IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. V (Jan. 2014), PP 56-62
www.iosrjournals.org

An Efficient Approach for Prevention of Cooperative Black Hole Attack on DSR Protocol

Sunil Kumar Yadav[1], Shiv Om Tiwari[2]
[1](Computer Engineering, Siddhant College of Engineering/ University of Pune, India)
[2](Electronics and Telecommunication, Siddhant College of Engineering/ University of Pune, India)

Abstract : *In the mobile ad hoc networks, the major role is played by the routing protocols in order to route the data from one mobile node to another mobile node with security. But in such mobile networks, routing protocols are vulnerable to various kinds of security attacks such as blackhole node attacks. The routing protocols of MANET are unprotected and hence resulted into the network with the malicious mobile nodes in the network. These malicious nodes in the network are basically acts as attacks in the network. In this paper, we are considering the one such attack on mobile ad hoc network called blackhole attack. We proposed methods to detect and prevent cooperative blackhole attack in the MANET. We modify the existing DSR protocol to adopt the proposed cooperative algorithm of blackhole attack detection as well as prevention without the affecting overall performance of the network. Mobile nodes in the mobile ad hoc networks are acts host node and router node means nodes in the MANET are responsible for both data forwarding and routing mechanisms. But because of few malicious nodes which acts as misbehaving & selfish nodes, data packets not delivered to the destination and dropped by such nodes. We investigating the performance of existing DSR protocol with this new modified security enabled DSR protocol using the performance metrics like throughput, delay and jitter. Simulations for this work are carried out over the NS2 simulator.*

Keywords: *Ad Hoc Networks, Black Hole Attack, DSR, Routing Protocols, Security*

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. The communication among these mobile nodes depend upon the kind of routing mechanism used called multihop routing protocols. These routing protocols are responsible for building the communication routes as well as wireless communication network. Mobile Ad hoc networks having different types routing protocol like reactive, proactive and hybrid. These protocols are used in different scenario and mobility pattern. The reactive protocol such as DSR and AODV protocols are frequently used MANET protocols. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies**.** Most of the routing protocols for MANETs are thus vulnerable to various types of attacks. In this work we consider Dynamic Source Routing (DSR) protocol which is venerable to well known Black hole attack. This attack becomes more sever when a group of malicious nodes cooperate with each other. In case of Black hole node attack, the malicious node falsely advertises itself as a valid route to a destination node during the route discovery process with the intention of intercepting packets. Thus for proposed approach, we are basically carrying our investigation over the mechanism of Black hole node detection and their avoidance while keeping the performance of routing protocol. For the investigation purpose in this work, we are using the DSR (Dynamic Source Routing) protocol. The proposed algorithm is based on the concept of cooperative Black hole attack detection and prevention. The rest of the paper is organized as follows. Section II discusses some related work in security mechanism in routing for MANETs. Section III gives an overview of DSR protocol and the cooperative black hole attack. Section IV describes the proposed approach and the associated algorithm. Section V presents the important results obtained in simulation. Section VI concludes the paper and some future scope of work.

II. RELATED WORKS

A number of protocols were proposed to solve the black hole problem which require a source node initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination. Sun B. et al. [1], used AODV as their routing protocol, the detection scheme used neighbourhood-based method to detect the black hole attack. Shurman et al. [2], proposed two techniques to prevent the black hole attack in the MANETs. Djenouri D et al. [4], proposed a solution to monitor, detect and remove the black hole attack in Manets. The aim of this approach is to consider and avoid false accusation attacks vulnerability, as well as decreasing false positives that might be caused by channel conditions and nodes mobility. Hesiri Weera singhe et al. [5] proposed an algorithm to identify Collaborative black hole attack. In this

paper the AODV routing protocol is slightly modified by adding an additional table i.e. Data routing information (DRI) table and cross checking using further request (freq) and further reply (FREP). If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (route request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination.

