Navjot Int. Journal of Engineering Research and Applications www.ijera.com
ISSN : 2248-9622, Vol. 5, Issue 6, (Part - 5) June 2015, pp.131-137

RESEARCH ARTICLE OPEN ACCESS

To mitigate Black-hole attack with CBDS in MANET

Navjot * Er.Pooja Rani**
*(M.tech Student ,Department of CSE, Rayat & Bahra, Mohali Campus,Tehsil- Kharar, Punjab-140104,)
** (Associate Professor, Department of IT, Rayat & Bahra, Mohali Campus,Tehsil- Kharar, Punjab-140104)

Abstract-
Mobile ad-hoc network is self configured network that consist of mobile nodes which communicate with each other. Distributed self-organized nature of this network makes it venerable to various attacks likes DOS attack, Black hole attack, wormhole attack and jamming attack etc. Blackhole attack is one of the serious attack in network in which information loss occur which degrades the performance of network. In this work black hole attack is detected with the help of CBDS (cooperative Bait Detection Algorithm) and MD5 is used for the security purpose. This work is implemented in Network simulator and performance is checked on the bases of network parameters.
***Keywords*-**end to end delay, overhead, PDR, throughput

I. INTRODUCTION

Mobile ad hoc networks (MANETs) [12] have become important in increasingly large range of applications, such as battlefields and other military environments, disaster areas, and some other activities. A MANET is a multi-hop wireless network (without wire) that is formed dynamically from an accumulation of mobile nodes without the assistance of a center coordinator. As the radio propagation range is in limit, every mobile node has information in limit, such as its own ID and the Medium Access Control (MAC) address of its one-hop neighbors. Therefore, if two nodes are not in the radio propagation range, a multi-hop, via one or more intermediate nodes, is needed to forward packets. With recent invention in wireless technology, portable computing platforms and small wireless devices become indispensable devices [6]. The use of a portable device is constrained by its energy, making power conservation the most critical issue for portable devices and their uses. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on above of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute). MANETs circa 2000-2015 typically communicate at radio frequencies.

1.1 Mobile Ad Hoc Network

MANETs is called Mobile Ad hoc Networks. Mobile implies “mobility”. Ad hoc is a Latin word that means “for this only”. MANET is an autonomous collection of mobile nodes that communicate over wireless links [4].

MANET is a minimum IP based system of mobile and wireless machine nodes associated with radio. In operation, the nodes of a MANET don't have a concentrated organization mechanism. It is known for its route network properties where every node go about as a "router" to forward the movement to other indicated hub in the system.

MANET is a less remote system. The nodes moves haphazardly and sort out themselves discretionarily [10]. The nodes specifically correspond through remote connections with one another's radio reach, while that are far off separated utilization different nodes as hand-off, in a multi-jump steering capacity [3]. As the nodes are mobile, the structure of the system changes alertly and dynamically over the long run. Ad-hoc networks are self-designing and self-sorting out, so to keep up communication between nodes in the system, every node carries on as a source; begin point, a host and a switch.

"A mobile Ad-Hoc system (MANET) is a self-arranging system of mobile routers (and related hosts) associated by wireless links." [4].

Some of the principle components of MANET are as follows [3]:

a) MANET can be framed with no previous framework.

b) It deal with element topology where nodes may join and leave the system whenever with their own decision and the multi-jump directing may continue changing as nodes join and withdraw from the system.

c) It has extremely constrained physical security, and accordingly expanding security is a noteworthy concern.

d) Every node in the MANET can help with directing of parcels in the system.

e) Both Bandwidth & Power in cutoff

1.2 Types of MANET

• Vehicular Ad hoc Networks (VANETs) are utilized likewise as a part of correspondence. Communication among vehicles and in the middle of vehicles and roadside equipment. Intelligent vehicular Ad-Hoc systems (In VANETs) are a sort of computerized reasoning that helps vehicles to carry on in intelligent manner during vehicle to vehicle collision, accidents, drunken driving with telephone calls [7].

