An Intrusion Detection System for Combating Attacks against Cognitive Radio Networks using OSPF

Arjita Singh Sengar
M. Tech. Scholar
Technocrats Institute of Technology- Advance
Bhopal (M.P.)

Pankaj Soni
Professor
Technocrats Institute of Technology- Advance
Bhopal (M.P.)

ABSTRACT
In this paper, the method of Intrusion Detection System (IDS) is implemented, which is based on the principle of network, nodes or information misuse detection system, which can accurately compare the signatures of known attacks and has a low rate of packet dropout's alarms.

Security is a major concern in wireless technology and this work deals with security in wireless mobile ad-hoc network by using Novel IDS in Open Shortest Path First (OSPF) routing protocol. We are bounding wireless mobile ad-hoc network nodes to getting updates from unknown or unwanted nodes on the same network through routing table; we are using a Novel intrusion detection technique with the help of routing protocols in the MANET (mobile ad hoc network).

MANET is very popular, efficient, easy and secure way of communication between two or more mobile user ends and we can send and receive data, information, updates and signals from one end to another known end securely by using Novel IDS technique and by blocking unknown nodes in MANET. We are using NS2 simulation tool for performing our method.

Keywords
Open Shortest Path First (OSPF), MANET (mobile ad hoc network), Intrusion Detection System (IDS), Ad hoc on Demand Routing Protocol (AODV), Dynamic Source Routing Protocol (DSR).

1. INTRODUCTION
MANETs have bound distinctive characteristics that build them susceptible to many styles of attacks. Since they are deployed associate in nursing open surroundings wherever all nodes co-operate in forwarding the packets within the network, malicious nodes are troublesome to notice. Hence, it's quite troublesome to style a secure protocol compared to wired or infrastructure-based wireless networks.

This section discusses a number of the problems and challenges that a designer of secure protocols faces. These problems are analyzed with regard to the first goals of a secure protocol – confidentiality, integrity and handiness, credibility and non-repudiation. The attacks and threats allowed by existing Eduard MANET routing protocols are then mentioned. The operating of some secure routing protocols that address these threats like SEAD, ARIADNE, ARAN and SRP is then delineating.

Consecutive section discusses another necessary issue in MANETs- certificate-based authentication. It surveys some mechanisms planned and analyzes the necessities for effective certificate-based authentication in MANETs.

Ad-hoc networks were primarily used for military applications. Since then, they have become a lot of and a lot of well-liked among the computing trade. Applications embody emergency search and rescue operations, preparation of sensors, conferences, exhibitions, virtual faculty rooms and operations in environments where construction of infrastructure is hard or expensive. Ad-hoc network types are shown in Fig 1 below:

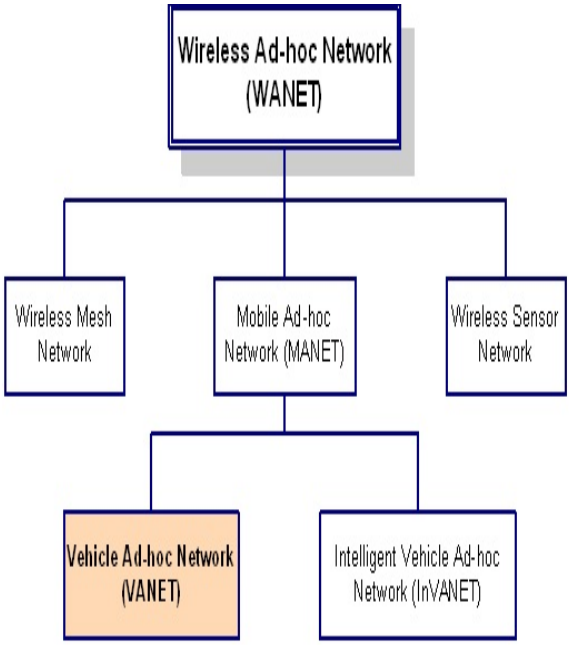

Fig 1: Ad-hoc network types

2. ATTACKS VICTIMIZATION FABRICATION
In this sort of attack, a malicious node tries to inject pretend messages or routing packets to disrupt the routing mechanism. Such attacks area unit tough to discover during a Eduard. MANET since the routing packets seem to be legitimate packets to the nodes processes them. The subsequent attacks area unit samples of attacks by fabrication.

