ISSN:0975-9646

Notion of Black Hole in Wireless Networks targeting on iMANET

Natasha Tomar#1, Mr. Amit Chaudhary*2

#*[M. Tech.]Computer Science and Engineering,*
Uttar Pradesh Technical University, Lucknow, India

* *Department of CSE,*
IIMT Engineering College, Meerut, U. P., India

Abstract— **Internet based Mobile Ad hoc Networking (iMANET) is a growing scope of wireless technology that combines self-organizing mobile networking infrastructures. A large range of applications of this technology varies from commercial applications to military services. At each level, security is a major concern for the reliability of the network. Although several challenges are there with heterogeneous character of hybrid MANET but researchers always seek to develop more secure mechanism. Black hole attack is a kind of denial of service attack in which a node advertises itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. In this paper, first the notion of black hole is analyzed as the security threat to Ad hoc Networks and afterward, the concept is applied on a layer of iMANET as a proposal of security solution.**

Keywords— **iMANET, ISP, BGP, EIGRP, OSPF, GNS, Security, Black hole, Routing Protocol, Infrastructured Networks.**

I. INTRODUCTION

Wireless networking is a method by which organizations, telecommunication networks and homes avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless applications and devices mainly emphasize on Wireless Local Area Networks. This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. Wireless communications networks are generally implemented based on two approaches: Ad-hoc Wireless Networks and Infrastructured Wireless Networks [1].

In Wireless Ad-hoc network, under black hole attack, the malicious node sends a route reply very early. It does not look into the route table for route information, it just send the route reply immediately it finds the RREQ .with higher sequence no and appears that it has the freshest route for destination. As a result of this, the route is established through the malicious node. When the data packet is transmitted through this node it simply drops the packet. Figure 1 shows a wireless ad-hoc network.

In infrastructure based wireless networks, all the devices in the network communicate through a single access point, which is generally the wireless router (further connected to central connection point). Ad-hoc based network is also known as "peer-to-peer" network. Devices on the wireless network connect directly to each other. Infrastructured Wireless Networks is a vastly explored area. The current focus of research is predominantly directed towards security threat to the networks. The risk factor in infrastructure networks is also subjected to denial of service. However, it may be at vast level because the attacker may target any node and this node may also be the single access point. If the attack happens on central connection point then its consequences can be seen at broad level. Figure 2 shows an Infrastructured Wireless Network [2].

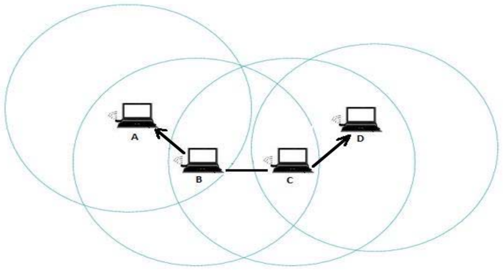


Fig. 1 Mobile Ad-Hoc Wireless Network

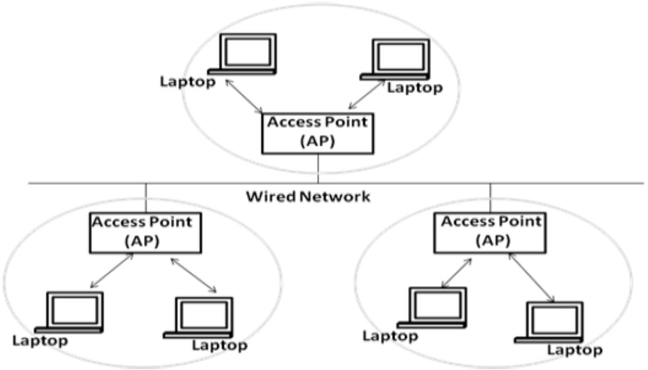


Fig. 2 Infrastructured Wireless Network

II. CHARACTERISTICS AND LIMITATIONS OF WIRELESS NETWORKS

The distinguishing feature of wireless networks is that packets are transmitted with the presence of wireless links. A device can send messages in a wireless network via the wireless medium, air, to another device provided that the receiver is within the transmission range of the sender. This adds flexibility to how a wireless network is formed and structured [2].

