I.J.Modern Education and Computer Science, **2012, 8, 47-53**
Published Online August 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2012.08.07

A Study of Black Hole Attack on MANET Performance

C. K. Nagpal
Principal, Echelon Institute of Technology, Faridabad, India
Email: nagpalckumar@rediffmail.com
Chirag Kumar
Department of Electronics Engineering, YMCA UST, Faridabad, India
Email: chiragarora35@gmail.com
Bharat Bhushan
Department of Electronics Engineering, YMCA UST, Faridabad, India
Email: bhrts@yahoomail.com
Shailender Gupta
Department of Electronics Engineering, YMCA UST, Faridabad, India
Email: shailender81@gmail.com

Abstract — Mobile Ad hoc Network (MANET) is a self-organized wireless network, consisting of nodes (mobile devices) responsible for its creation, operation and maintenance. The communication in the MANET is of multihop in nature due to absence of any fixed infrastructure. An attacker may intrude easily into MANET by posing as legitimate intermediate node and present various types of security attacks on data exchanges taking place between source and destination. In this paper we study the impact of presence of black hole node on MANET performance on the basis of reachability, hop count, neighbor node density and path optimality. We observe that as the percentage of black hole nodes increases, the MANET performance degrades significantly.

Index Terms — Black Hole, Network, Performance Parameters, Security

I. INTRODUCTION

Mobile ad hoc network (MANET) [1-4] is a combination of mobile nodes forming a temporary network, without the requirement of any kind of fixed network infrastructure, although commercial wireless technologies are generally based on towers and high-power base stations. MANET is characterized [5-6] by fast installation, low bandwidth, limited processing capability etc. The communication in MANET is via intermediate nodes of the network. In the absence of proper security mechanisms, an attacker node may join the network easily and act as an intermediate node which may be threat to security of data being exchanged. Various issues and challenges related to security are as under:

Shared Broadcast Radio channel: The nodes in MANET share common radio channel that makes easier for the attacker to pose threat.

Insecure operational environment: The Nodes in MANET have to work in battlefields etc where the environment is hostile to MANET operation.

Lack of central authority: Due to lack of central authority like BS etc in MANET, it is very difficult to implement security mechanisms.

Lack of association: Since the topology of the MANET is dynamic in nature, in the absence of any authentication mechanism, an intruder can easily carry out security attack.

Limited resource availability: Due to limited availability of resources like battery power [7-10], processing capability and bandwidth etc. with the nodes of MANET, it is very difficult to the implement complex security mechanism [11-13].

Due to all the above deficiencies in MANET these networks are vulnerable to attacks by malicious nodes. The network security attack [14-15] can be broadly classified in two categories i.e. passive and active attacks. A passive attack does not disrupt the operation of the network except for snooping the data. The requirement of the confidentiality is violated if the attacker is able to interpret the data. Since the network operation is not affected, it is very difficult to detect this kind of attack.

In contrast active attack tries to alter or destroy the data being exchanged and disrupts the normal operation of the network. Active attack can be further classified as external and internal attacks. External attack is committed by external nodes and internal attack is done by nodes which are part of the MANET having shortages of resources like battery power and bandwidth etc. It is very difficult to isolate these nodes.

Different security attacks are done on various layers of the network out of which network layer attacks are most important. Some of the network layer security attacks are described below:

Wormhole attack: In this attack [16-18], an attacker receives packets at one location and tunnels them at

another location where these packets are resent into the network. In the absence of proper security mechanisms, most of the existing routing protocols may fail to find the valid routes.

Blackhole attack: In this attack [19-21] a malicious node [10] may advertise a good path to a destination during routing process. The intention of the node may be to hinder the path finding process or interpret the packet being sent to destination.

Alternatively black-hole scenario may be defined as the one in which the cannel properties tend to be asymmetric i.e. the signal strength in both direction may not be same. In this case a node which receives the data packet but does not forward it is termed as black hole. In either case the normal operation of the MANET is disrupted.