• Internet based versatile specially appointed systems (I MANETs) are Ad-Hoc systems that connect portable nodes [8]. Fixed internet gateway nodes. For instance, different sub-MANETs may be connected by a classic Hub-Spoke VPN to make a topographically conveyed MANET. In such kind of systems ordinary specially appointed directing calculations don't make a difference specifically.

• Military MANETs are utilized by military units with accentuation on security, reach, and incorporation with existing frameworks. Regular waveforms incorporate the US, Persistent Systems' Wave Relay, and Trellis product's TSM [2].

1.3 Characteristics of MANETs

• Dynamic topologies: Nodes are allowed to move arbitrarily; along these lines, the system topology- -which is ordinarily multichip- -may change arbitrarily and quickly at unpredictable times, and may comprise of both bidirectional, unidirectional connections [8].

• Bandwidth-constrained, variable capacity links: Wireless connections will keep on having essentially lower limit than their hardwired counterparts. Moreover, the acknowledged throughput of wireless communication subsequent to representing the impacts of multiple access, fading, noise, and interference condition, and so forth., is often much less than radio maximum condition [10].

• Energy-constrained operation: Some or the greater part of the nodes in a MANET may depend on batteries or other exaustable means for their energy [11]. The most essential system design criteria for streamlining may be energy preservation.

• Limited physical security: Mobile wireless networks are by and large more inclined to physical security dangers than are fixed cable nets. The expanded possibility of eavesdropping, pooling, and denial of attacks ought to be carefully considered. Existing connection security procedures are regularly connected inside of remote systems to lessen security dangers [14]. As an advantage, the decentralized way of system control in MANETs gives extra strength against the single purposes of disappointment of more unified.

1.4 MANET Challenges

A MANET [6] environment needs to overcome certain issues of constraint and limitations. It comprises of taking after:

• The qualities of remote connection are time-varying in nature - There are transmission obstruction like path loss, blockage and interference that adds to the suspect able behavior of remote channels. The reliability of remote transmission is opposed by diverse elements [12].

• Limited scope of remote transmission - The limited radio band brings about reduces information rates compared with the remote systems. Subsequently best use of bandwidth capacity is essential by keeping low overhead as could reasonably be expected.

• Packet loss because of error in transmission - MANETs experience higher packet loss because of variables, for example, hidden terminals that outcomes in crashes, remote channel issues (high bit lapse rate (BER)), obstruction, and successive breakage in ways brought on by versatility of nodes, expanded impacts because of the presence of hidden terminals and uni-directional connections [15].

1.5 Applications of MANET

• The technology of Mobile Ad hoc Networking is fairly synonymous with Mobile Packet Radio Networking Mobile Mesh Networking (a term that showed up in an article in The Economist in regards to the structure of future military systems) and Mobile, Multi-jump n/w, Wireless Networking (maybe the most exact term, in spite of the fact that somewhat unwieldy). There is present and future requirement for dynamic ad hoc network technology. The rising field of mobile and nomadic computing, with its present emphasis on versatile IP operation, ought to progressively

increase and require very highly adaptive mobile networking technology [12]

• Effectively managed multichip, Ad-Hoc network cluster which can work autonomously or [13], more than likely, be appended sooner or later to fixed Internet.

• Some uses of MANET technology could incorporate modern and business applications including cooperative versatile information trade. Mobile base network can be fill in as strong, cheap choices or improvements to cell-based versatile system frameworks. There are likewise existing and future military network requirement for robhust for hearty, IP-consistent information benefits inside of portable remote correspondence systems; a number of these systems comprise of profoundly element or we can say haphazardly self-sufficient topology portions. Likewise, the creating innovations of "wearable" figuring and correspondences may give applications to MANET technology [16].

• In flame/safety operations or different situations obliging quickly deployable correspondences with survivable, proficient element organizing [12]. There are likely different applications for MANET innovation which are not right away acknowledged or imagined by the creators. It is, basically, enhanced IP-based systems administration innovation for element.

