems, particularly in MANETs in light of the remote way of the system. MANET acquires security dangers that are confronted in wired and additionally remote systems and furthermore acquaints security assaults one of a kind with itself due its attributes. Hubs in MANET have constrained calculation and power abilities that make the system more helpless against Denial-of-Service [DoS] assaults. It is hard to execute cryptography and key administration calculations which require significant calculations like open key calculations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Hub versatility presents additionally a trouble of recognizing stale courses and fake courses. A noxious hub can assault the system layer in MANET either by not sending bundles or by changing a few parameters of steering messages, for example, arrangement number and IP addresses, sending fake messages a few times and sending fake directing data to upset directing operations. An extensive number of assaults on MANET are known and numerous arrangements have been proposed to oppose them.

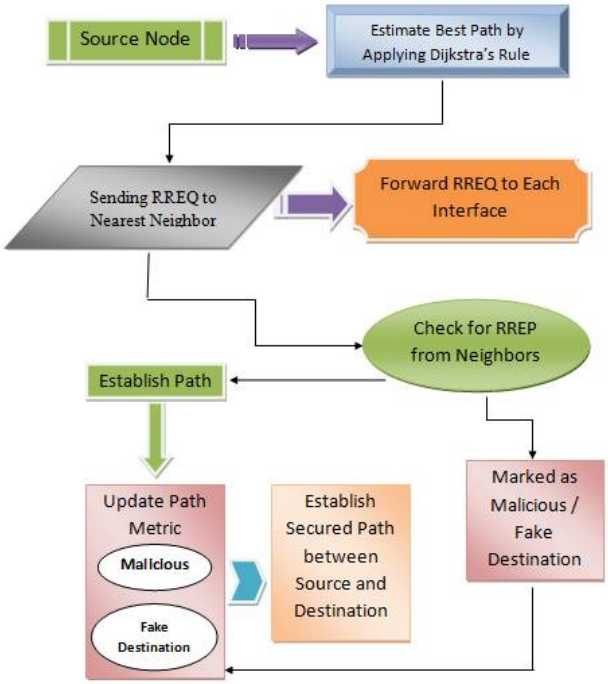


**Fig.1. System Architecture Design**

Reproduction contemplates have demonstrated the effect of such assaults and the viability of proposed resistance systems. Security instruments can be added to existing directing conventions to oppose assaults. Cryptographic systems are utilized to guarantee the genuineness and honesty of steering messages.

A noteworthy concern is the exchange off amongst security and execution, given the restricted assets accessible at numerous MANET hubs. Both symmetric and deviated cryptography have been utilized and in addition hash anchoring. Cases of these security upgraded conventions are Authenticated Routing for Ad-hoc Networks [ARAN], Secure Link State Routing Protocol [SLSP], and Secure Ad-hoc On-request Distance Vector Routing/steering [SAODV].

Notwithstanding the power and calculation cost of utilizing cryptographic systems, the execution of secured instrument is more awful than non-secured within the sight of a few assaults. Securing the steering messages does not ensure the identification of these vindictive hubs.

We present another Blackhole Resisting Mechanism [BRM] that can be utilized for all on-request steering conventions. Every hub in this component is in charge of observing the conduct of its neighbors to distinguish vindictive hubs and prohibit them. We fuse our proposed component into AODV for instance of its utilization with on-request directing conventions. This paper exhibits a critical change in execution when utilizing our instrument.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

**TABLE.1 INPUT PARAMETERS**

| Parameter | Value |
|---|---|
| Number of Nodes | 50-120 |
| Source Node and Destination Node | User Choice based on Selected Number of Nodes |
| Transmission Packet Size | 1000-2000 kBps |
| Packets Transmission Speed | 30-70 bps |
| Node Mobility Speed | 100-500 |
| Individual Node Strength | 100-200 J |

## II. EXISTING SYSTEM

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In blackhole attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination.

In grayhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. The malicious nodes are termed as Fictitious Nodes in this case and there is no alternative mechanisms to solve the routing issues and avoid the attack possibilities while communication.

## III. PROPOSED SYSTEM SUMMARIZATION

A detection protocol called the Blackhole Resisting Mechanism (BRM) is presented, which aims at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs via the effective identification and removal of Attacker Nodes in scenario. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique.