Byzantine attack: Here [22] compromised intermediate nodes carries out attack such as loops, routing packets on non optimal paths and selectively dropping packets.

Information disclosure: A compromised network node may leak the important or confidential information such as network topology, geographical information of nodes and optimal routes to the nodes etc.

Resource consumption attack: An attacker node acting as intermediate node may initiate unnecessary request for routes, frequent generation of beacon packets or forwarding stale routes to nodes. This result in over consumption of nodes limited resources and keeps the node unnecessary occupied.

In this paper we analyze the impact of the presence of the black-hole nodes on the MANET performance. We have found that as the percentage of black hole nodes increases, the network performance degrades. The paper is organized as follows: section 2 gives description about simulation setup parameters, results are provided in section 3 and section 4 provides conclusion.

II. Literature Survey

S. Dourker [23] et al performed a performance analysis of ad hoc networks in the presence of the black hole nodes. In this they studied the effects of black hole attacks on the network performance. For this purpose the study was carried out on the packet loss with and without a black hole node using simulator NS-2. A solution was also proposed by them in order to minimize the effect of black hole attacks. This solution improved the network performance in the presence of a black hole by about 19%.

S. Sharma [24] et al provides a solution in order to overcome the effect of black hole attack on the performance of MANET. To provide security in small networks is easy as compare to large networks. So, they divide large network into number of zones and implemented Secure-ZRP protocol which can be used to prevent black hole attack in zones or outside the zones. Performance evaluation is done in QUALNET simulator. Their analysis shows that the performance of ordinary routing protocol is low in comparison to the Secure Zone Routing Protocol.

M. Medadian [25] et al proposed a method in order to minimize the effect of black hole attack, to wait and check the replies from all the neighboring nodes to find a safe route but this approach suffers from high delay. The Simulation results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

Another study was carried out by V. Palanisamy [26] et al to measure the effect of the black hole nodes on the performance of MANET. They studied the impact of black hole node and also their position in the simulation region. The performance comparison is done by using performance metrics packet delivery with respect to three scenarios as: Black hole attack node near sender, black hole attack node near receiver and anywhere within the network.

N. Sharma [27] et al analyzes the impact of black hole attack by presenting two methods. The first method is to find more number of paths to the destination. The second is to exploit the packet sequence number included in any packet header. Their simulation shows that in comparison to the original ad hoc on demand distance vector (AODV) routing scheme, the second solution can verify 75% to 98% of the route to the destination depending on the pause time at a minimum cost of the delay in the networks.

Okoli Adaobi [28] et al worked to find the impact of black hole attack on the performance of MANET and also found the impact of position of black hole node. According to them under the on-demand routing protocol, the closer a malicious node is to the source of traffic, the greater the extent of damage inflicted on the networks.

III. Simulation Setup Parameters

This Section describes the simulation setup process, various parameters used in simulation process and the performance metrics used in the simulation process.

A. Simulation Setup

To find the impact of presence of black hole nodes on the MANET performance, a simulator was designed in MATLAB 7.0. The simulation process was carried out for 40 and 50 number of nodes. The nodes were uniformly distributed in the simulation region by using rand function of MATLAB. To create path between source and destination Dijkstra's Shortest Path Routing Algorithm was used. Since black hole nodes do not participate in normal routing process, these were made unreachable. Fig. 1 shows the snapshot of simulation region showing the deployment of the nodes. The path shown in red color is formed by nodes including black holes, whereas path formed in cyan color is formed by nodes avoiding black holes.