A. Characteristics

1) ***Availability:*** Wireless Networks WLANs are available anywhere in the world at an affordable cost.
2) ***Productivity:*** The universal access to the network and Internet can translate into real savings.
3) ***Robust:*** Ability to cope with node failures.
4) ***Scalability:*** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed ranging from peer-to-peer networks (suitable for a small number of users) to full infrastructured networks (of thousands of users that enable roaming over a broad area) [3].
5) ***Quality of Service:*** Quality of Service is a measure of network performance that reflects the network's transmission quality and service availability. As traffic QoS parameters includes throughput, delay and loss rate etc.
6) ***Security****:* Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users.

B. Limitations

- Packet loss due to transmission errors
- Variable capacity links
- Frequent disconnections/partitions
- Limited communication bandwidth
- Limited Physical security
- Low data transmission rates.
- Higher delays, higher jitter

III. CONSTRAINTS IN IMANET

Due to the relatively low capacities achievable over mobile,
multihop wireless networks is not yet well suited for providing high-speed, wide-area, infrastructure networking functionality. However, this does not mean that wide spread usage of MANET technology is not possible or will not occur at the edges of the network. Following are some major constraints in iMANET [4]:

1) ***Dynamic topologies:*** Nodes are free to move randomly. The network topology, which is typically multihop, may change arbitrarily and rapidly at unpredictable times.
2) ***Bandwidth, variable capacity, asymmetric Links****:* Wireless links will continue to have considerably lower capacity than their hardwired counterparts. Another effect is that MANETs will have to be operated in heterogeneous environments with varying bandwidth-delay characteristics.
3) ***Energy-constrained operation****:* Some or all of the nodes in ad-hoc networks may rely on batteries for their energy. For these nodes, power conservation is a critical design issue.
4) ***Wireless vulnerabilities and limited physical security****:* Mobile wireless networks are generally more prone to information and physical security threats than are fixed, hardwired networks.

IV. BLACK HOLE NOTION

In networking, the literary meaning of black hole is- 'A place in the network where incoming traffic is silently dropped without sending any information message to the source node that the data did not reach its destination'. These black hole nodes are invisible in the whole network and can only be detected only by monitoring the lost traffic [5], [6], [7].

According to the Black hole attack in MANET, a malicious node uses the routing protocol to promote itself as having the shortest path to the node whose packets it wants to intercept and drops all routing packets without forwarding it to its neighbours. Further this situation leads to the denial of service. Several solutions are recommended for the detection of the black hole in the system and for removal as well. But it is inadequate because every method comes with its drawback.

Thus, we studied the concept of this attack very deeply and initiated to look towards the thought with new perspective. Resultantly, we created the black hole and implemented it as the security solution aspect. Our target of this solution is internet based ad-hoc network, in which mobile host layer and mobile router layer will be connected with fixed network. This mobile router layer may be either mobile hosts or mobile routers and the fixed network is traditional fixed internet. Such system needs some **hybrid approach** that should be capable enough to work in both to find the path to the gateway and in local Manet as well [8]. So, we worked on its one component that is traditional fixed internet. We decided to make an effort at this platform for the experiment of notion of the positive aspect of black hole. We wanted to show the effect at large level so we showed it at WAN level in which we used both wired and wireless system wherever required with internet connectivity, in which we implemented the concept of black hole positively. The name black hole is conceptually same but with different impact. We successfully created it with additional security. For security add on we implemented cryptographic approach and tried to cover the best possibilities. We have also analysed the bandwidth consumption, packet drop ratio, round trip time and throughput to measure the performance.

V. EXPERIMENTAL WORK

To implement the positive aspect of black hole at the traditional fixed internet level, two major modifications are required. First, each node should be able to have the information only about that node, to which it sends the packet. Second, in this system, we structured the ISP as black hole node to show the wide impact because Internet Service Provider is the key source of information about the routers. For this purpose we used GNS3 simulator. There are various methods for the security of the ISP but they are very costly and complex so, here we tried to simplify the technique with reduced cost.

