I. J. Computer Network and Information Security, **2012, 6, 49-55**
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.06.07

Preventive Aspect of Black Hole Attack in Mobile AD HOC Network

Kumar Roshan,Vimal Bibhu
Department of Computer Science & Engineering,
DIT School of Engineering, Plot -48A, Knowledge Park – III, Greater Noida, Uttar Pardesh, India
kmr.roshan1@gmail.com
vimalbibhu@gmail.com

Abstract — Mobile ad hoc network is infrastructure less type of network. In this paper we present the prevention mechanism for black hole in mobile ad hoc network. The routing algorithms are analyzed and discrete properties of routing protocols are defined. The discrete properties support in distributed routing efficiently. The protocol is distributed and not dependent upon the centralized controlling node. Important features of Ad hoc on demand vector routing (AODV) are inherited and new mechanism is combined with it to get the multipath routing protocol for Mobile ad hoc network (MANET) to prevent the black hole attack. When the routing path is discovered and entered into the routing table, the next step is taken by combined protocol to search the new path with certain time interval. The old entered path is refreshed into the routing table. The simulation is taken on 50 moving nodes in the area of 1000 x 1000 square meter and the maximum speed of nodes are 5m/sec. The result is calculated for throughput verses number of black hole nodes with pause time of 0 sec. to 40 sec., 120 sec. and 160 sec. when the threshold value is 1.0.

Index Terms — AODV – Ad Hoc On Demand Distance Vector Routing, MANET–Mobile Ad Hoc Network, DSDV,CBR -Constant bit Pattern, TCP – Transmission Control Protocol

I. INTRODUCTION

In the present era, the study of MANETs has gained a lot of interest of researchers due to the realization of the nomadic Computing A Mobile Ad hoc Network (MANET), as the name suggests, is a self-configuring network of wireless and hence mobile devices that constitute a network capable of dynamically changing topology. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV, Dynamic source routing (DSR) and Destination-sequenced distance-vector routing (DSDV). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack [1].

The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets [2][3]. In other terms, a malicious node uses the routing protocol to advertise as having the shortest path to nodes whose packets it wants to intercept. In the case of AODV protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised, if the reply from malicious node reaches to the requesting node before the reply from the actual node, a fake route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to form a denial-of-service attack. Another instance can be seen when considering a category of attacks called “The Black Hole Attacks”. Here, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

II. WORKING OF BLACK HOLE

Based on original AODV protocol, any intermediate node may respond to the RREQ message if it has fresh enough route, which is checked by the destination sequence number contained in the RREQ packet. In Figure 4 node 1 is source node where as node 4 is destination node. Source node broadcasts route request packet to find a route to destination node. Here node 3 acts as black hole. Node 3 also sends a route reply packet to the source node. But a route reply from node 3 reaches to source node before any other intermediate node. In this case source node sends the data packet to destination node through node 3. But as the property of black hole node that this node does not forward data packets further and dropped it. But source node is not aware of it and continues to send packet to the node 3. In this way the data, which has to be reached to the destination, fails to reach there. There is no way to find out such kind of attack. These nodes can be in large number in a single MANET, which makes the situation more critical is shown in figure 1 [5].