III. DSR AND MANET SECURITY PROBLEMS

(A) DSR Overview

The MANET reactive protocol is known as the Dynamic Source Routing protocol (DSR) which is efficient and very simple one. It is designed in the multi-hope MANET of number of mobile nodes. DSR are known as the on demand routing protocol that means the routes are build only it is required for communication in the network. It becomes the self configuring and self organizing network without infrastructure network support. This is possible only using the DSR routing protocol. In the network mobile node acts as the both host as well as router in the network and to make the communication between the source and destination node it forward the packet over the multi-hope network within the range of wireless network nodes. The DSR protocol dynamically handles the routing mechanism. Especially, if any node leaves the network, joins or breakage link because of the network conditions. Other routes are also detected by DSR protocol automatically in such same cases. Because of the changing in the mobility rapidly in the network, an intermediate node sequence hop which is necessary to communicate with the destination may be changes according to the changes in the mobility. This is resulted into the network topology change frequently. The DSR is contain the two routing mechanism which is working together to make the data transmission from the source to destinations. This mechanism is known as the route discovery and route maintenance.

(i) Discovery of Route

The rout which is discovered for transmission of the data from source to destination is maintained by the DSR mechanism. By using this mechanism the source node detect whether the current route from source to destination is working properly or not, this is because of the topology changes route become invalid. That means they are not longer to work source to destination. The source node attempt to use another route which knows the destination node address when the route maintenance procedure shows that link is broken, otherwise again fires the route discovery procedure to find out the new route from the source to destination. When the actual data transmission procedure is going on then and then only route maintenance process activated. Maintenance and discovery for route mainly working for demand fashion only. The DSR protocol not requires the periodic packet at any level as compared to the other protocol of the MANET. That means the DSR protocol not uses any advertising mechanism of routing or link sensing or detection of packet of neighbor and all doesn't depend on other protocols for any kinds of function. Mechanism is completely depending on behavior of the network demand and there no periodic activities that allow the packet overhead caused by the DSR to scale down to the zero case all the routes are stationary with each other. The route require for the communication are already discovered. DSR automatically scales to the routes which are in use currently when the node moves more and more and changing the communication pattern frequently. In the response to the route discovery mobile node may learn and cache the multiple routes to the destination which allows the rapid changes in the routing information. Because the mobile node with having many route from the source to destination can try another route which is cached in case if the current route failed. To avoid the overhead of route discovery in case of route fails cache the multiple routes.

For example, Figure 1 illustrates an example Route Discovery, in which a node **A** is attempting to discover a route to node **E**. To initiate the Route Discovery, **A** transmits a ROUTE REQUEST message as a single local broadcast packet, which is received by (approximately) all nodes currently within wireless transmission range of **A**. Each ROUTE REQUEST message identifies the initiator and target of the Route Discovery, and also contains a unique *request id*, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. This route record is initialized to an empty list by the initiator of the Route Discovery.

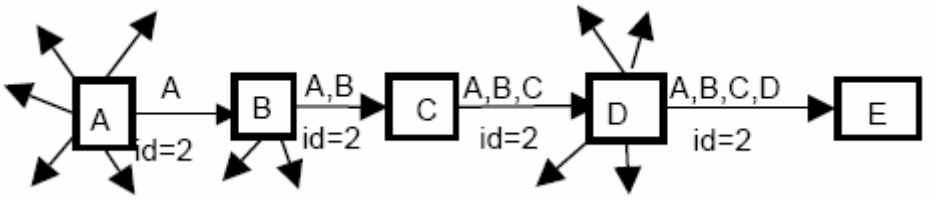

Figure 1: Node A is the initiator and Node E is the target

When the target node receives the ROUTE REQUEST message, it returns a ROUTE REPLY message to the ROUTE Discovery initiator with a copy of the accumulated route record from the ROUTE REQUEST. This route is cached in the Route Cache when the initiator receives the ROUTE REPLY and is used in sending subsequent packets to this destination. When the target node finds a ROUTE REQUEST message from the same initiator bearing the same request ID or if it finds its own address is already listed in the route record of the ROUTE REQUEST message, it discards the REQUEST. If the target node does not find the ROUTE REQUEST message from the initiator, then it appends its address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet. When Route Discovery is initiated the copy of the original packet is saved in a local buffer called Send Buffer. The packets are kept until a source route is available or a timeout or Send Buffer overflow occurs.