A. Network Formation and Protocol Activation

In this mechanism, there are total six routers out of which four Routers R1, R2, R3 and R4 used Open Shortest Path First protocol for the communication among with each other and to validate the routing information and prevent invalid information from being propagated throughout the network [9]. Router R6 is the Area Border Router and used Open Shortest Path First protocol. For the security aspect we implemented totally stub area [10]. For the authentication purpose we implemented MD5 algorithm produced by cryptographic hash function [11]. On Router R5, we used Enhanced Interior Gateway Routing Protocol 100. To make two different routers of different protocols capable to communicate with each other we used Border Gateway Protocol. Hence, on Routers R2, R3 and R5, we applied BGP100 so that these routers share their information with each other. Now, since R6 is using OSPF2 and Router R5 that is made ISP is using EIGRP100 protocol, hence, to establish the communication, we have to use BGP so we have applied BGP200 on R6 to make communication possible between BGP100 and BGP200.

TABLE I
NETWORK FORMED BETWEEN DIFFERENT ROUTER PAIRS

Router Pairs	Network
Network between R1 and R2	192.1.12.0/24
Network between R2 and R3	192.1.23.0/24
Network between R3 and R4	192.1.34.0/24
Network between R2 and R5	192.1.25.0/24
Network between R3 and R5	192.1.35.0/24
Network between R5 and R6	192.1.56.0/24 and 192.2.56.0/24

After successful compilation of protocols, blackhole is ready to be implemented.

B. Implementation of Black Hole

We implemented black hole as the mitigation scheme to deal the denial of service attack. It drops the undesirable traffic before it enters the network. We modified the routing according to the concept of black hole to achieve the desired result.

By configuring the BGP routes, we found that router R1 can list out all the available paths in the network because we used dynamic routing and it can send packet from any node to any node but when it has its next hop as the black hole attack then it discard that path and packet travels from source to destination directly.

```
blackhole router:
     concept-statement black-hole{
        from {
           protocol bgp;
           as-path domes_Only;
           implmnt_black-hole;
           route-pass 0.0.0.0/0 prefix-length-range /32-/32;
        }
        then {
           implmnt set no-export;
           next-hop 192.1.56.0;
        }
          }
```

Also, the cryptographic authentication implemented on the routers is the combination of a pre-defined message-digest-key which runs through the MD5 algorithm and that must be the same between routers of an area. In this approach, packet with higher sequence number will be processed and lower sequence number will be discarded. In our network, R1 and R2 are working on network 192.1.12.0/24 on area1 which is connected with backbone area0. Router R2 and R5 are working on network 192.1.25.0/24 with backbone area0 on OSPF. Router R3 and R4 are working on network 192.1.34.0/24 on area2 which is connected with backbone area0. Router R3 is connected with R5 via network 192.1.35.0/24. This network is in OSPF1 with area0 and so on.

```
interface Serial0/0
 ip address 192.1.34.4 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 hardwork
 clock rate 2000000
!
```

Here, interface serial 0/0 indicates the interface on which authentication code is implemented message digest 5 and password is “hardwork”, this password will be encrypted after execution and will be in the form of hash code. For example, hardwork-> 060B06254D5D (here). If the cryptographic passwords of router do matches then communication will not be started.

C. Simulation and Result Analysis

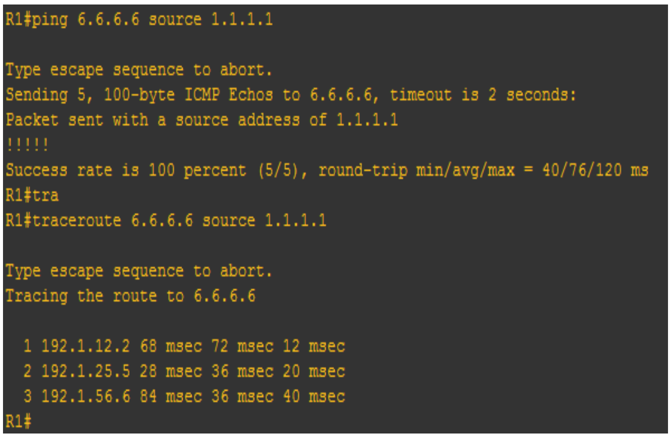
We use the GNS3 Simulator to simulate the black hole notion because GNS3 provides more real touch to the simulation. It has graphical front and dynamips as the core program that allows the simulation.