2. Dark gap assault

MANETs face diverse securities dangers

The initially proposed arrangement here for dark black hole is to discover more and more course to the destination (excess courses, no less than three distinct courses). At that point, the source node uni-cast a ping packet to the destination utilizing these three courses (we ought to allocate distinctive parcel IDs and grouping number, so any node who get the first parcel will not drop the second one just in one condition in the event that it exists in both ways). The receiver and the malicious in addition any transitional node may have a course to the destination will answer to this ping solicitation. The source will check those acknowledgements, and process them with a specific end goal to make sense of which one is not sheltered and may have malicious node.

The second proposed solution exploits the packet sequence number included in any packet header. The node in this situation needs to have two extra tables; the first table consists of the sequence numbers of the last packet sent to the every node in the network, and the second table for the sequence number received from every sender. During the RREP phase, the intermediate or the last node must include the sequence number of last packet received from the source that initiates RREQ. Once the source receives this RREP, it will extract the last sequence number and then compare it with the values in the table. If it matches the transmission will take place. If not, this replied node is a malicious node, so an alarm text will be broadcast as a warring the network about this node.
These assaults are sorted as:-

2.1 Black Hole Attack: one malicious node uses directing convention to claim itself of being briefest way to last node yet drops steering bundles and doesn't send parcels to its neighbors [17].

1.6 Internal Black Hole Attack

Internal black hole attack is that when internal node act as a attacker. This is also called active attack. Internal attack is that when the internal node is doing misbehaving, such as not using proper bandwidth or proper processing Capability also the misbehaving node tells the entire node that it will be a shortest path to reach the destination. The internal malicious node also changes the data when it sends from first node to last node [12]. in This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node

1.7 External Black Hole Attack

It is also called passive attack. It stays outside the network, but disturbs the network by creating n/w congestion and wants a control over the internal node of the network by sending a RREQ to the source that it's a shortest path to reach in the last node and carry data from the source. [6]
External attackers physically stay outside of the system and deny access to network movement or making blockage in system or by upsetting the whole system.

1. Malicious nodedistinguishes the active route and recalls the destination address.

2. Malicious node sends a course answer bundle (RREP) including the destination location field satirizes to an obscure destination address [17].

Hope count value is situated to lowest value qualities and the sequence value is set to be the highest.

3. Malicious node sends RREP to the nearest nodes which have a place with the active route. This can likewise be send straightforwardly to the information source node if course is accessible.

4. The RREP received by the nearest node to the malicious node will transferred by means of the set up inverse route to the information of source hub.

5. The new data got in the course answer will permit the source hub to upgrade its steering table.

6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route

1.8 Black hole Attacks are classified into two categories

1.8.1 Single Black Hole Attack

In Single Black hole Attack in which one node acts as attacker. It is also known as Black Hole Attack .it has single malicious nodes.

1.8.2 Collaborating Hole Attack

In Collaborative Black Hole Attack more than one nodes act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes According to the original AODV protocol, when first node S wants to communicate with the last node D, the first node S shows the course ask for (RREQ) parcel [4]. The neighboring dynamic nodes overhaul their directing table with a section for the source hub S, and check in the event that it is the last hub or has a sufficiently crisp course to the destination hub. If not, the transitional hub redesigns the RREQ (expanding the jump tally) and surges the system with the RREQ to the last hub D until it achieves hub D or some other middle hub which has a sufficiently new course to D, as delineated by illustration in Figure 1. The last hub D or the middle of the road hub with a sufficiently new course to D, starts a course reaction (RREP) in the opposite bearing, as portrayed. Hub S begins sending information parcels to the neighboring hub which reacted in the first place, and tosses alternate reactions. This works is fine when the system has no noxious nodes. Specialists have proposed answers for recognize and evacuate a solitary dark gap hub. Be that as it may, the instance of numerous dark opening nodes acting in coordination has not been tended to [17]. Case in point, when numerous dark opening nodes are acting in a joint effort with one another, the first dark gap hub B1 alludes to one of its buddies B2 as the following bounce. As per [3], the source hub S sends a "Further Request (FRq)" to B2 through an alternate course (S-2-4-B2) other than by means of B1. Hub S inquires as to whether it has a course to hub B1 and a course to last hub D. Since B2 is chipping in with B1, its "Further Reply (FRp)" will be "yes" to both the inquiries. Presently per the arrangement proposed in [3], nodes begins passing the information parcels expecting that the course S-B1-B2 is more secure. In any case, in actuality, the bundles are devoured by hub B1 and the security of the system is bargained.