In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. Our cipher scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage. BRM is Dynamic Source Routing (DSR) based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the response message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply message or the malicious node reply forged ROUTE RESPONSE.

This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a blackhole attack. To resolve this issue, the function of HELLO message is added to the BRM to help each node in identifying which nodes are their adjacent nodes within one hop. This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program to detect the exact addresses of malicious nodes. The baiting request packets are similar to the original route request packets, except that their destination address is the bait address.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

**Proposed Algorithm**

***Step 1:*** Select nodes, F={$N_i$} where $N_i$ is within the range of source node toward the forward direction of destination.

***Step 2:*** For every $N_i$, calculate distance $d_k = \sqrt{(x_2 - x_1)^2 - (y_2 - y_1)^2}$ where $d_k$= distance between two forward nodes.

***Step 3:*** Calculate node speed $N_0$ = |Ss-Sk| Where Ss -> Speed of Source Node, Sk -> speed of Forward node

***Step 4:*** Compute Distance D = ($d_k$-Pi) + No; Where $d_k$=Distance;
Pi=Energy of node;
No=Speed node;

***Step 5:*** Select Min(C) from every $N_i$;

## IV. LITERATURE SURVEY

SAODV [18] is an enhancement of AODV routing protocol to fulfil security feature. The protocol operates mainly by appending an extension message to each AODV message. The extension messages include a digital signature of the AODV packet using the private key of the original sender of the routing message and a hash value of the hop count. SAODV uses asymmetric cryptography to authenticate all non-mutable fields of routing messages as well as hash chain to authenticate the hop count (the only mutable) field. Since all fields except the hop count of routing messages are non-mutable they can be authenticated by verifying the signature using the public key of the message originator. So, when a routing message is received by a node, the node verifies the signature of the received packet. If the signature is verified, the node computes the hash value of the hop count; if the routing message is RREQ or RREP; and compares it with the corresponding value in the SAODV extension. If they match, the routing message is valid and will be forwarded with an incremented hop count and a new hash value or if the destination has been reached generate the RREP.

S. Lee [7] proposed a solution that modified the AODV routing protocol by introducing two new packets; the route confirmation request (CREQ) and route confirmation reply (CREP). An intermediate node has to send CREQ to its nexthop node toward the destination node in addition to RREP to the source node. Upon receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has a route, it sends the CREP to the source. After receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are coordinated, the source node judges that the route is appropriate. One drawback of this method is that it cannot avoid the cooperative blackhole attack if two consecutive nodes work together as the first node asked its next hop node to send CREP to the source.

L. Tamilselvan [16] proposed a solution that designed upon a Fidelity Table in which each participating node is assigned with a fidelity level that determines the node reliability. A default fidelity level is assigned to each node and this level is updated based on the behavior of the node. When a source node receives RREP, it waits to receive further route replies from its neighboring nodes and then selects a neighbor node with a highest fidelity level to forward data to the destination node. A destination node acknowledges receiving the data by sending ACK. Updating the fidelity level of node relies on trusted participation of the node in the network. The source node increments or decrements the fidelity level of the forwarding node upon receiving or missing the ACK respectively. Node is eliminated from the network if its fidelity level reaches zero and marked as a malicious node. The main drawback of this solution is the high end-to-end delay specially when the malicious node is far away from the source node.

N. Mistry [8] introduced a solution that depends on analysing all received RREP. As source node receives first RREP, it waits MOS WAIT TIME seconds to receive multiple RREPs. During this time, the source node saves all the received RREPs in a table. Thereafter, the source node makes an analysis of all stored RREPs from the table, and rejects any having very high destination sequence number and considering its sender as malicious. The remaining entries in the table are arranged according to their destination sequence number and the node with the highest number is selected. This technique also records the identity of suspected malicious nodes to discard any upcoming control packets received and/or forwarded from/to that node and a routing entry for that node will not be maintained. The algorithm introduces high end-toend delay as nodes have to wait for multiple RREPs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