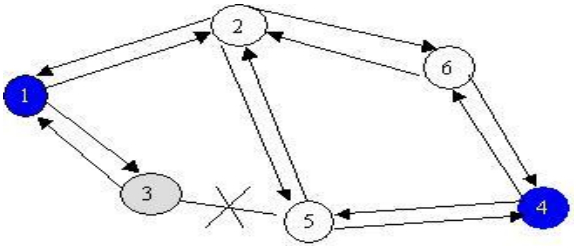

Figure 1: Black Hole Attack

III. ROUTING PROTOCOL IN MANET

Routing means how we can route a data packet from a source to a destination. In the case of MANET, a packet necessarily route several hops (multi hop) before reaches to the destination, a routing protocol is needed [6]. The routing protocol has two main functions, selection of routes for various source destination pair and delivery of the messages to their correct destination. Movement of nodes in MANET causes the nodes to move in and out of the range from one another, as a result there is continuous making and breaking of links in the network. Since the network relies on multi-hop transmissions for communication, this imposes major challenges for the network layer to determine the multi-hop route over which the data packets can be transmitted between a given pair of source and destination nodes. Figure 5 shows how the movement of a single node (C) changes the network topology rendering the existing route between A and E (i.e. A-C-E) unusable [7]. The network needs to evaluate the changes in the topology caused by this movement and establish a new route from A to E (such as A-D-C-E) is shown is figure 2.

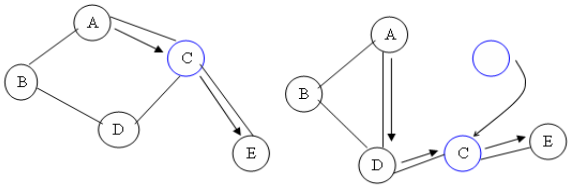

Figure 2: Path changes due to mobility of node

IV. DESIRABLE PROPERTIES OF ROUTING PROTOCOLS OF MANET

There are some desirable properties in routing protocol that are different from conventional routing protocol like link state and distance vector routing protocol

.

4.1 Distributed operation

The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the same case for stationary networks. The difference is that nodes in an ad-hoc network can enter/leave the network very easily and because of mobility the network can be partitioned [8].

4.2 Loop Free

To improve the overall performance, we want the routing protocol to guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.

4.3 Demand Based Operation

To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. This means that the protocol should only react when needed and that the protocol should not periodically broadcast control information.

4.4 Unidirectional Link Support

The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

4.5 Security

The radio environment is especially vulnerable to impersonation attacks, so to ensure the wanted behavior from the routing protocol; we need some sort of preventive security measures. Authentication and encryption is probably the way to go and the problem

here lies within distributing keys among the nodes in the ad-hoc network.

4.6 Power Conservation

The nodes in an ad-hoc network can be laptops and thin clients, such as PDAs that are very limited in battery power and therefore uses some sort of stand-by mode to save power. It is therefore important that the routing protocol has support for these sleep modes.

4.7 Multiple Routes

To reduce the number of reactions to topological changes and congestion multiple routes could be used. If one route has become invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure [9].

4.8 Quality Service Support

Some sort of Quality of Service support is probably necessary to incorporate into the routing protocol. This has a lot to do with what these networks will be used for. It is necessary to remember that the protocols are still under development and is probably extended with more functionality. The primary function is still to find a route to the destination, not to find the best/optimal/shortest-path route

V. AD HOC ON DEMAND VECTOR ROUTING

AODV shares DSR's on-demand characteristics in that it also discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination [10]. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers [11].

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves

5.1 Characteristics of AODV

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm deal with topology and routing information. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANET's [12]. AODV allows mobile nodes to responds to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and avoiding the "count-to-infinity" problem offers quick convergence when the ad hoc network topology changes. When link breaks, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.The metrics of a network on the basis of that we can check out the performance of a MANET, simulation parameter that will be used for generating the result of this new routing protocol, results and the analysis on the basis of these results.

VI. SIMULATION MODEL

The mobility simulations that have done in this paper used the node movement pattern of 50 nodes in the area of 1000x1000 square meter and maximum speed of nodes will be 5 m/sec. Also the traffic pattern of 50 nodes in which there will be maximum 5 connections with CBR (constant bit pattern) and different seed value have been used in the simulation. Seed value is used for generating the random traffic pattern. By changing only the seed value for generating the CBR or TCP connections, it changes the complete traffic pattern files. In another term, with different seed value, number of connection I same but timing of connections will change and also the placement of these connections will change.