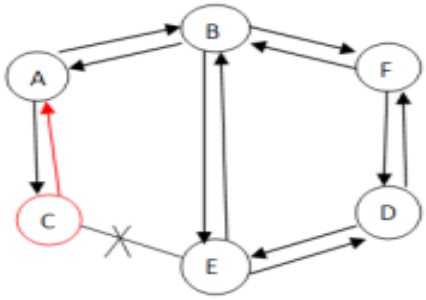
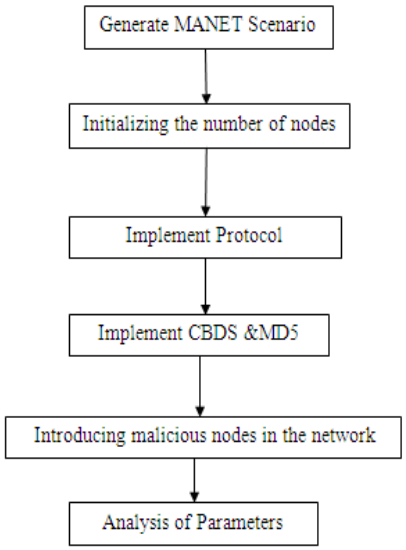


Figure 1: Black hole attack

1.9 Flow of Work



II. ALGORITHMIC STEPS

Step 1. Generate wireless scenario
Step 2. Initialize n number of nodes
Step 3. Apply CBDS
a) Send RREQ
b) If (RREQ = true)
{System working fine}
Else if (time of reply > threshold)

{End process}
Else
{Send RREQ again}
End if
End if
If (PDR< certain threshold)
{Send Bait RREQ}
Else
{End process}
End if
If (RREP == true)
{Check union}
Else
{End process}
End if
Step 4. Apply MD5
a) Append padding bits
b) Append Length
c) Initiate MD buffer
d) Process message in 16-word blocks
e) Output

III. RESULT AND DISCUSSION

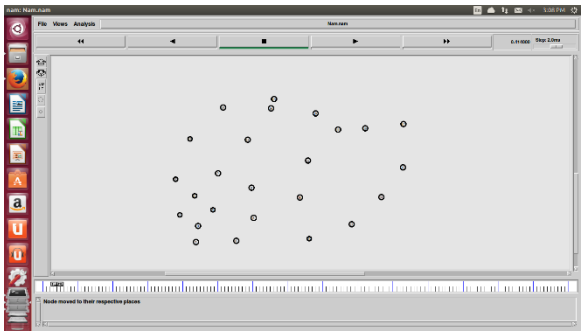


Fig. 2 Representation of nodes
In this scenario the nodes take their respective positions.

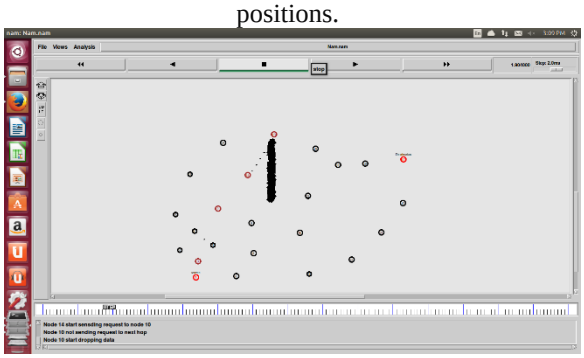


Fig 3. Representation of attacker

In this figure source and destination are defined. Node 14 starts sending the request to node 10. Node 10 is not sending request to next hop and hence, node 10 starts dropping data.