N. Choudhary [4] introduced a solution that based on sensing the wireless channel. This approach assigns a max trust value to all its neighboring nodes. A node will not do any further communication with a neighbor whose trust value is less than min trust value. When a source node receives a RREP message, it updates its routing table, starts transmitting the data packets and inserts a unique sequence number with each transmitted data packet. When a node forwards a data packet, it sets a timer and listens to the wireless channel in promiscuous mode to ensure that this packet is forwarded by a next hop neighbor. When the timer expires without hearing the retransmission of this packet, the node reduces the trust value for its next hop node. Trust value information is updated and disseminated to other neighboring nodes. If the trust value of a node decreases below min trust value, it will be isolated by all the nodes in the network.

## V. EXPERIMENTAL RESULTS

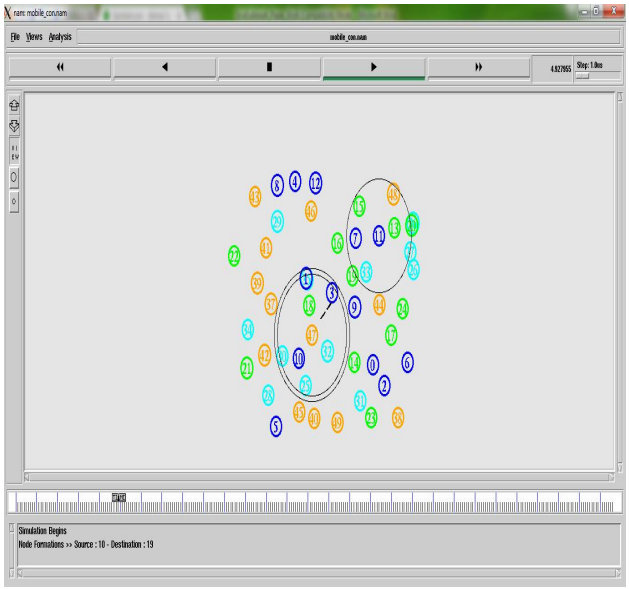


**Fig.2 Wireless Node Formation**

The above figure.2 illustrates the graphical simulation environment and the wireless node formation scenario.

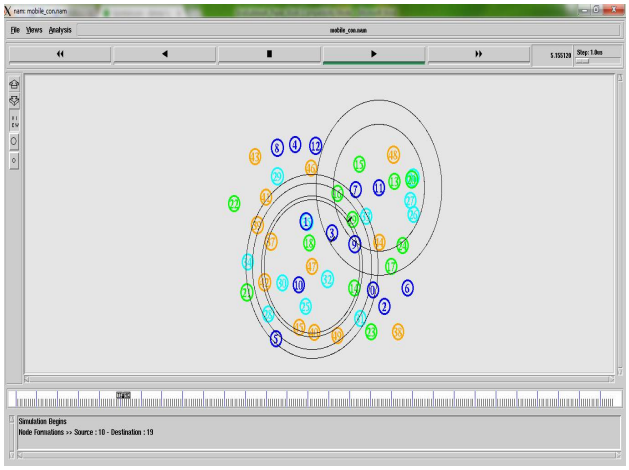


**Fig.3 Communication Process**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The above figure.3 illustrates the wireless node formation and communication procedures between source and destination.

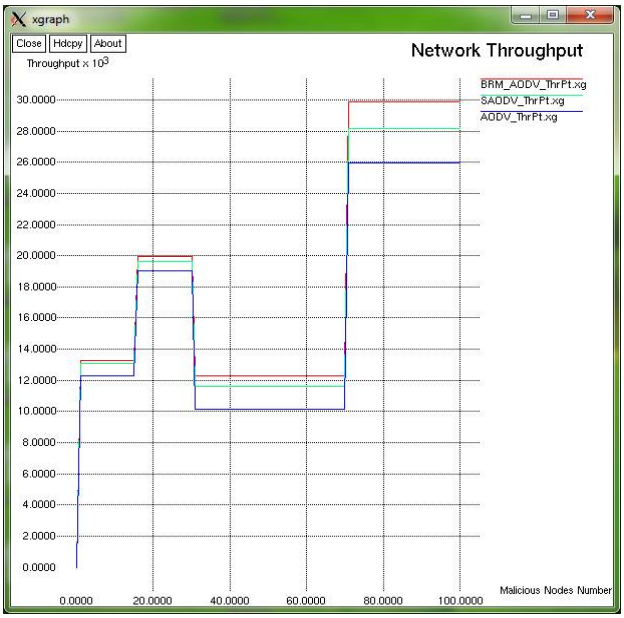


**Fig.4 Throughput Analysis**

The above figure.4 illustrates the analysis of throughput and its evaluations.