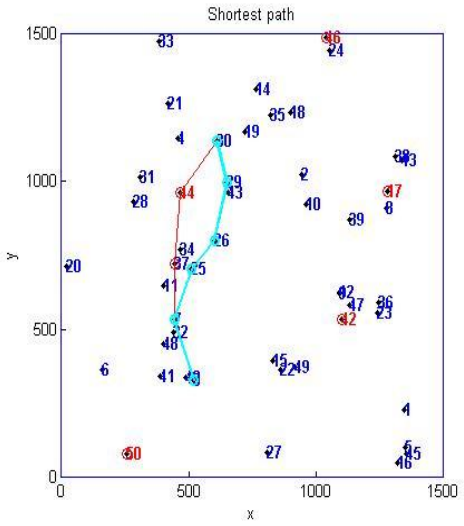

Figure 1. Snapshot of Simulation Process

B. Simulation Process

The simulation process is carried out for 40 and 50 nodes by placing them randomly and uniformly in the simulation region. The percentage of black hole nodes is varied from 0 to 100. Various simulation set up parameters are shown in Table 1. Algorithm for the simulation process is as shown in Fig. 2.

```
Algorithm
{
Hop Count = 0;
Path length = 0;
Reachability = 0;
for Black hole node (percentage) = 0:10:100
{
    for Source = 1 to N-1
    {
        for Destination = Source + 1 to N
        {
            for Iteration = 1 to 25
            {
                Distribute node randomly
                if (path exist = Y)
                {
                    Calculate
                    Path length = Total distance from S to D
                    Hop count = Number of intermediate nodes
                    Reachability = Reachability + 1;
                    }
            }
        }
    }
  Average Reachability = (2*reachability/N(N-1)*25)
  Average Path Length = path length/ reachability
  Average hop count = hop count/ reachability
}
}
```

Figure 2. Algorithm of simulation process.

C. Performance Metric Used

The performance metric used to find the impact of black hole nodes are as follows:

Hop Count: Defined as the number of total number of intermediate nodes from source to destination for successful operations.

Reachability: Defined as the fraction of successful routes to the total number of routes (reachable or not).

Neighbor Node Density: Defined as the average number of neighboring nodes in a network.

Path Optimality: Defined as the ratio of the shortest path containing black hole nodes to the shortest path length formed without the presence of black hole nodes.

TABLE I. SIMULATION SETUP PARAMETERS

Parameter	Value
Size of Region	2250000 sq. units
Shape of Region	Square: 1500(Length)
Number of Nodes Deployed	40,50
Transmission Range	250
Percentage of Black Hole Nodes	0-100
Routing Algorithm Used	Dijkstra's Shortest Path Routing Algorithm
Routing Strategy Used	Shortest Path Routing
Performance Metrics Used	♠ Hop Count ♠ Throughput ♠ Neighbour Node Density ♠ Path Optimality
Placement of Nodes	Random
Number of iterations	25

IV. RESULTS AND DISCUSSIONS

A. Impact on hop count

Fig. 3 shows the impact of black hole count on Hop Count. Fig. 3 and Fig. 4 show the results for 40 and 50 numbers of nodes respectively. Following inference can be made from the fig. 3 and 4.

- ♠ As the percentage of black hole nodes increases, there is consistent decrease in value of hop count.
- ♠ The value of hop count decreases to zero as the percentage of nodes reaches to 100%. At very high concentration (nearly 100%) of black hole nodes the number of intermediate nodes reduces to zero since at this concentration the

communication is in between neighboring nodes only.

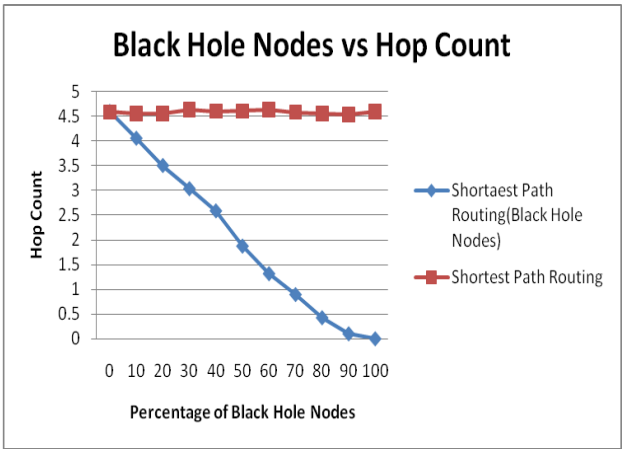

Figure 3. Impact on Hop Count for 40 nodes.

