Protect the AODV Protocol with Secure Routing Information Protocol from Gray Hole Attack

[1]Niharika Sood, [2]Er.Rasbir Singh

1M.Tech, Department of Computer Engineering, RIMT university, MGG

Sood.niharika3@gmail.com

2Assistant Professor, Department of Computer Engineering, RIMT university , MGG

Rasbir.rai@gmail.com

Abstract-Today MANETs has reached to its pinnacle, as the demand for the MANETs are increasing day by day. Due to the increasing demand for MANETs in various areas such as in Military operations, in flood affected areas etc., threat of security has also increased. MANETs has no protection from harms, so information can be accessed by both authorized network users and catty attackers as MANETs don't have centralized administration. In the presence of catty nodes, the main problem in MANETs is to design the rich security solution that can protect MANETs from various routing attacks. Flooding attack is kind of the security threat in which source node sends huge amount of data, Root Request (RREQ) and Sync packet to destination node, due to which the receiver shall not work properly as it would be engaged in receiving the excessive amount of data, RREQ and Sync packets from the attacker. In this paper we apply Gray hole attack on MANET & check the performance of the network after then we apply routing information protocol on the network to increase the performance of the network.

Index Terms: MANET, Routing Protocol, Security, Attacks.

Introduction:

MANET is an infrastructure less network which is established automatically on demand. It is a set of wireless nodes that are configured automatically on the fly thus making it suitable candidate as it is useful in emergency situations, as shown in fig. 1 [1], [2]. In other words it is a multi-hop communication network organized temporarily with nodes that have receivers and transmitters [3]. The topology of network is dynamic which is created and modified on the fly [4]. MANET supports many routing protocols such as Dynamic MANET On-demand routing protocol (DYMO), Optimized Link State Routing protocol (OLSR), Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) and Ad Hoc On-demand Vector Routing (AODV). Mobility is the fundamental difference between other networks and MANET [5]. Wireless Sensor Network (WSN) traffic also can be relayed over MANET. It does mean that WSN communications are possible between devices of MANET [6]. MANET supports TCP/IP protocol to integrate communication with wired networks as well [1]. Every node in MANET acts as a host in the network and also router which can cooperate in communication [7]. As MANET topology is dynamic in nature which makes the procedure of routing more difficult and vulnerable to Denial of Service (DoS) attacks such as flooding which results in network congestion [8]. MANETs are vulnerable to attacks such as location disclosure, black hole, replay, worm hole, blackmail, Denial of Service and routing table poisoning.

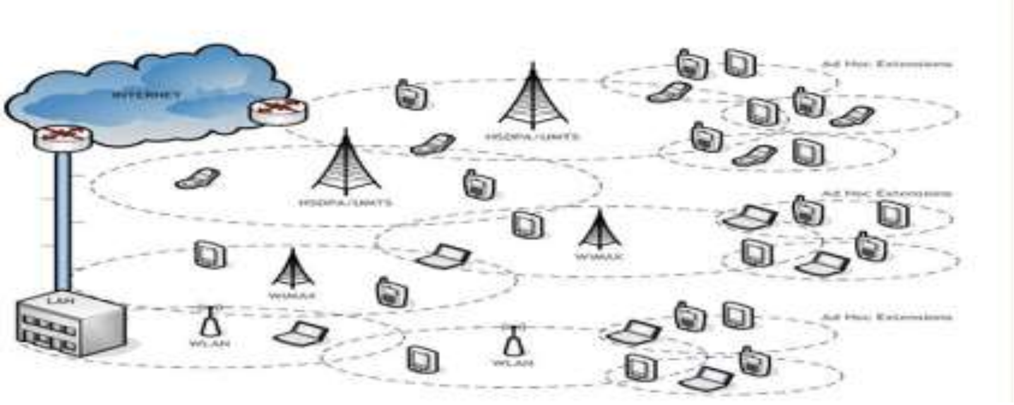

Fig 1: MANET Network

Routing Protocols:
There are three types of routing protocols:
[1] Reactive routing protocol.
[2] Proactive routing protocol.
[3] Hybrid routing protocol.