1) Simulation: Minimum System Requirements for Simulator are: RAM, Processor, Operating System, Tools should be 2 GB, 1.50 GHz, Windows/Linux/MacOS, Complete GNS3 and IOS image file respectively. Simulation parameters that we used are cited in Table II.

TABLE II
SIMULATION PARAMETERS

Parameters	**Values**
Routing Protocols	BGP, EIGRP, OSPF
Region	Large Scale
No. of nodes	6
Black Hole Node	1
Movement Model	Black hole notion
Traffic type	Transit
Simulation time	1000s

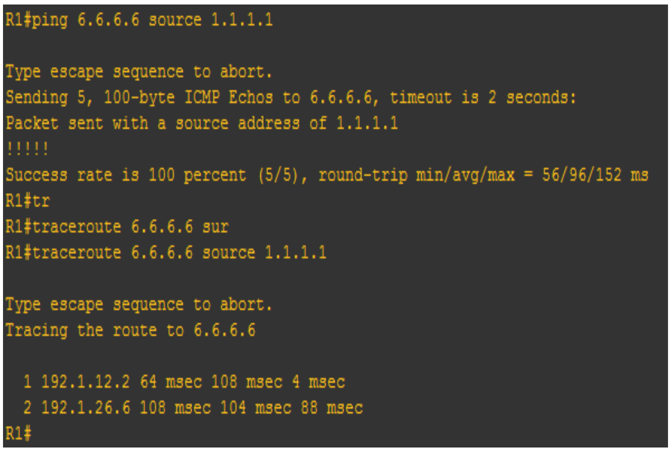
We analyzed the packet transmission by analyzing the bandwidth consumption, throughput and number of packet drop with respect to the every 260 seconds. Before that it is necessary to analyze some implementation steps at console. Figure 3 indicates the Route information from R1 to R6 before Black hole implementation.



```
R1#ping 6.6.6.6 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/76/120 ms
R1#tra
R1#traceroute 6.6.6.6 source 1.1.1.1

Type escape sequence to abort.
Tracing the route to 6.6.6.6

  1 192.1.12.2 68 msec 72 msec 12 msec
  2 192.1.25.5 28 msec 36 msec 20 msec
  3 192.1.56.6 84 msec 36 msec 40 msec
R1#
```

Fig. 3 Before Black hole implementation

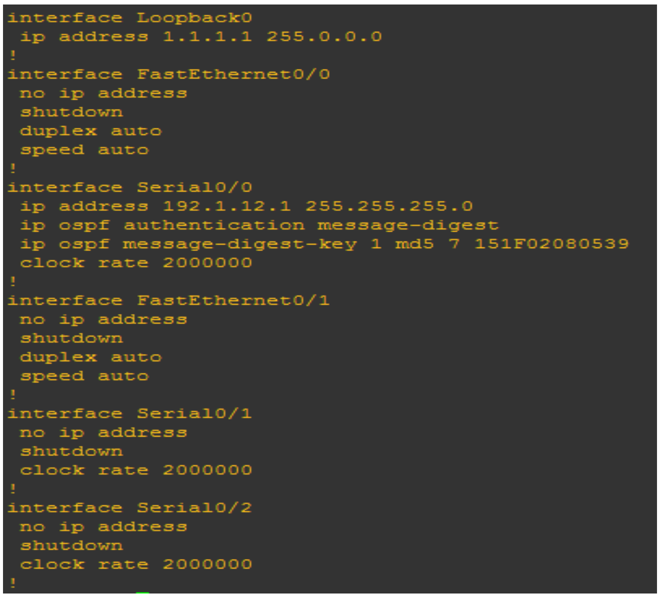
Figure 4 indicates the Route followed from R1 to R6 after Black hole implementation.



```
R1#ping 6.6.6.6 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/96/152 ms
R1#tr
R1#traceroute 6.6.6.6 sur
R1#traceroute 6.6.6.6 source 1.1.1.1

Type escape sequence to abort.
Tracing the route to 6.6.6.6

  1 192.1.12.2 64 msec 108 msec 4 msec
  2 192.1.26.6 108 msec 104 msec 88 msec
R1#
```