Traffic generator [11] is located under ~ns/indep-utils/cmu-scen-gen/ and is called cbrgen.tcl and tcpgen.tcl. They may be used for generating CBR and TCP connections respectively.
To create CBR connections, run

```
ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed]
[-mc connections] [-rate rate] / <outdir>
```

The generator for creating node movement [11] files is to be found under ~ns/indep-utils/cmu-scen-gen/setdest/ directory. Compiles the files under setdest with argument in the following way.

```
./setdest –n <num_of_nodes> -p <pausetime> -s <maxspeed> -t <simtime> -x<maxx> -y <maxy / <outdir>
```

The general setting regarding simulation result for nodes are summarized in table 1.

Table 1. General Setting for Simulation Result

Communication Type	CBR
Number of Nodes	50
Maximum mobility speed of nodes	5 m/sec
Simulation Area	1000m x 1000 m
Simulation Time	200 sec
Packet Rate	4 packets/sec
Packet Size	512 bytes
Number of Connections	5
Transmission Range	250 m
Pause Times	0,40,120,160 sec
Number of malicious nodes	0, 3,5
Transmission Speed	10 Mbps

6.1 Throughput

It is the total number of received packet per unit time. In another term, throughput is the packet size (in term of bits) that is going to be transmitted divided by the time that is used to transmit these bits.

Throughput = Total No. of packet received / Total traversing time

6.2 End to End Delay

This is defined as the delay between the time at which the data packet was originated at the source and the time it reaches the destination.
Delay = Receiving time – Sending time

6.3 Packet Delivery Ratio (PDR)

The ratio between the number of packets received by the CBR sink at the final destination and the number of packets originated by the CBR sources.

PDR = Total No. of packet received / Total No. of packet sent.

VII. RESULT

First, results are calculated for throughput vs. number of black hole node with pause times 0 sec, 40 sec, 120 sec and 160 sec, when threshold value (th2 is 1.0). These line charts are shown below in figure 3,4,5,6,7,8,9 and 10.

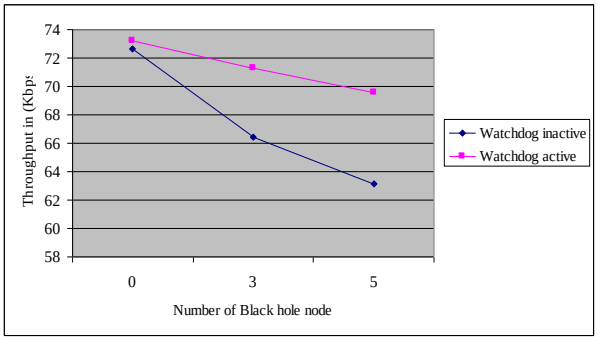

Figure 3: Throughput vs. Black hole nodes for 0 second pause time.

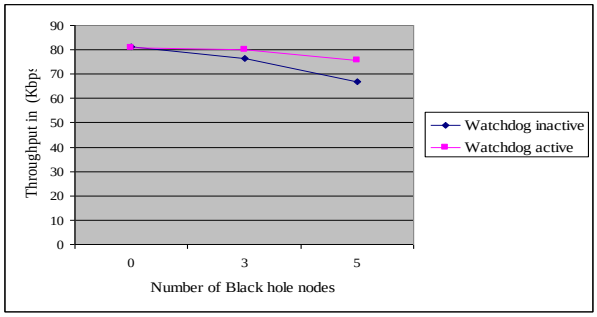

Figure 4: Throughput vs. Black hole nodes for 40 second pause time.