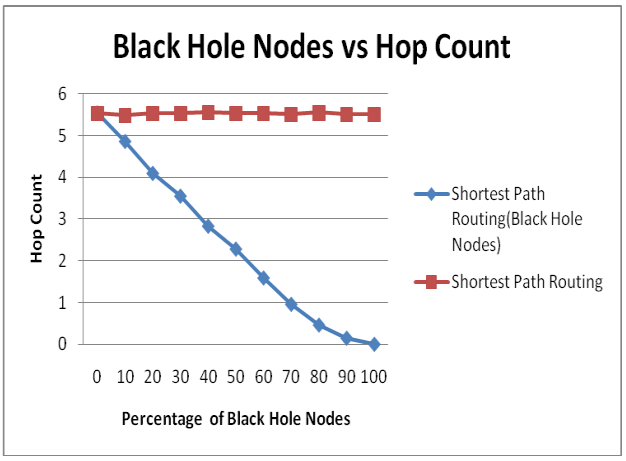

Figure 4. Impact on Hop Count for 50 nodes.

B. Impact on Reachability

Fig. 5 and 6 shows the impact of black hole on reachability. Fig. 5 shows the impact for 40 nodes and fig. 6 shows the impact for 50 nodes. Following inference can be made from the fig. 5 and 6.

- As the percentage of black hole nodes increases, there is decrease in value of reachability.
- For a given area deployed with higher number of nodes the reachability value is quite high than the area employing lesser number of nodes.
- The value of reachability reduces to 10% for 40 number of nodes and 15% for 50 number of nodes as the percentage of nodes reaches to 100%. It should be noted here that even in an environment containing 100% concentration of black hole nodes the reachability value doesn't reaches zero level since the communication between neighboring nodes still occurs.

C. Impact on Neighbor Node Density

Fig. 7 and 8 show the impact of bandwidth on Neighbor Node Density. Fig. 7 shows the effect for 40 nodes and fig. 8 for 50 nodes. Following inference can be made from the figure:

- As the percentage of black hole node increases there is decrease in value of Neighbor Node Density. This is due to the fact that the black hole nodes don't reply to route request packets hence the neighbor node density decreases and reaches to zero at 100% concentration of black hole nodes.
- For fixed size area the neighbor node density will be higher for an environment having higher number of nodes.
- The value of Neighbor Node Density decrease to zero as the percentage of nodes reaches to 100%.

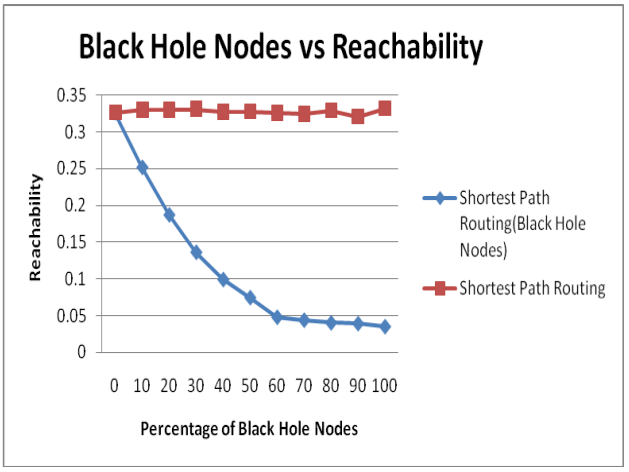

Figure 5. Impact on Reachability for 40 nodes.

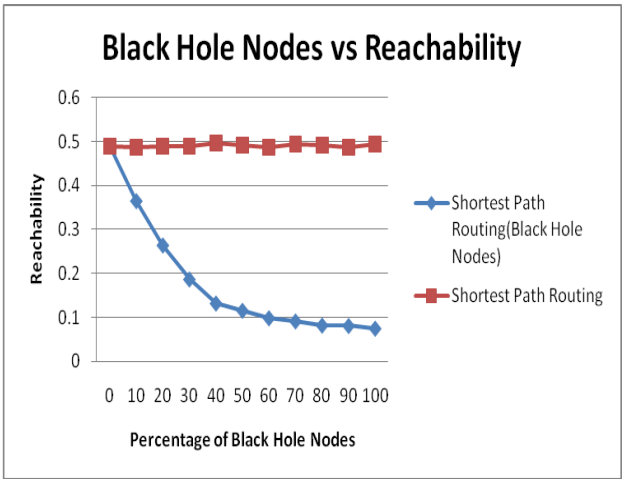

Figure 6. Impact on Throughput for 50 nodes.