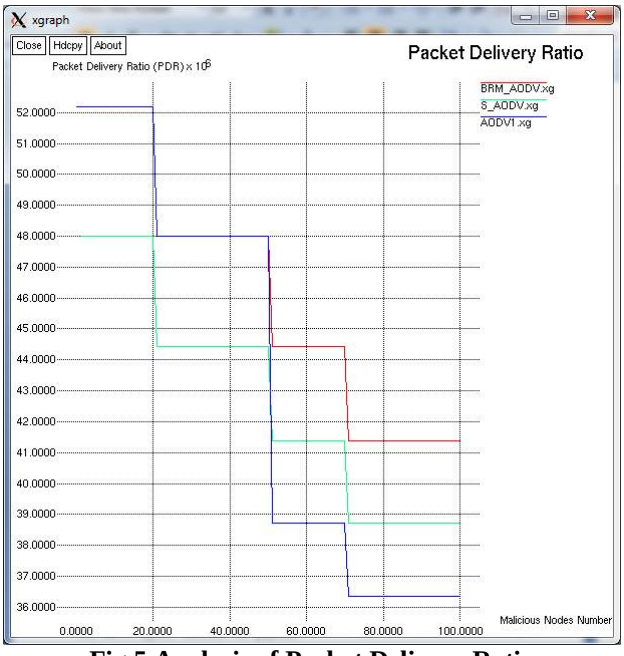


**Fig.5 Analysis of Packet Delivery Ratio**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The above figure.5 illustrates the analysis of PDR and its evaluations.


**Fig.6 Average End-to-End Delay**

The above figure.6 illustrates the analysis of end-to-end delay and its evaluations.

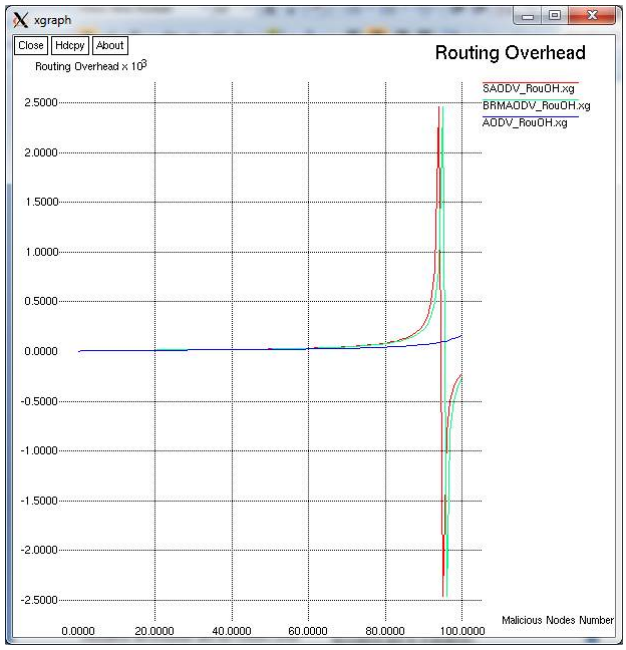


**Fig.7 Analysis of Routing Overhead Ratio**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The above figure.7 illustrates the Analysis of Routing Overhead between Source and Destination.