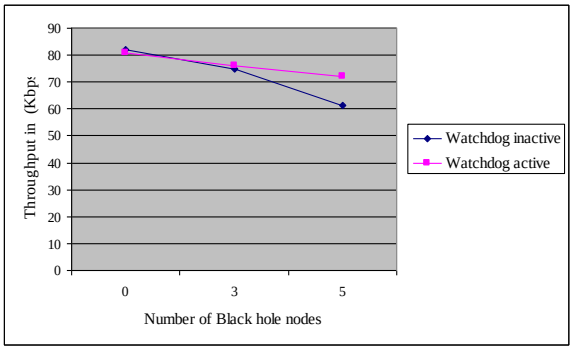

Figure 5: Throughput vs. Black hole seconds pause time

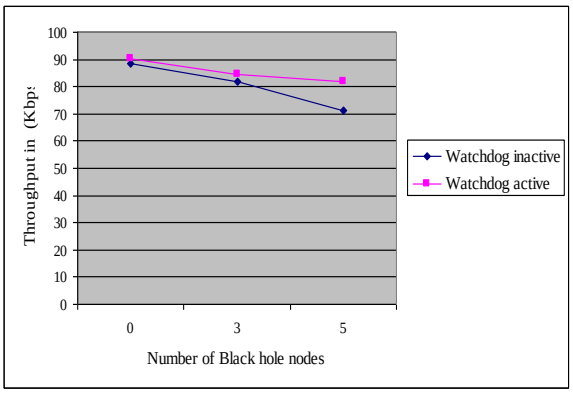

Figure 6: Throughput vs. Black hole nodes for 160 seconds pause time

The results are shown in table 7 increases in the value of throughput when the modified AODV based on watchdog mechanism is active in the presence of 3 black hole nodes, when scenario of node movement for pause time is 0 sec, 40 sec, 120 sec and 160 sec given in table 2.

Table 2: Percentage increase in Throughput in the presence of 3 Black hole nodes

Pause Time (sec)	Throughput in (kbps) with Watchdog inactive	Throughput in (kbps) with Watchdog active	% Increase in Throughput
0 sec	63.42	71.61	7.81%
40 sec	76.62	80.11	4.55%
120 sec	75.13	76.92	2.38%
160 sec	81.91	84.82	3.55%

The results are shown in table 8 increases in the value of throughput when the modified AODV based on watchdog mechanism is active in the presence of 5 black hole nodes, when scenario of node movement for pause time is 0 sec, 40 sec, 120 sec and 160 sec is given in table 3.

Table 3: Percentage increase in Throughput in the presence of 5 Black hole nodes

Pause Time (sec)	Throughput in (kbps) with Watchdog inactive	Throughput in (kbps) with Watchdog active	% Increase in Throughput
0 sec	63.14	69.56	10.16%
40 sec	66.96	75.67	13.06%
120 sec	61.25	72.2	17.87%
160 sec	71.45	81.65	14.28%