(ii) Route Maintenance

When a packet with a source route is forwarded, each node in the source route makes sure that the packet has been received by the next hop in the source route. The confirmation of receipt will be received only by re-transmitting the packet for a number of times. Node A is the originator of a packet to the desired destination E. The packet has a source route through intermediate nodes B, C and D. Node A is responsible for

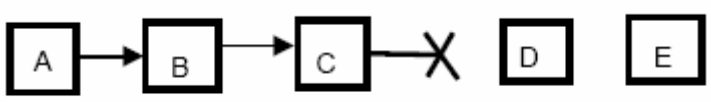

Figure 2: Node C is unable to forward a packet from A to E over the next node D

receipt of the packet at B, node B at C, node C at D and node D at E. Node B confirms receipt of packet at C by overhearing C transmit the packet to forward it to D. The confirmation of acknowledgement is done by passive acknowledgements or as link-layer mechanisms such as option in MAC protocol. When a node is unable to deliver a packet to the next node then the node sends a ROUTE ERROR message to the original sender of the packet. The broken link is then removed from the cache by the originator.

(B) Cooperative Black Hole Attack Problem

(i) Black Hole

A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets.

(ii) Cooperative Black Hole attack

According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 2. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neigh boring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.

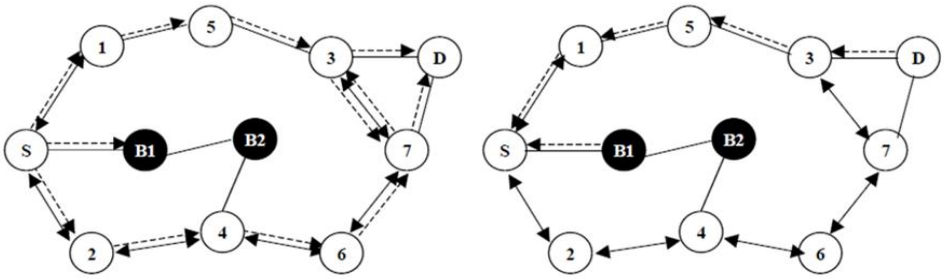

Fig.3 Network flooding of RREQ **Fig.4 Propagation of RREP messages**

IV. Proposed Approach & Design

In this section we proposed the new approach for blackhole prevention in DSR using the route cache mechanism of DSR based on cooperative behaviour. On the detection of blackhole node or misbehaving node, during the processing of path construction we have to get the blackhole node id and pass it to *add to path* function of DSR. In that function paths are ready to add in route cache, however priory to adding each path in route cache we are parsing those paths for the presence of blackhole node id. If the blackhole node is appears in path, we have to simply dump that path and add all rest of paths for the intended source destination pair communication. This process is making use of normal time of caching process only. Due this, delay is minimized as compared to previous blackhole detection mechanisms, packet dropped ratio is reduced drastically.

Algorithm: *Blackhole Attack Prevention*

```
Step1: Identify the blackhole nodes and prepare its list.
Step2: during path construction
Path = new Path ();
Count = 0;
Read the blackhole nodes list file nodes.info
While (nodes.info! = null)
Count++;
J++;
if (count>0)
 {
   for (int j=0;j <= count;j++)
  {
    if(addrs[i].addr != p[j])
     {
      cout<<"\t"<<p[j]<<":"<<"is a blackhole node detected, Now Apply Algoithm Making Secure Path"<<"\n";
   path[i] = ID(addrs[i]);
%% transfer function call to add_to_path function in mobilecache
 }
Step 3: During the add_to_path fuction
Int n= length (path)
While (n !=null)
routecache->trace[path];
if (routecache->net.id ==blackhole->net.id)
{
routecache->net_id.dump();
cache [index].dump ();
goto done;
}
else
Add current path to cache;
End.
```

Following figure shows the flowchart of this algorithm.