Fig. 4 After Black hole implementation

Figure 5 signifies the MD5 cryptographic authentication at router R1. Similarly, it is applied on router R2, R3, R4.



```
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.1.12.1 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 151F02080539
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
```

Fig. 5 Cryptographic authentication at Router R1

2) *Result Analysis:* We analyzed the traffic by analyzing the Round trip time, Bandwidth Consumption, Packet drop ratio etc. with 100 byte packet size each. For observations we used wireshark. Wireshark is a tool for observing the messages exchanged between executing protocol entities.

- **Bandwidth Consumption:** After the execution of black hole notion with positive implementation we observed that bandwidth consumption reduced to 37.782 bytes/sec.

- **Packet Drop Ratio:** We calculated the packet drop ratio after every 60 seconds by calculating the difference between sent packets and received packets per unit time. We performed the operations on GNS3 for 20 iterations and found that there is an effective decrease in the PDR up to 37.01% from black hole notion.

- **Average Round Trip Time and Throughput**: On the basis of observations, it is found that the authentication algorithms that we implemented for the security aspect in the system and the concept of black hole notion with positive implementation itself takes little bit more time hence the round trip time increased but it is negligible in terms of security solution. Before the implementation the average round trip time for the source 1.1.1.1 to 6.6.6.6 was 76 msec and after the implementation it is computed 96 msec. Similarly from the source route 4.4.4.4 to 6.6.6.6 it was 70 msec and after implementation it is computed 120 msec. Figure 6 shows the round trip time graph.

  Now the Throughput, it is the average rate of successful message delivery over a communication channel. It is measured in terms of data packets per second. The graph can be drawn in Packets/tick. We observed the pattern for 1000 sec but here we are showing specifically for 100 seconds. The graph shown in Figure 7 is drawn in terms of bytes/tick where tick leads to second. It implies after implementation, a significant improvement can be seen in scenario. Throughput pattern is almost uniform in the entire set-up.