D. Impact on Path Optimality

Fig. 9 and 10 show the impact of bandwidth on Path Optimality. Fig. 9 shows the effect for 40 nodes and fig. 10 for 50 nodes. Following inference can be made from the fig. 9 and 10.

- As the percentage of black hole nodes increases, there is decrease in value of Path Optimality.
- For fixed size area the path optimality is higher for an environment having higher number of nodes.

- The value of Path Optimality reaches to nearly 17% as the concentration of black hole nodes reaches to 100%.

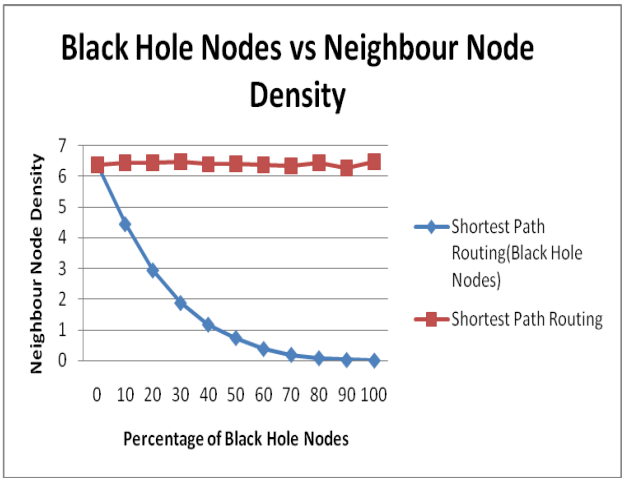

Figure 7. Impact on Neighbour Node Density for 40 nodes.

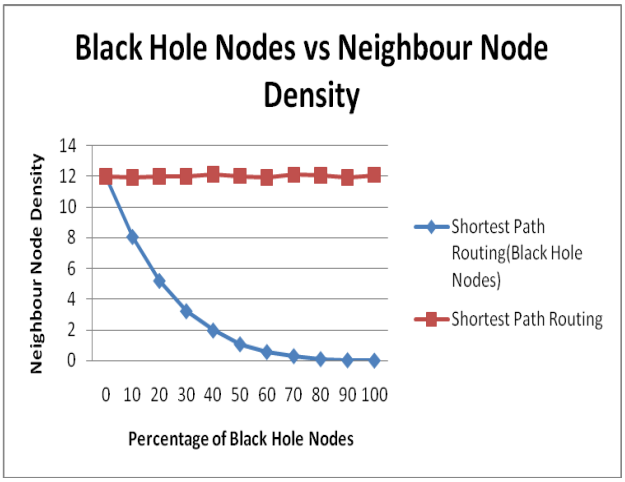

Figure 8. Impact on Neighbour Node Density for 50 nodes.

V. Conclusion

The impact of black hole nodes on the performance of routing protocol can be concluded as follows:

- The values of hop count and path optimality tend to decrease linearly. As the percentage of nodes reaches to 100 percent the values approaches zero.
- The values of reachability does not reach zero level even at 100% concentration of black hole nodes since at this concentration the communication still prevails between neighboring nodes.

All these results can be very useful for the protocol designers while designing any protocol for ad hoc network.