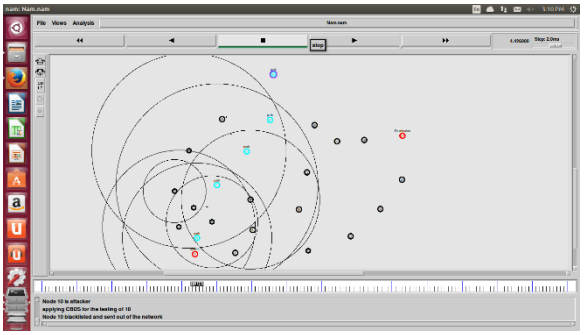


Fig. 4 Applying CBDS

In this scenario it is found that node 10 is attacker. CBDS is applied for testing of node 10. Node 10 is blacklisted and sent out of the network.

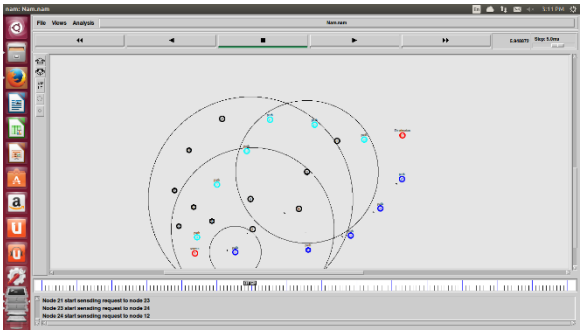


Fig. 5 Representation of new path selected
Figure 5 represents the new path that is selected after discarding the attacker.

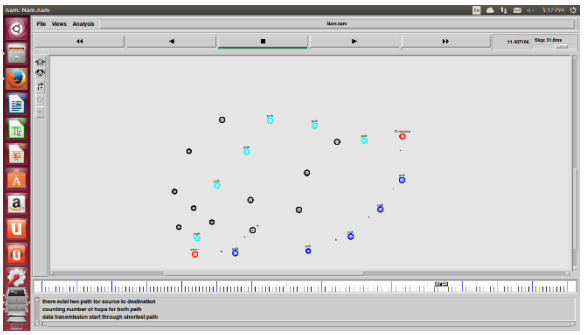


Fig. 6 representing two paths

Figure 6 represents two paths for source to destination. This will count number of hops for both the paths. But data transmission starts through shortest path.

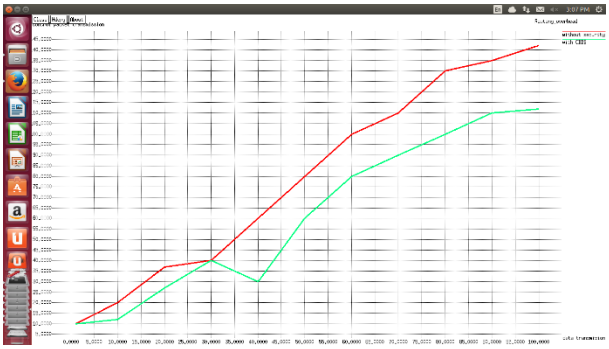


Fig. 7Representing overhead

This graph represents routing overhead. Green line represents routing overhead with CBDS and without CBDS.

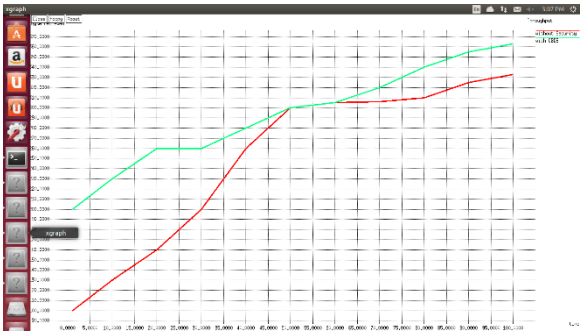


Fig 8 Represents throughput

Throughput is total number of successful bites received. This graph represents throughput.

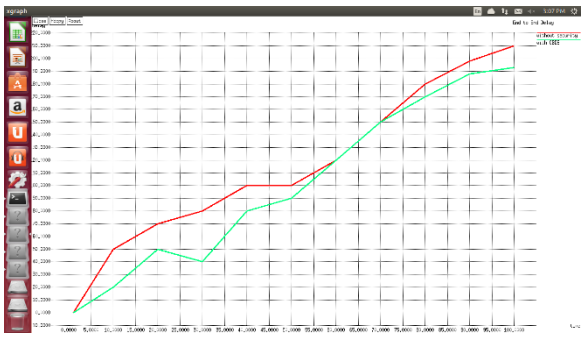


Fig. 9 Represents end to end delay

This figure represents end to end delay of nodes. With CBDS delay is lesser as compared to without CBDS hence, Afterapplying CBDS result are better.