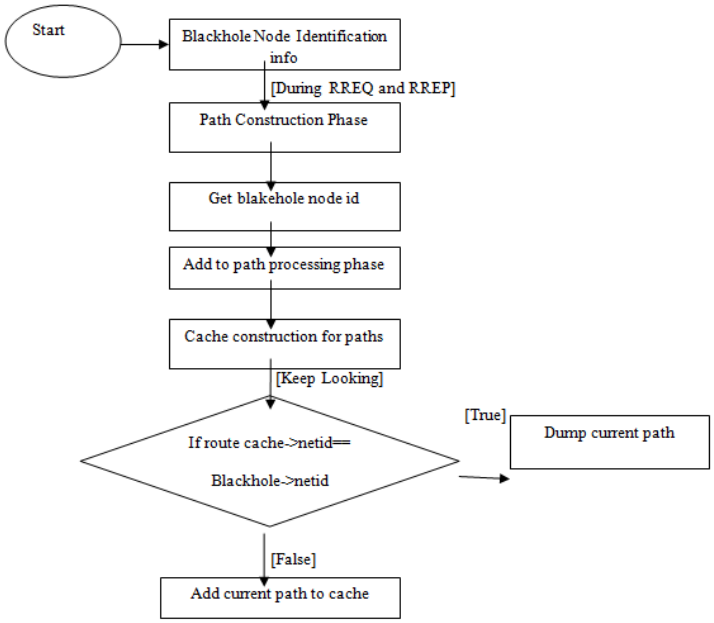

Fig. 5 Flow chart of Proposed Algorithm

V. SIMULATION

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator *ns-2*. Performances of the three protocols are evaluated: (i) Standard DSR protocol, (ii) DSR with malicious nodes cooperating in a blackhole attack (iii) DSR with the proposed algorithm. In this section we will present the three performance metrics for the proposed approach such as throughput, delay, jitter etc. The chosen parameters for simulation are presented in Table I.

Parameter	Value
Simulation time	600 sec.
Simulation area	600*600m
No. of mobile nodes	10/20/30
Routing protocols used	DSR/DSR(detection)/DSR(prevention)
Traffic type	CBR(UDP)
Number of malicious node	2 in case of 10 nodes 4 in case of 20 nodes 6 in case of 30 nodes
Host pause time	10 sec

Table: I Simulation parameters

Below in this section, various results are conducted and according to the performance comparison is carried out. **Throughput:** This metrics calculates the total number of packets delivered per second, means the total number of messages which are delivered per second.

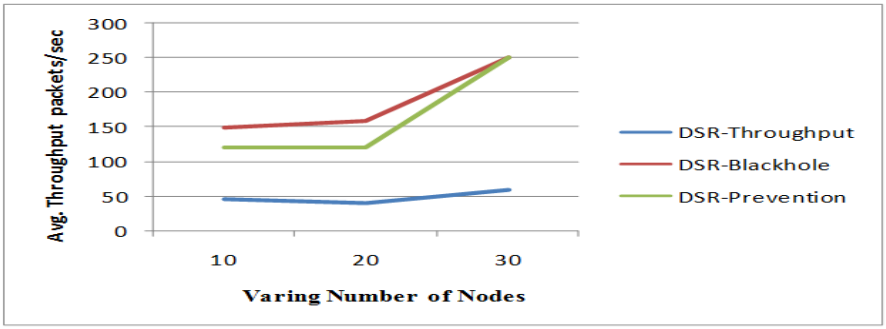

Fig. 6 Average Throughput (Packet/Sec)

Above graphs showing the performance of normal DSR, blackhole affected DSR and proposed blackhole prevention based DSR. From above graph, when the blackhole node introduced in DSR networks like 10, 20

and 30 nodes, unnecessarily fake packets received by network mobile nodes from attacker nodes and hence this increases the total number of packets sent and received in one second.