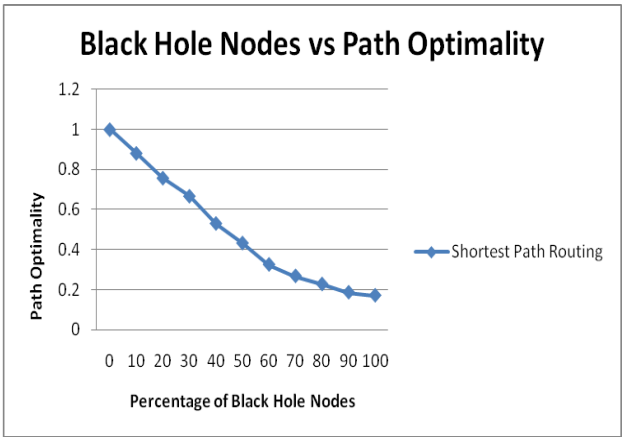

Figure 9. Impact on Neighbour Node Density for 50 nodes.

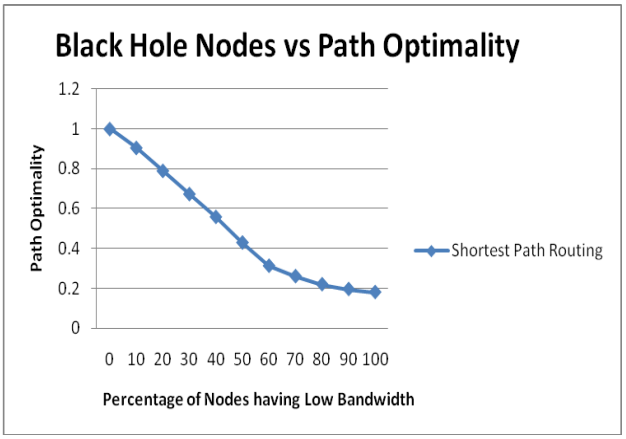

Figure 10. Impact on Neighbour Node Density for 50 nodes.

References

[1] Charles E. Perkins, “Mobile Ad-Hoc Networks,” Addison-Wesley(2000).

[2] J. E. Wieselthier, E. Altman, A. Ephremides, J. P. Macker, H. B. Russell, M. Steenstrup, and S. B. Wicker," Wireless ad hoc networks – part II", IEEE Journal on SAC , Volume 23, Number 3, March 2005.

[3] Giorgos Papastergiou, Ioannis Psaras , Vassilis Tsaoussidis," Deep-Space Transport Protocol: A Novel Transport Scheme for Space DTNs", Computer Communications Volume 32, Issue 16, 15 October 2009, Pages 1757–1767 , Elsevier.

[4] Hany Samuel,Weihua Zhuang,Bruno Preiss,"DTN Based Dominating Set Routing for MANET in Heterogeneous Wireless Networking", Journal Mobile Networks and Applications Volume 14 Issue 2, April 2009 Pages 154 - 164.

[5] J. Mackar and S. Corson, RFC 2501, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF 1999.

[6] Chim Yuen Chong, Raymond Seah Kwang Wee, Sim Soon Lian, Tan Jia Hui,“Moblie Ad hoc Networking”,http://www.dsta.gov.sg/DSTA_horizons/2006/Chapter_7. Htm.

[7] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux, J. Y. Le Boudec, "Self- Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes," IEEE Communications Magazine, Vol. 39, No. 6, June 2001.

[8] L. Buttyán, J.-P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Technical report No. DSC/2001/001, Swiss Federal Institution of Technology, Lausanne, January 2001. http://icawww.epfl.ch/hubaux/.

[9] L. Buttyán, J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Technical Report No. DSC/2001/046, Swiss Federal Institution of Technology, Lausanne, 31 August 2001. http://icawww.epfl.ch/hubaux/.

[10] Shailender Gupta, C. K. Nagpal and Charu Singla,"IMPACT OF SELFISH NODE CONCENTRATION IN MANETS",International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[11] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[12] Hao Yang,Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang,"Security in mobile ad hoc networks: challenges and solutions",Wireless Communications, IEEE Feb 2004.

[13] Hongmei Deng, Wei Li, D.P.Agrawal,"Routing security in wireless ad hoc networks",Communications Magazine, IEEE Oct 2002.

[14] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour,"A survey of routing attacks in mobile ad hoc networks",Wireless Communications, IEEE October 2007.