2.1 Falsification route errors
This sort of attack exploits the printed mechanism of causation route error (RERR) packets in AODV and DSR routing protocols.

2.2 Route cache poisoning
It refers to attacks that modify or corrupt the routing tables by injecting pretend routing packets. Such associate attack is feasible against associate optimized version of the DSR

protocol, within which nodes discover routes from neighboring nodes by listening promiscuously on the printed channel.

3. SPECIAL ATTACKS

Apart from the attacks delineate on top of their area unit 2 alternative severe attacks that area unit attainable against routing protocols like AODV, DSR, etc. they're delineate below-

3.1 Wormhole attack

The hollow attack could be a severe sort of attack within which 2 colluding malicious nodes will tunnel packets through a "tunnel" or vertex cut within the network as shown in Fig 2.

Here, M and Q area unit 2 malicious nodes that tunnel the packets from one subnet to a different. Such a kind of attack is tough to discover in an exceedingly network and severely damages the communication between the nodes. Such associate degree attack is prevented by victimization packet leashes that attest the temporal arrangement data within the packet to discover faux packets within the network [14].

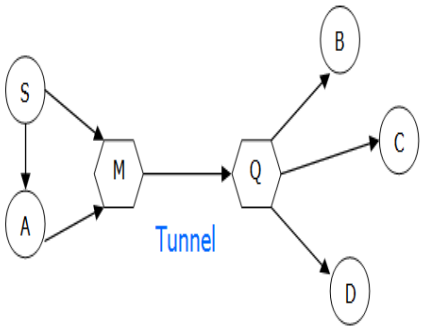

Fig 2: Wormhole attack

3.2 Part Attack

During this attack, a node advertises a zero metric for all destinations inflicting all nodes around it to route packets towards it. The AODV protocol is prone to such associate degree attack. A lot of details on this attack are found in [15].

4. PROPOSED SYSTEM

We have given the new technique of intrusion detection and interference system mistreatment OSPF routing protocol. During this work, we worked on security in wireless mobile ad-hoc network by mistreatment Novel IDS wireless network supported OSPF routing protocol. OSPF routing protocol may be a distance vector and link state (hybrid) routing protocol used for higher performance and decreasing routing load and provides secure communication between wireless nodes. We have a tendency to square measure implementing the tactic of IDS that is predicated on the principle of network, nodes or info misuse detection system, which might accurately compare the signatures of renowned attacks and encompasses a low rate of packet dropout's alarms. we have a tendency to square measure bounding wireless mobile ad-hoc network nodes to obtaining update from unknown or unwanted nodes within the same network through routing table we have a tendency to square measure mistreatment Novel intrusion detection technique with the assistance of routing protocols in Eduard MANET (mobile unexpected network). Eduard MANET is incredibly widespread and economical, best and secure approach of communication between 2 or a lot of mobile user ends and that we will send and receive knowledge, info, updates and signals from one finish to a different renowned finish firmly by mistreatment Novel IDS technique and by obstruction unknown nodes in Eduard MANET.

5. PROPOSED SOLUTION

We can take these all parameters from previous paper[3], we also calculate the same overheads in those parameters .We can observe that after involving TTL field it gives better performance.

We can calculate the following parameters:-

1. PDR (Packet Delivery Ratio) - It is the number of delivered data packet to the node. Greater is the value of packet delivery ratio better is the performance of the node.
2. PDR= (Number of Packet's Transmitted)/ (Total Number of Incoming Packets)
3. CO (Control overhead) - The ratio of the number of routing protocol control packets transmitted to the number of data packets is known as Control overhead.
4. CO = (Number of Control Packet's Transmitted)/ (Total Number of Packets)
5. PMIR (Packet Misroute Rate) - Node sends packet to the wrong destination is called misroute data packet. PMIR ratio is the number of misroute packet is delivered to the transmitted packets.

PMIR= (Number of Packet's Misrouted)/ (Total Number of Incoming Packets)

6. PROPOSED ALGORITHM

1. Collect all the metrics using NS-3 test bed and save as .M file.
2. Extract .M file using DOM (Dynamic Object Module) and input in IDS.
3. Calculate PDR, CO and PMIR
4. If (PDER>0.9) and ((CO >= 70) and (PMIR > =0.3)

Node is malicious

Else No-operation

7. SIMULATION ENVIRONMENT

We used Network simulator-2 (NS2) for implementation of proposed work. The methodologies we acclimated are bigger strengthening apprehension adjustment and cusum algorithm to strengthen the fulfillment of radio network. We acclimated C/C++ and TCL accent for implementation.