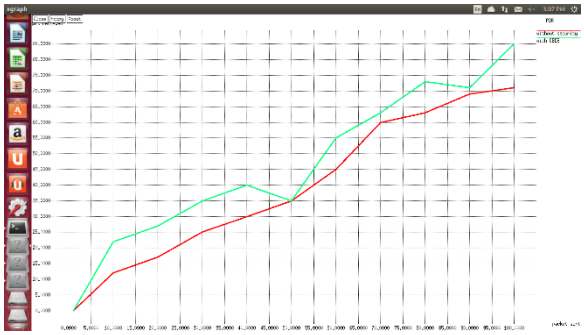


Fig .10 Represents PDR

This figure represents PDR (Packet delivery ratio). PDR with CBDS is good as compared to Without CBDS.

IV. CONCLUSION

In this work blackhole attack is mitigated with the help of cooperative bait detection scheme and message digest 5. MD5 is used for the security of messages. This research is concluded on the bases of quality of service parameters like throughput, packet delivery ratio, delay and overhead. It is examine that parameters give better result with CBDS and MD5 scheme rather than other simple blackhole approaches. In future this can also be dined using some artificial intelligent technique and its security can be enhanced by using cryptography.

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing" In *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Vol. 3, pp. 90–100, Feb. 1999.

[2] DanaiChasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET" in *Military Communications Conference, 2009. MILCOM 2009. IEEE* Vol.2, Issue 2, pp. 1-6.

[3] H. Tian and H. Shen, "Multicast-based inference of network-internal loss performance," in *Proc. of 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN 2004)*, Hong Kong, China, Vol.6 pp. 288–293.

[4] Kartik Kumar Srivastava, AvinashTripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" in *International journal Computer Technology & Applications Dec 2003,Vol.3, Issue 6*, pp. 1915-1921.

[5] N. G. Duffield and F. Lo Presti, "Network tomography from measured end-to-end delay covariance" in *IEEE/ACM Transactions on Networking, Dec. 2004, Vol.12, Issue 6*, pp. 978–992.

[6] Dutta, C.B "A novel black hole attack for multipath AODV and its mitigation", *IEEE conf. on Recent Advances and Innovations in Engineering*, May 2014, 1 – 6.

[7] Vicomsoft, "Knowledge share whitepapers wireless networking Q&A", Vicomsoft connect and protect, Jan 2003.

[8] Wikipedia, "The free encyclopedia-, Mobile ad-hoc Network", http://en.wikipedia.org/wiki/Mobile_ad-hoc_ network, Oct-2004.

[9] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug-1998.
[10] HumayunBakht, "Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks", http://www.computingunplugged.com/issues/ issue200410/00001395001.html, April-2003.
[11] Loutfi, Valerie, Bruno. "Securing mobile adhoc networks", MP71 project, 2003.
[12] Mario Joa-Ng, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks", IEEE Journal on selected areas in communications, Vol. 17, No. 8, Aug-1999.
[13] PadminiMisra, "Routing Protocols for ad hoc mobile wireless Networks", http://www.cse.ohio-state.edu /~jain/cis788-99/ftp/adhoc_routing/#TDRP, Nov-1999.
[14] Avdesh Kumar Bhatt, ChanderMohini and Shikha Thakur, " A New Efficient and Reliable On-Demand Routing Protocol for MANET (ERORPM)" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 5, May 2013.
[15] Anju Gill and ChanderDiwaker, "Comparative Analysis of Routing in MANET" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 7, July 2012.
[16] Rakesh Kumar, ManojMisra, and Anil K. Sarje, "A Simplified Analytical Model for End-To-End Delay Analysis in MANET" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.
[17] TamilSelvan, L., Chennai ; Sankaranarayanan, V.," Prevention of Blackhole Attack in MANET ",Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference, pp-21-24.