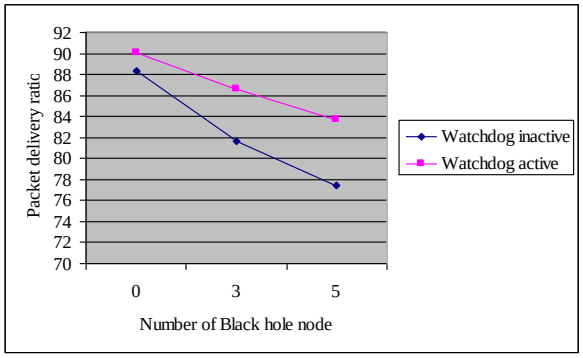

Figure 7: Packet delivery ratio vs. Black hole node for 0 second pause time

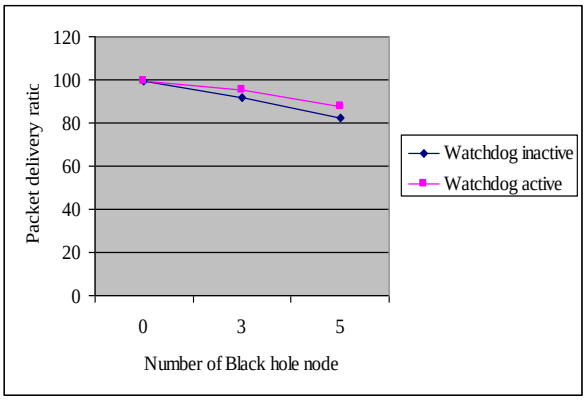

Figure 8: Packet delivery ratio vs. Black hole node for 40 seconds pause time

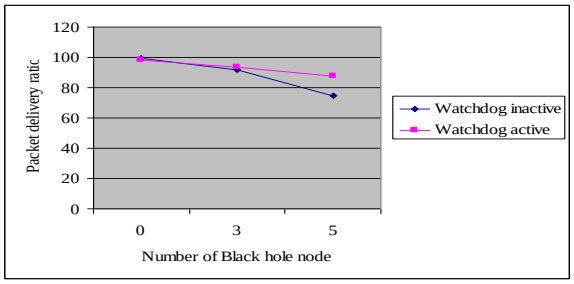

Figure 9: Packet delivery ratio vs. Black hole node for 120 seconds pause time

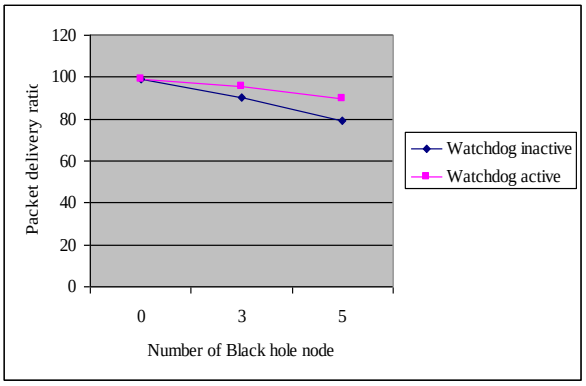

Figure 10: Packet delivery ratio vs. Black hole node for 160 seconds pause time

The results are shown in table 9 increases in the value of packet delivery ratio when the modified AODV based on watchdog mechanism is active in the presence of 3 black hole nodes, when the scenario of node movement for pause time is 0 sec, 40 sec, 120 sec and 160 sec in given in table 4.

Table 4: Percentage increase in PDR in the presence of 3 Black hole nodes

Pause Time (sec)	Packet delivery ratio with Watchdog inactive	Packet delivery ratio with Watchdog active	% Increase in Packet delivery ratio
0 sec	81.82	86.62	5.86%
40 sec	91.36	94.56	3.50%
120 sec	91.41	94.13	2.72%
160 sec	90.11	96.31	6.88%

The results are shown in table 10 increases in the value of packet delivery ratio when the modified AODV based on watchdog mechanism is active in the presence of 5 black hole nodes, when the scenario of node movement for pause time is 0 sec, 40 sec , 120 sec and 160 sec is given in table 5.

Table 5: Percentage increase in PDR in the presence of 5 Black hole nodes

Pause Time (sec)	Packet delivery ratio with Watchdog inactive	Packet delivery ratio with Watchdog active	% Increase in Packet delivery ratio
0 sec	77.45	83.71	8.08%
40 sec	82.37	87.43	6.14%
120 sec	74.48	87.39	17.33%
160 sec	79.5	89.73	12.86%

In another simulation, when threshold value (th2 is 0.5), and all other simulation parameter is same as that for threshold value (th2 is 1). Line charts are shown in figure 11.

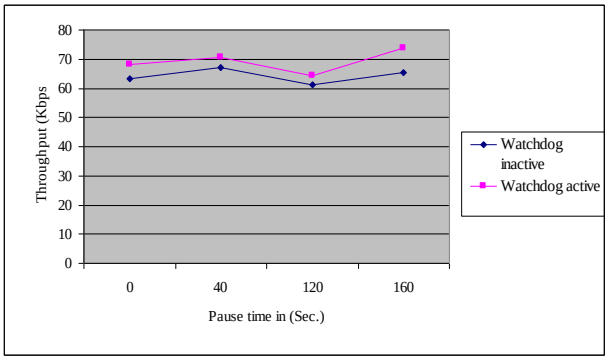

Figure 11: Throughput vs. Pause time for 5 Black hole nodes

VIII. CONCLUSION

Simulated results are taken on ns-2.31 which runs on Red Hat Linux Enterprise Server. A network of 50 nodes was taken for simulation with different pause time i.e. 0, 40, 120 and 160 seconds. Throughput and packet delivery ratio was calculated for existing AODV running for different scenarios having 0, 3 and 5 black hole nodes.