Network simulator-2 (NS) is a widely used network simulator for network related research work. NS (variant 2) is an object-oriented, adjustment actor developed at Berkely. It is accounting in C++ and Otcl (Tcl program accent with Acquisitive extensions developed at MIT). NS offers abundant accoutrement for simulation of TCP and UDP. It's as well acclimated in routing and multicast systems over lively and Wi-Fi networks. The NS mission is now a allotment of the VINT venture. NS as good accoutrements media admission band protocols for LAN. NS initiatives develops accoutrement for simulation results. NS is specially high quality for assuming LAN and WAN. It accoutrements

adjustment protocols corresponding to TCP and UDP. It as well accoutrements cartage antecedent fulfilment similar to Telnet, FTP, internet. It as well accoutrements router chain alignment apparatus equivalent to Drop Tail.

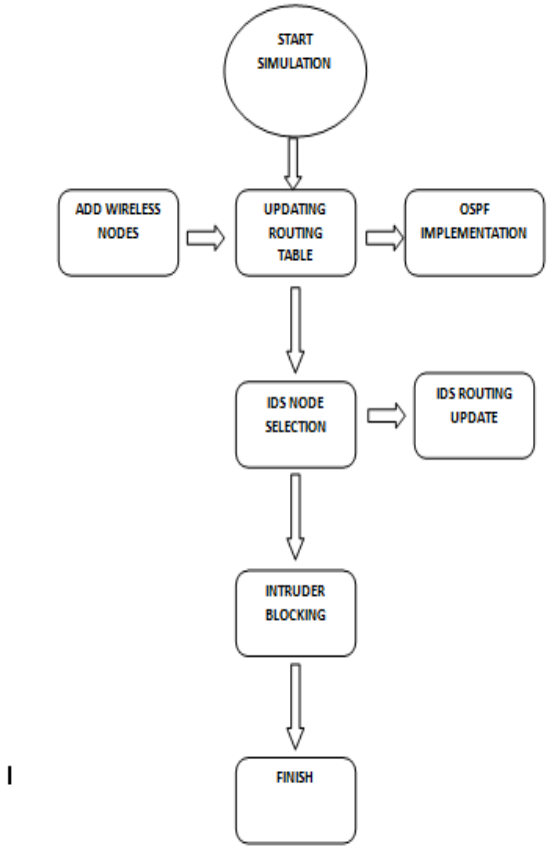

Fig 3: Flow Chart

7.1 Hardware requirements

- Processor - Pentium –IV
- Speed - 1.1 GHz
- RAM - 512 MB (min)
- Hard Disk - 40 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LCD/ LED

7.2 Software Requirements

- Operating system: Windows XP.
- Tool: NS2

Fig 4 shows the basic topology of Ad-hoc Network, in ad-hoc network nodes are ready to boot up and to send updates handshaking signals to each other. Fig 5 shows update signal transmission between wireless mobile ad-hoc nodes, synchronization process of wireless network. Fig 6 shows the analysis of attacks and combative attacks result.

Table 1: Simulation parameters

Simulation Parameters	
Protocols	OSPF, Modified OSPF
Simulation Time	100s
No. of Nodes	10
Dimension of simulated area	800×600
Speed	30 m/s
Mobility Model	Random Waypoint
Traffic Type	Constant Bit Rate (CBR)
Packet Size	1000 bytes
Pause Time	10-100s
No. of connections	10

8. RESULT ANDCONCLUSION

After simulation work and implementation of IDS, we found higher performance of mobile ad-hoc network and extremely less packet dropouts. This method increased routing performance and diminished routing load, and additionally helps to notice persona non grata for mobile ad-hoc network. We highlighted the importance on planning applicable intrusion detection systems to combat attacks against psychological feature radio networks. Also, we tend to projected easy nonetheless effective IDS, which might be simply enforced within the secondary users' psychological feature radio code.

Our projected IDS uses non-parametric consume algorithmic program, which offers anomaly detection. By learning the traditional mode of operations and system parameters of a CRN, the projected IDS is in a position to notice suspicious (i.e., abnormal or abnormal) behavior arising from associate attack. Specifically, we tend to bestowed associate example of a jam attack against a CRN secondary user and incontestable.