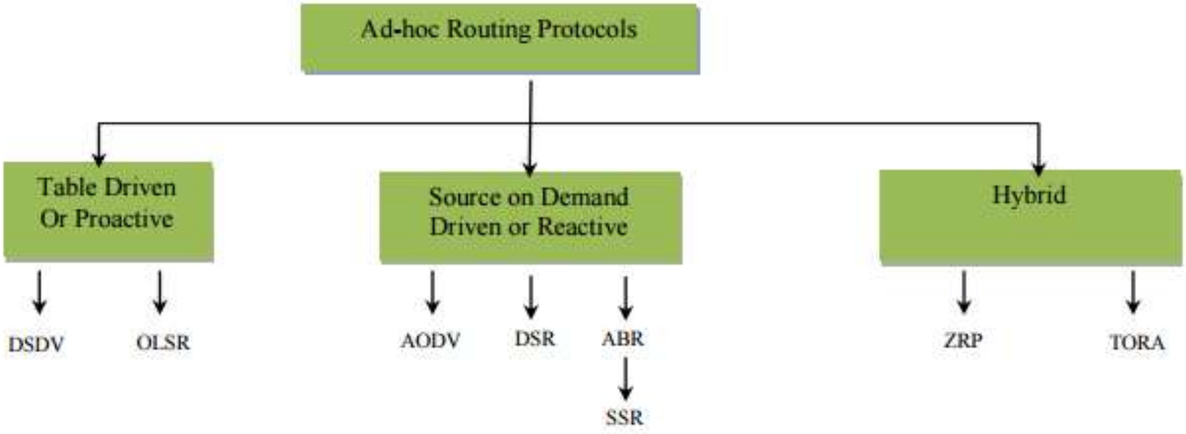
Ad-hoc Routing Protocols
Table Driven Or Proactive
Source on Demand Driven or Reactive
Hybrid
DSDV
OLSR
AODV
DSR
ABR
SSR
ZRP
TORA

Fig 2: Hierarchy of MANET Routing Protocols

Reactive Routing Protocols: Reactive protocols tend to decrease the control traffic messages overhead at the cost of increased latency in discover a new routes. Source initiated route discovery in reactive routing protocols and less delay. In reactive protocols there is no need of distribution of information [5]. It consumes bandwidth when data transfers from source to destination. Reactive Protocols are AODV (Ad-hoc On Demand Distance Vector), DSR (Distance Vector Routing) and ABR (Associativity Based Routing). MANET is also called Mesh network. It is highly adaptable and rapidly deployable network. MANET has a dynamic topology [11] [12] [13].

	Protocol Property	**Reactive**
S.No.	**Protocol Name**	**AODV**
1	Complexity	Average
2	Route	Dynamic
3	Memory Size	Low
4	Bandwidth	Maximum
5	Topology Size	Large
6	Convergence Time	Mostly Fast
7	Mission Failure	Low

Table 1: Comparison of Routing Protocols

AODV: AODV adopts traditional routing tables; one entry per destination which is in contrast to DSR that maintains multiple route cache entries for each destination. The initial design of AODV is undertaken after the experience with DSDV routing algorithm. Like DSDV, AODV provides loop free routes while repairing link breakages but unlike DSDV, it doesn't require global periodic routing advertisements. Apart from reducing the number of broadcast resulting from a link break, AODV also has other Significant features. Whenever a route is available from source to destination, it does not add any overhead to the packets. However, route discovery process is only initiated when routes are not used and/or they expired and consequently discarded. This strategy reduces the effects of stale routes as well as the need for route maintenance for unused routes. Another distinguishing feature of AODV is the ability to provide unicast, multicast and broadcast communication. AODV uses a broadcast route discovery algorithm and then the unicast route reply massage. The following sections explain these mechanisms in more detail. [5]

Route Discovery: When a node wants to send a packet to some destination node and does not locate a valid route in its routing table for that destination; it initiates a route discovery process. Source node broadcasts a route request (RREQ) packet to its neighbors, which then forwards the request to their neighbors and so on. Fig. 2 indicates the broadcast of RREQ across the network. To control network-wide broadcasts of RREQ packets, the source node use an expanding ring search technique. In this technique, source node starts searching the destination using some initial time to live (TTL) value. If no reply is received within the discovery period, TTL value incremented by an increment value. This process will continue until the threshold value is reached. When an intermediate node forwards the RREQ, it records the address of the neighbor from which first packet of the broadcast is received, thereby establishing a reverse path. When the RREQ is received by a node that is either the destination node or an intermediate node with a fresh enough route to the destination, it replies by unicasting the route reply (RREP) towards the source node. As the RREP is routed back along the reverse path, intermediate nodes along this path set up forward path entries to the destination in its route table and when the RREP reaches the source node, a route from source to the destination established. Fig. 3 indicates the path of the RREP from the destination node to the source node.[5].