Using same simulation parameter modified AODV was tested on above-mentioned networks having 0, 3 and 5 black hole nodes, for both watchdog active and inactive mode.

The experimental results show that when the black hole nodes is increased up to 6% of total network nodes then in the presence of watchdog active throughput increases up to 3% to 8% for different scenarios. When the black hole nodes is increased up to 10% of total network nodes then in the presence of watchdog active throughput increases up to 10% to 18% for different scenarios.

The experimental results also show that when the black hole nodes is increased up to 6% of total network nodes then in the presence of watchdog active packet delivery ratio increases up to 2% to 7% for different scenarios. When the black hole nodes is increased up to 10% of total network nodes then in the presence of watchdog active packet delivery ratio increases up to 6% to 17% for different scenarios.

Calculated value of throughput for 5 block holes in the network, when threshold value is 0.5 is increased by approximately 5%-8%, where as in the case of threshold values 1.0 throughput is increased by 10%-18% for the same network when watchdog is active. Thus we can say that throughput for 5 black hole nodes with threshold value 0.5 in the network with varying pause time 0, 40,120,160 seconds, decreases when compared with throughput calculated for threshold value 1.0.

REFERENCES

[1] Tamilselvan, L and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. *The 2nd International Conference on Wireless Broadband and Ultra WidebandCommunications.*AusWireless,21-21.

[2] Chen Hongsong; Ji Zhenzhou; and Hu Mingzeng (2006). A novel security agent scheme for AODV routing protocol based on thread state transition. *Asian Journal of Information Technology*,5(1),54-60.

[3] Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative black hole attack in wireless Ad hoc networks. *In Proceedings of 2003 International Conference on Wireless Networks*, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

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

[5] J. Hortelano et al., "Castadiva: A Test-Bed Architecture for Mobile AD HOC Networks", 18th IEEE Int. Symp. PIMRC, Greece, Sept. 2007.

[6] Vesa Kärpijoki,"Security in Ad hoc Networks," http://www.tcm.hut.fi/Opinnot/Tik110.501/2000/papers/karpijoki.pdf.

[7] Janne Lundberg, "Routing Security in Ad Hoc Networks,"http://citeseer.nj.nec.com/cache/papers/cs/19440/http:zSzzSzwww.tml.hut.fizSz~jluzSznetseczSz netsec-lundberg.pdf/routing-security-in-ad.pdf

[8] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.

[9] B.Wu *et al.*, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, Springer, vol. 17,2006.

[10] Sanjay Ramaswamy, Huirong Fu ,Manohar Sreekantaradhya, John Dixon and Kendall Nygard. **"**Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.

[11] P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European WirelessConference, 2002.

[12] Santoshi Kurosawal, hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV – based Mobile Ad Hoc Networks by Dynamic Learning Method" in International Journal of Network Security, Vol.5, No.3, pp.338-346, Nov.2007

Author Profile:

Mr. Kumar Roshan is MCA and pursuing M.Tech in Computer Science & Engineering from IETE, New delhi. He has published many papers in international journals.

Mr. Vimal Bibhu is M.Tech is Computer Science & Engineering and Pursuing Doctor of Philosophy in Computer Science from B.R.A Bihar University Muzaffarpur, Bihar, India. He has published many papers in different International Journals. He is also member of different professional organizations like - IACSIT, IEANG and SERC.