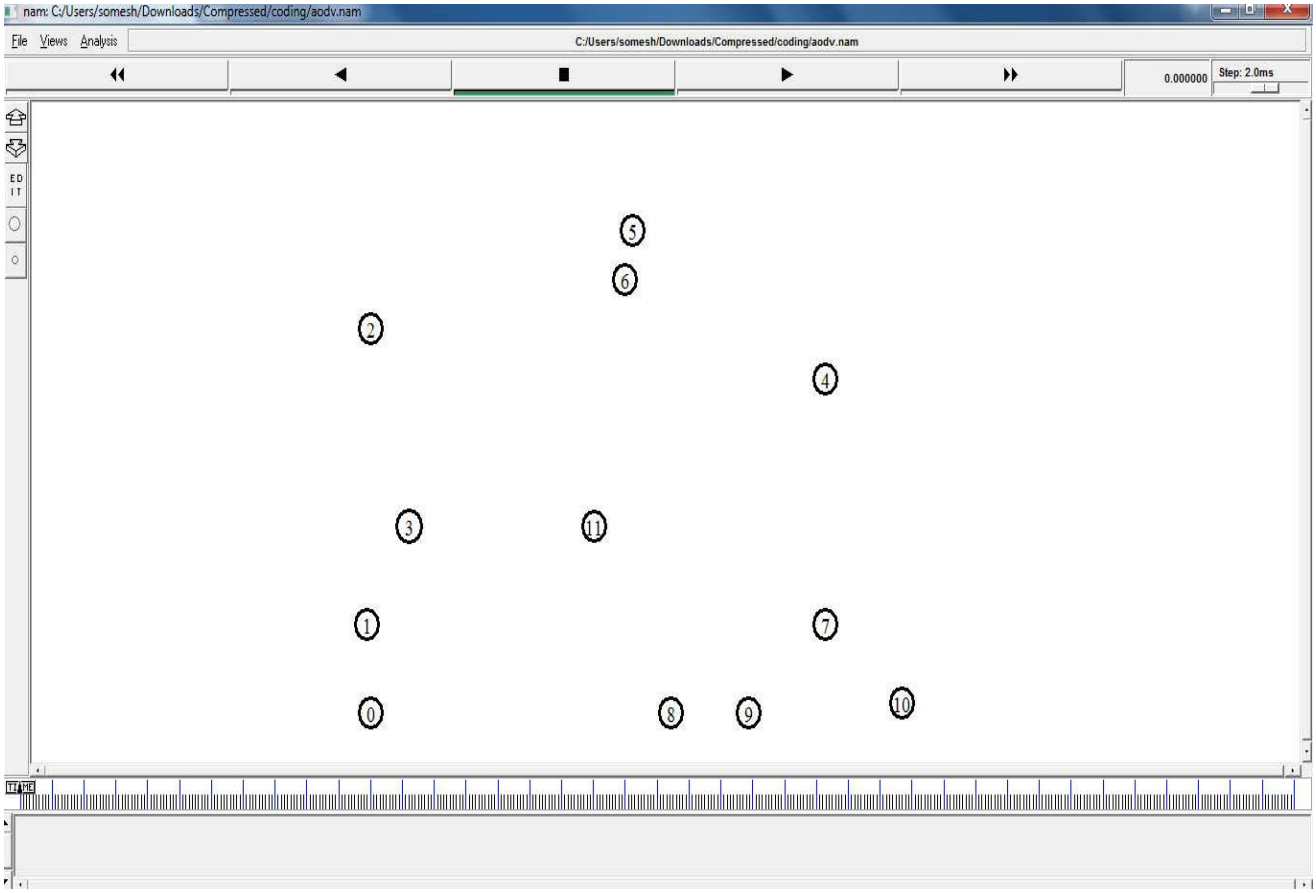

Fig 4: Topology of inactive mobile ad-hoc network

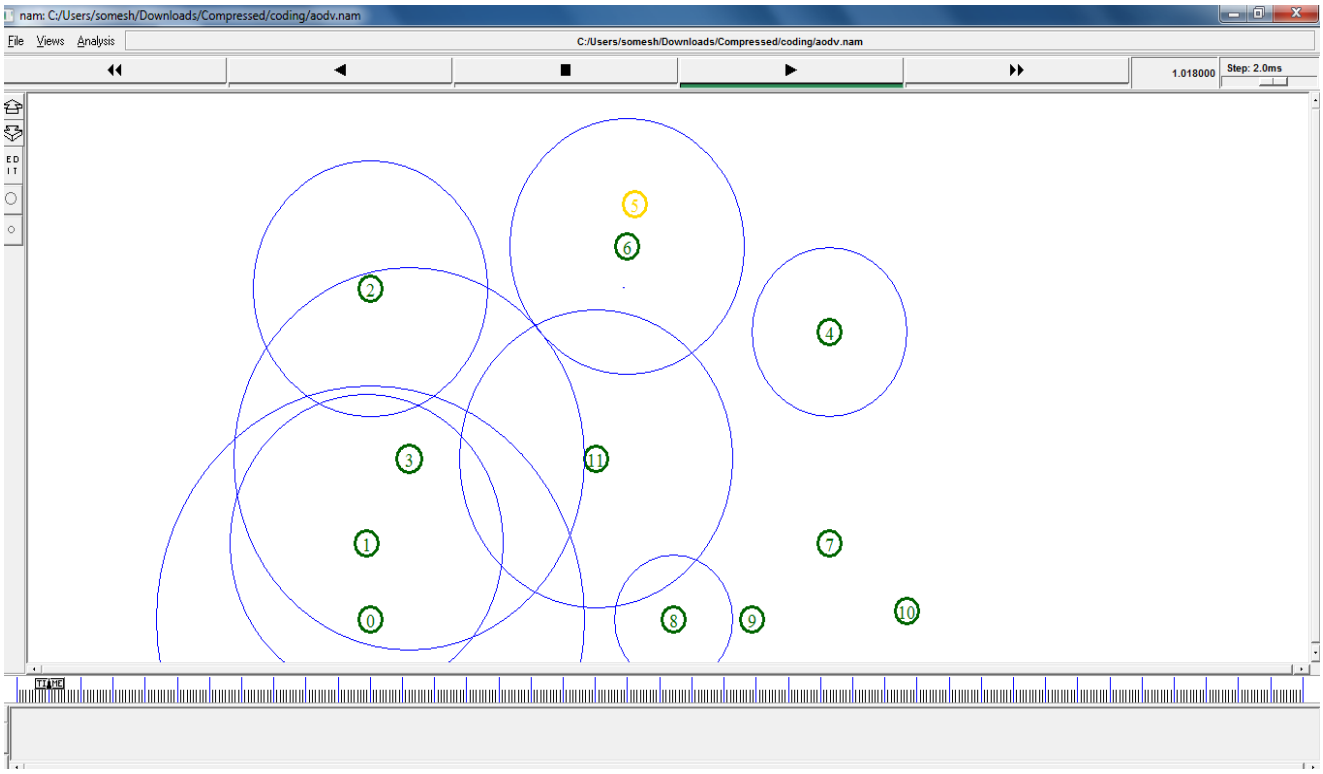

Fig 5: Topology updating and Packet delivery system in mobile Ad-hoc Network

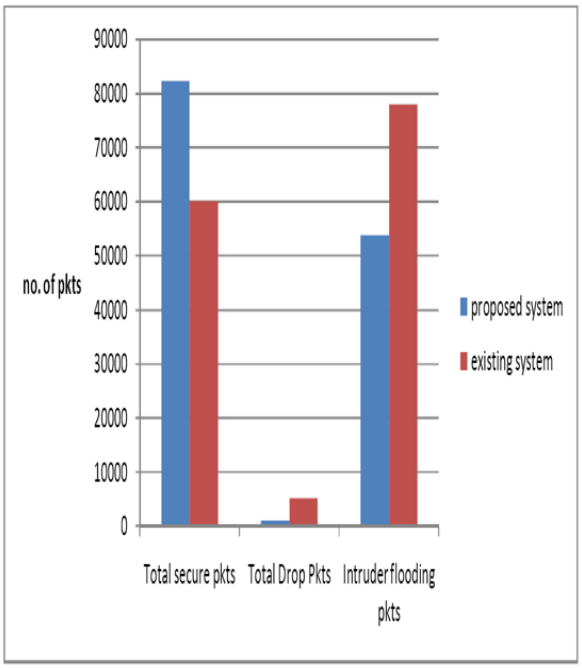

Fig 6: Result analyzes graph

In this work, we worked on intrusion detection system in mobile ad-hoc network by doing necessary changes in OSPF routing protocol for higher performance, result and security considerations. After simulation work and implementation of IDS, we found higher performance of mobile ad-hoc network and extremely less packet dropouts. This method increased routing performance and diminished routing load, and additionally helps to notice persona non grata for mobile ad-hoc network.