[15] Hoang Lan Nguyen,Uyen Trang Nguyen,"A study of different types of attacks on multicast in mobile ad hocnetworks",http://dx.doi.org/10.1016/j.adhoc.2006.07.005Volume 6, Issue 1, January 2008, Pages 32–46.

[16] Khin Sandar Win,"Analysis of Detecting Wormhole Attack in Wireless Networks",World Academy of Science, Engineering and Technology 48 2008.

[17] Yih-Chun Hu, A. Perrig, D.B.Johnson,"Wormhole attacks in wireless networks",Selected Areas in Communications, IEEE Journal 2006.

[18] N.Song, L.Qian, X. Li,"Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach",Parallel and Distributed Processing Symposium, 2005.

[19] A. Patcha, A. Mishra,"Collaborative security architecture for black hole attack prevention in mobile ad hoc networks",Radio and Wireless Conference, 2003. RAWCON '03.

[20] Bo Sun, Yong Guan, Jian Chen, U.W.Pooch,"Detecting black-hole attack in mobile ad hoc networks",Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492).

[21] L. Tamilselvan, V. Sankaranarayanan,"Prevention of Blackhole Attack in MANET",Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on 27-30 Aug. 2007.

[22] S. Marano, V. Matta, L. Tong,"Distributed Detection in the Presence of Byzantine Attack in Large Wireless Sensor Networks",Military Communications Conference, 2006. MILCOM 2006. IEEE.

[23] S. Dokurer, Y. M. Ert , C. E. Acar," Performance analysis of ad-hoc networks under black hole attacks", SoutheastCon, 2007. Proceedings. IEEE.

[24] S. Sharma, Rajshree, R. P. Pandey, V. Shukla, " Bluff-Probe Based Black Hole Node Detection and prevention", Advance Computing Conference, 2009. IACC 2009, IEEE International.

[25] M. Medadian, M. H. Yektaie, A. M. Rahmani, "Combat with Black hole attack in AODV routing protocol in MANET", First Asian Himalayas International Conference on 3-5 Nov. 2009.

[26] V. Palanisamy, P. Annadurai, S. Vijayalakshmi," Impact of black hole attack on multicast in ad hoc network (IBAMA)", Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on 28-29 Dec. 2010.

[27] N. Sharma, A. Sharma," The Black-Hole Node Attack in MANET", Second International Conference on Advanced Computing & Communication Technologies 2012.

[28] Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian," Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-Organised Networks", New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on 7-10 May 2012.

Dr. C. K. Nagpal is principle in Echleon Institute of Technology. He received his Ph. D. degree in Computer Science from the YMCA University of Science and Technology, Faridabad. His academic interests include network security, software reliability and artificial intelligence.

Dr. C.K.Nagpal
Principal
Echleon Institute of Technology,
Faridabad
E-mail: nagpalckumar@rediffmail.com

Mr. Chirag Kumar has B. Tech (ECE) from Kurukshetra University and pursuing his M.Tech (ECE) from YMCA University of Science and Technology. His academic interests include network security and fuzzy logic.

Mr. Chirag Kumar
Student
YMCA University of Science and Technology
Faridabad
E-mail: chiragarora35@gmail.com

Mr. Bharat Bhushan has B. Tech (Electronics) from PEC and M.Tech (Electronics) from YMCA University of Science and Technology. His academic interests include Mobile Ad-hoc Network, Network Security.

Bharat Bhushan
Assistant Professor (Electronics Engg.)
YMCA University of Science and Technology,
Faridabad
E-mail: bhrts@yahoomail.com

Mr. Shailender Gupta is B. Tech (Electronics) and M. Tech (Computer Engg.) and pursuing his Ph. D in the area of ad-hoc mobile network security from YMCA University of Science and Technology. His academic interests include network security, automata theory and fuzzy logic.

Shailender Gupta
Assistant Professor (Electronics Engg.)
YMCA University of Science and Technology,
Faridabad
E-mail: shailender81@gmail.com