End to end packet delay: This metrics calculates the time between the packet origination time at the source and the packet reaching time at the destination. Here if any data packet is lost or dropped during the transmission, then it will not consider for the same. Below graph showing the performance of end to end delay, due to the blackhole prevention process the end to end delay performance of proposed approach is increases slightly as compared to normal DSR working. Same thing is reflecting in following jitter performance graph

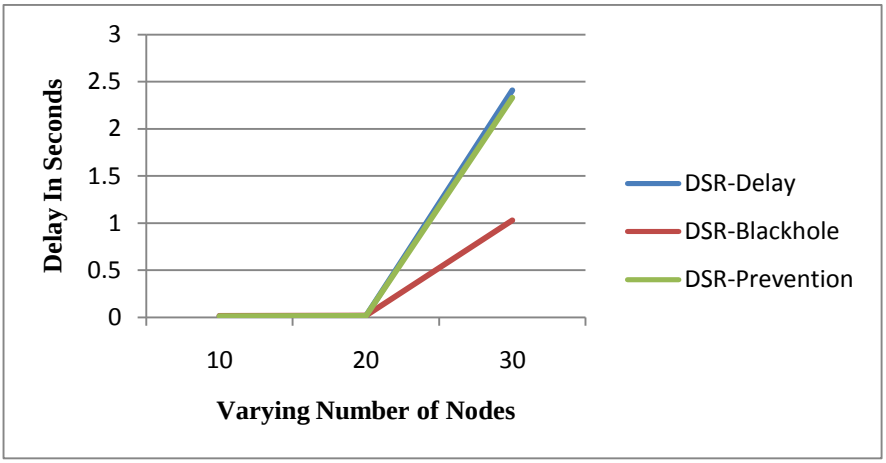

Fig.7 Delay in Seconds

Jitter: jitter refers to the variation in the packet in the packet arrival time. It is uneven delay in the delivery of audio or video packets.

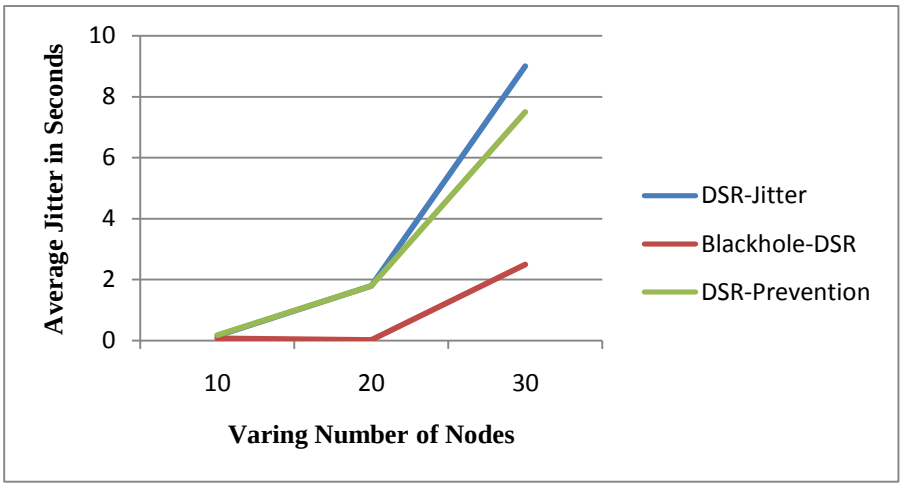

Fig. 8 Average Jitter in Seconds

Packet Dropped Ratio: This is the first and most important performance parameter which we have checked against the normal DSR, DSR in presence of blackhole attack and new proposed modified DSR to prevent blackhole attacks. Following graph is showing the performance of PDR with three network scenarios such as 10, 20 and 30 nodes.