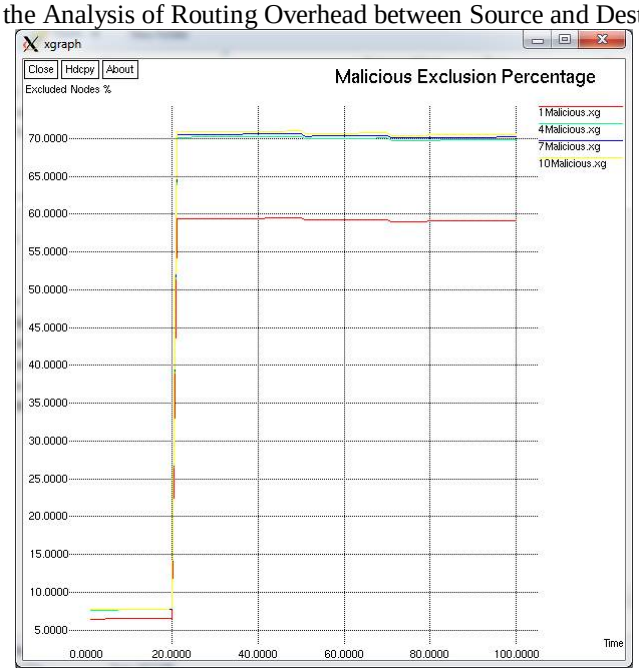


**Fig.8 Analysis of Malicious Exclusion Percentage**

The above figure.8 illustrates the Analysis of Malicious Exclusion Percentage.

## VI. CONCLUSION

The framework presented another idea of Self-Protocol Trustiness [SPT] in which identifying a vindictive gatecrasher is proficient by consenting to the ordinary convention conduct and drawing the malignant hub to give a verifiable admission of its noxious conduct. We presented another Blackhole Resisting Mechanism [BRM] that can be fused into any receptive directing convention in MANET. The proposed component did not utilize cryptographic procedures which preserves the power and calculation assets. Moreover, the component did not require any extra bundles and thus does not bring about any extra overhead. For instance, we joined our Blackhole Resisting Mechanism into AODV to concentrate the execution of the system under the nearness and nonattendance of the component. Recreation comes about demonstrated that BRM-AODV gives an enormous change of the system execution in all system measurements over both AODV and SAODV. The proposed instrument prevailing with regards to identifying blackhole hubs inside a brief timeframe in any case the quantity of malignant hubs and the time they are taking an interest in the system. Future work incorporates extending this thought to other responsive conventions, and affirming its general appropriateness.

## REFERENCES

[1] M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In 8th International Conference for Internet Technology and Secured Transactions (ICITST), pages 290–295, London, UK, Dec 2013.
[2] M. A. Abdelshafy and P. J. King. AODV & SAODV under attack: performance comparison. In ADHOC-NOW 2014, LNCS 8487, pages 318–331, Benidorm, Spain, Jun 2014.
[3] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. B¨ol¨oni, and D. Turgut. Routing protocols in ad hoc networks: a survey. Computer Networks, 55(13):3032–3080, September 2011.
[4] N. Choudhary and L. Tharani. Preventing black hole attack in AODV using timer-based detection mechanism. In International Conference on Signal Processing And Communication Engineering Systems (SPACES), pages 1–4, Jan 2015.
[5] P. Joshi. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3:954–960, 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

**Vol. 5, Issue 5, May 2017**

[6] A. Kumar. Security attacks in MANET - a review. IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011, RTMC(11), May 2012.
[7] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.
[8] N. Mistry, D. C. Jinwala, and M. Zaveri. Improving AODV protocol against blackhole attacks. In International MultiConference of Engineers and Computer Scientists (IMECS), pages 1–5, Hong Kong, China, March 2010.
[9] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.
[10] P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In Symposium on Applications and the Internet Workshops, pages 379–383. IEEE Computer Society, 2003.
[11] M. Patel and S. Sharma. Detection of malicious attack in MANET a behavioral approach. In IEEE 3rd International on Advance Computing Conference (IACC), pages 388–393, 2013.
[12] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, 1997.
[13] K. Sanzgiri and et al. Authenticated routing for ad hoc networks. IEEE Journal On Selected Areas In Communications, 23:598–610, 2005.
[14] N. Sharma and A. Sharma. The black-hole node attack in MANET. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, ACCT '12, pages 546–550, Washington, DC, USA, 2012. IEEE Computer Society.
[15] M. Singh, A. Singh, R. Tanwar, and R. Chauhan. Security attacks in mobile adhoc networks. IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011, RTMC(11), May 2012.