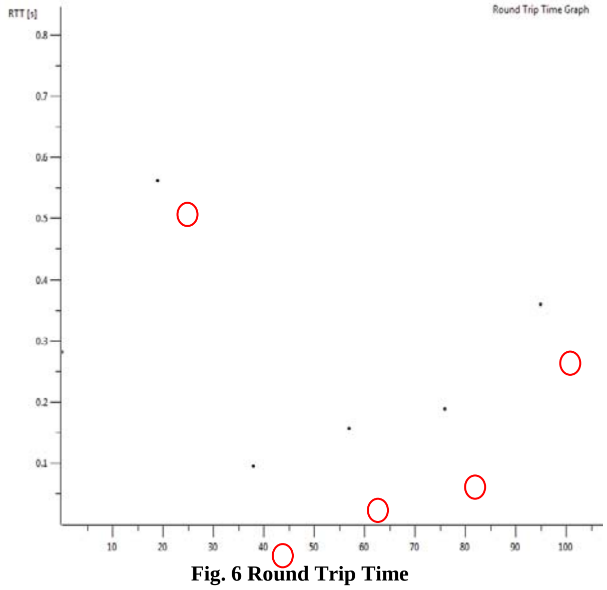


Fig. 6 Round Trip Time

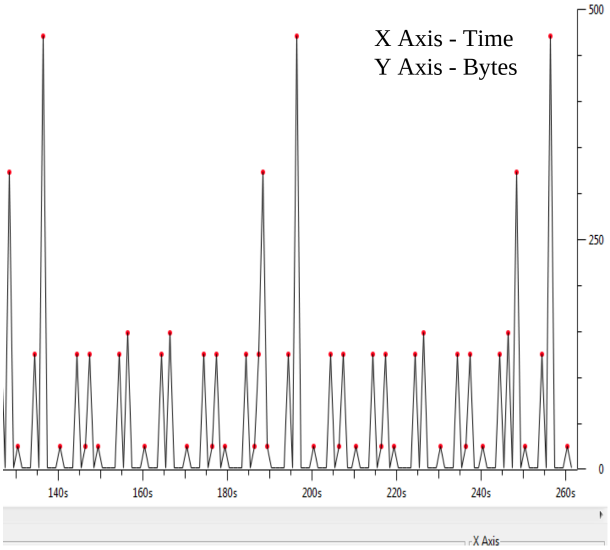


Fig. 7 Average Throughput (Bytes/tick)

VI. Conclusions

A. *Conclusion*

In this paper, we analyzed the behavior of Black Hole Attack as the threat to mobile ad-hoc networks and later on the notion is being simulated as the proposal of security solution to the fixed network layer of internet based mobile ad-hoc network to make the infrastructure network safe and sound. After network formation, we implemented the black hole notion. For the simulation, we chose GNS3 simulator and used specific parameters to show it. According to requirement, different protocols are used and observed the packets for 1000 seconds with one black hole node.

We computed the results, analyzed the graphs and found that by this approach the bandwidth consumption can be reduced up to a significant level. The main factor of analysis is packet drop ratio which is minimized by this approach. The throughput also enhanced. But it is found that focusing on stiff security, the round trip time increased. It should also be in main concern in further researches.

B. *Future Scope*

In this paper, the focus is only on one module of internet based ad-hoc wireless networks. Although it is complete in itself in terms of concept implementation and steps up to advance research but it is found in simulation that in this mechanism, round trip time increased, thus it should be minimized in further researches.

The solution at one platform (presented here) should also be embedded with complete hybrid network. Developing a distributed, scalable security architecture that interoperates with the emerging commercial infrastructure is also a necessary element for eventual widespread utilization of this technology. It opens the additional opportunities for the researchers.

Acknowledgment

I, Natasha Tomar, M. Tech. (Computer Science) Scholar, being the author of this research paper acknowledge that the work discussed here is original piece of research work carried out by me. The results presented have not been submitted anywhere else.

References

[1] Neelam Khemariya, Ajay Khuntetha, “An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs”, International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[2] Rajkumar Singh, Dr. A. K. Jain, “Research Issues in Wireless Networks”, Interational Journal of Advanced Research in Computer Science and Software Engineering”, volume 2, Issue 4, April 2012, ISSN 2277 128X.

[3] Vandana Jindal, A. K. Verma, Seema Bawa, “How two Adhoc network can be different: MANET & WSNs”, IJCST Vol 2, Issue 4, Oct.-Dec. 2011, ISSN:2229:4333.

[4] M. Scott Corson, Joseph P. Macker, “Internet-based Mobile Ad Hoc Networking”, IEEE Internet Computing, July-Aug, 1089-7801/ 99.

[5] Mohammad Al-Shurman et.al, “Black Hole Attack in Mobile Ad-Hoc Network” ACMSE 04, April 2-3, 2004, Huntsville, AL, USA.

[6] Medadian, M.; Mebadi, A.; Shahri , E., "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[7] Latha Tamilselvan, V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET”, Journal of Networks, Vol 3, No 5, 13-20, May 2008.

[8] Velmurugan Ayyadurai, Rajaram Ramasamy, “Internet Connectivity for Mobile Ad Hoc Networks Using Hybrid Adaptive Mobile Agent Protocol”, The International Arab Journal of Information Technology, Vol. 5, No. 1, January 2008

[9] V.Vetriselvan, Pravin R.Patil, M.Mahendran, “Survey on the RIP, OSPF, EIGRP Routing Protocols”, International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1058-1065

[10] Toni farley, patrick mcdaniel and kevin butler, “A Survey of BGP Security Issues and Solutions”, ACM Journal Name, Vol. V, Pages 1–23.

[11] Khalid Abu Al-Saud, Hatim Tahir, Moutaz Saleh and Mohammed Saleh, “A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2, and OSPF”, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.