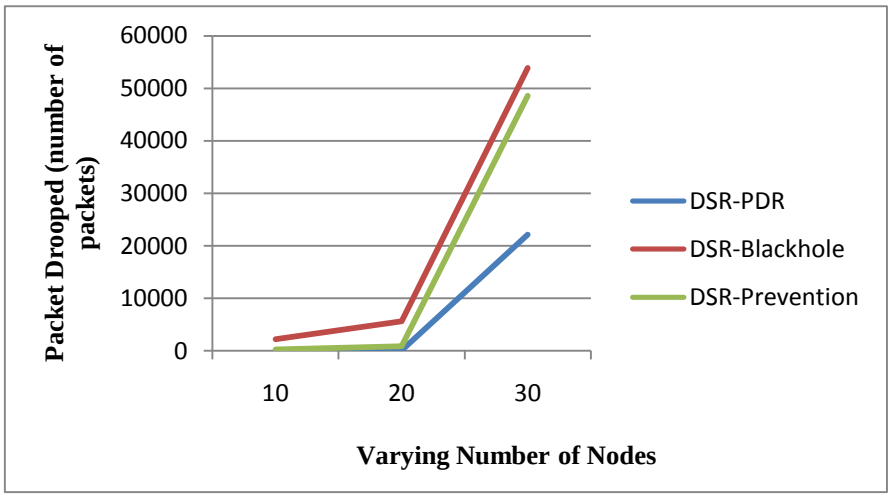

Fig. 9 Packet Dropped (Number of Packets)

From above graph, it's obvious that at the presence of blackhole attack in network makes the extra packet drops as compared to normal working of DSR. Hence to reduce such packet drops in the network, we have introduced the new approach to mitigate the blackhole attack from the MANET.

VI. CONCLUSION

In this paper, routing security issues in MANETs are discussed in general, and in particular the cooperative blackhole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple blackhole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the blackhole nodes. From results, this approach reduced the effect of blackhole attack in the MANET. As a future scope of work, the proposed security mechanism may be extended other type of attack such as Worm hole; jellyfish are needed to be studied in comparison with blackhole node.

REFERENCES

[1] Sun B, Guan Y, Chen J, "Detecting Black Hole Attack in Mobile Ad Hoc Networks", 5th *European Personal Mobile Communications Conference* Glasgow, United Kingdom, 22-25 April 2003.

[2] Al –Shurman M, Yoo S-M, Parks S, "Black Hole Attack in Mobile Ad Hoc Networks", 42nd *Annual ACM Southest Regional Conference (ACM-SE' 42)*, Huntsville, Alabama, 2-3 April 2004.

[3] Tamilselvan, L. and Sankaranarayanan, V., "Prevention of Blackhole attack in MANET", *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*. Aus Wireless, 21-21, 2007.

[4] Djenouri D, Badache N, " Struggling Against Selfishness and Black Hole Attacks in MANETs", *Wireless Communication and Mobile Computing* Vol. 8 Issue 6, pp 689-704, August 2008.

[5] H.Weerasinghe H. Fu., "Preventing Cooperative Blackhole Attack in Mobile Ad Hoc Networks, Simulation, Implementation and Evaluation". *International Journal of Software Engineering and Its Application* vol.2, No.3, 2008.

[6] Chang Wu Yu, Wu T-K Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", *Emerging Technologies in Knowledge discovery and Data Mining*, Vol, 4819, Issue 3, 2007.

[7] Kozoma W, Lazos L, "REAct: Resource- Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits". *Second ACM Conference on Wireless Network Security*, 16-18 March 2009.

[8] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", *International journal of Computer Science* Issue, Vol, 2 pp 54-59, 2009.

[9] Wang W, Bhargava B, Linder man M, "Defending against Collaborative Packet Drop Attacks on MANETs", 2nd *International workshop on Dependable Network Computing and Mobile Systems*, 27 September 2009.

[10] Jaydeep Sen, Sripad Koikonda, Arjit Util, " A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Network", *Second International Conference on intelligent system, Modeling and Simulation*, IEEE 2011 .

[11] Tsou P-C Chang, "Developing a BDSR Scheme to Avoid Black hole Attack Based on Proactive and Reactive Architecture in MANETs" *13th International Conference on Advanced Communication technology*, Phonix Park Korea, 13-16 Feb 2011.

[12] A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols". IETF RFC4593. Status Informational, October 2006.

[13] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, *Springer* 2008.

[14] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector (DSDV) routing for mobile computers" in *ACM SIGCOMM Symposium on Communications*, architectures and Protocols, pp. 234–244,September 1994.

[15] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.