Table 2: Comparison between previous & proposed system

S. No.	Parameters	Previous System	Proposed System
1	Number of secure packets transmitted	60056	82351
2	Number of dropped packets	5097	1108
3	Number of intruder flooding packets	78041	53771

9. FUTURE SCOPE

In future we are able to improve this work as persona non grata block or jam system for combating attacks and may additionally follow persona non grata block system mechanisms for work sweetening. In future, this work can be performed additional investigations on a way to enhance the detection sensitivity of the IDS.

10. REFERENCES

[1] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "An Intrusion Detection System (IDS) For Combating Attacks Against cognitive Radio Network," IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May 2013.

[2] Mostafa M. Fouda, Tohoku University and Benha University"An Intrusion Detection System (IDS) For Combating Attacks Against cognitive Radio Network," IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, June 2013".

[3] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," Journal of Communications, vol. 1, no. 1, pp. 38-47, Apr. 2006.

[4] O. Leon, R. Roman, and J. H. Serrano, "Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks", in Procw Orkshopon Wireless Cooperative Network Security (WCNS'11), Valencia, Spain, May 2011.

[5] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing cognitive radio networks", in International Journal of Communication Systems, vol. 23, no. 5, pp. 633-652, May 2010.

[6] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology (JIT), vol. 12, no. 2, pp.181-198, Mar. 2011.

[7] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto,"Detecting Blackhole Attack on OSPF-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol. 5, No. 3, pp. 338-346, Nov. 2007.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, vol. 14, no. 5, 85-91, Oct. 2007.

[9] Z. M. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," IEEE/ACM Transactions on Networking, vol. 18, no. 4, pp. 1234-1247, Aug. 2010.

[10] K. Ju and K. Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," International Journal of Security and Its Applications, vol. 6, no. 2, pp. 149-154, Apr. 2012.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proc. ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), Urbana-Champaign, Illinois, USA, May 2005.

[12] H. Wang, D. Zhang, and K. G. Shin, "Change-Point Monitoring for Detection of DoS Attacks," IEEE Trans. on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208, Oct. 2004.

[13] Jangkyu Yun, Seungyong Oh, Junhyung Kim, Sukgyu Lee, Kijun Han "An Implementation of OSPF Routing Protocol withMulti-Metrics" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 2010.

[14] Sethi and Udgata,"Optimized and Reliable Ad hoc On-demand Distance Vector (OROSPF)" International Journal of Computer Applications(0975-8887)Volume3-No.10,July 2010.

[15] Kowshika , Maheswari, karthik "an efficient packet forwarding in MANET with OSPF using random way

point mobility model" journal of mathematics and technology, issn: 2078-0257, no.3, august, 2010.

[16] J.Premalatha, P.Balasubramanie, Enhancing Quality of Service in MANETS by Effective Routing, IEEE. ICWCSC 2010.

[17] Li Yuanzhou, Hu Weihua, Optimization Strategy for Mobile Ad Hoc Network Based on OSPF Routing Protocol, IEEE. 978-1-4244-3709-2/10,2010

[18] C.E. Perkins, E.M. Belding-Royer, and I.D. Chakeres "Ad Hoc on Demand Distance Vector (OSPF) Routing" IETF Internet draft, Oct. 2003.

[19] Parma Nand, S.C. Sharma, Rani Astya,Simulation Based Parametric Analysis of OSPF Protocol for Ad-hoc Network Published in International Journal of Advanced Engineering & Applications,Jan. 2010

11. AUTHOR PROFILE

Mrs. Arjita Singh Sengar has received her Engineering degree in Electronics & Communication on June 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India and currently pursuing Master of Technology degree in Digital Communication from Technocrats Institute of Technology- Advance under Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India.

Prof. Pankaj Soni has received his Engineering degree in June 2008 and Master of Technology degree in Dec 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India. He is currently working as Professor in department of Electronics & Communication in Technocrats Institute of Technology- Advance, Bhopal, (M.P.) India. He has five years teaching experience. His research interest is in Digital Communication, Wireless Communication and VLSI Design.