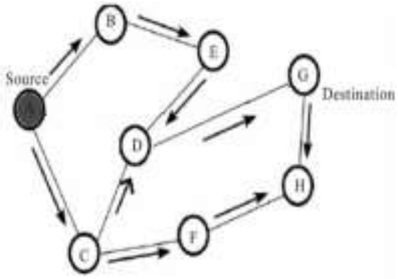

Fig 3: Propagation of Route Request

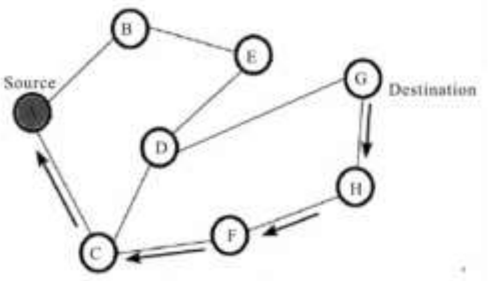

Fig 4: Route Reply

Route Maintenance: A route established between source and destination pair is maintained as long as needed by the source. If the source node moves during an active session, it can reinitiate route discovery to establish a new route to destination. However, if the destination or some intermediate node moves, the node upstream of the break remove the routing entry and send route error (RERR) message to the affected active upstream neighbors. These nodes in turn propagate the RERR to their precursor nodes, and so on until the source node is reached. The affected source node may then choose.

MANETs Routing Attacks: MANET is a collection of mobile nodes, sometimes nodes in MANET can be bad or malicious and these bad nodes cannot forward the packets due to their aim of conserving network resources such as band width, battery etc. by the denial of service. There are mainly two types of attacks in MANET. Active and Passive [9].

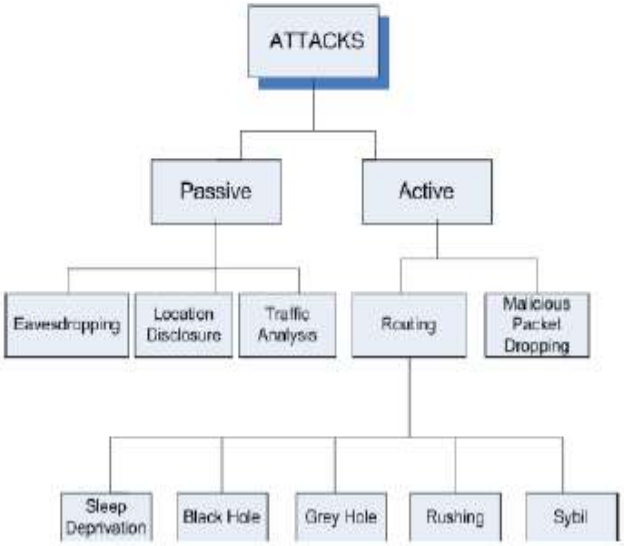

Fig 5: Attacks in MANET

Gray-hole attack:

A gray-hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Here, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication. Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. The complete phenomena create toughness against detection and prevention mechanism because nodes can drop packets partially not only due to its malicious nature but also due to overload,
Congestion or selfish nature.

Security Protocols:

Routing Information Protocol: The Routing Information Protocol (RIP) [16][19][21][22] is a distance-vector protocol that uses hop count as its metric. The Routing Information Protocol (RIP) provides the standard IGP protocol for local area networks, and provides great network stability, guaranteeing that if one network connection goes down the network can quickly adapt to send packets through another connection. It is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system. RIP itself evolved as an Internet routing protocol, and other protocol suites use modified versions of RIP. IP RIP is formally defined in two documents: Request For Comments (RFC) 1058 and 1723. RFC 1058 (1988) describes the first implementation of RIP, while RFC 1723 (1994) updates RFC 1058. RFC 1058 enables RIP messages to carry more information and security features.

Simulation: We have created a network with AODV protocol in OPNET & checked that how gray hole attack affects the AODV protocol. In this, we create 3 scenarios; in the first scenario we create MANET Network with AODV protocol & in the second scenario we apply gray hole attack on the network and in the last scenario we apply security Routing information protocol in the MANET . After that we compare the performance of all the three scenarios & check the performance of the network.

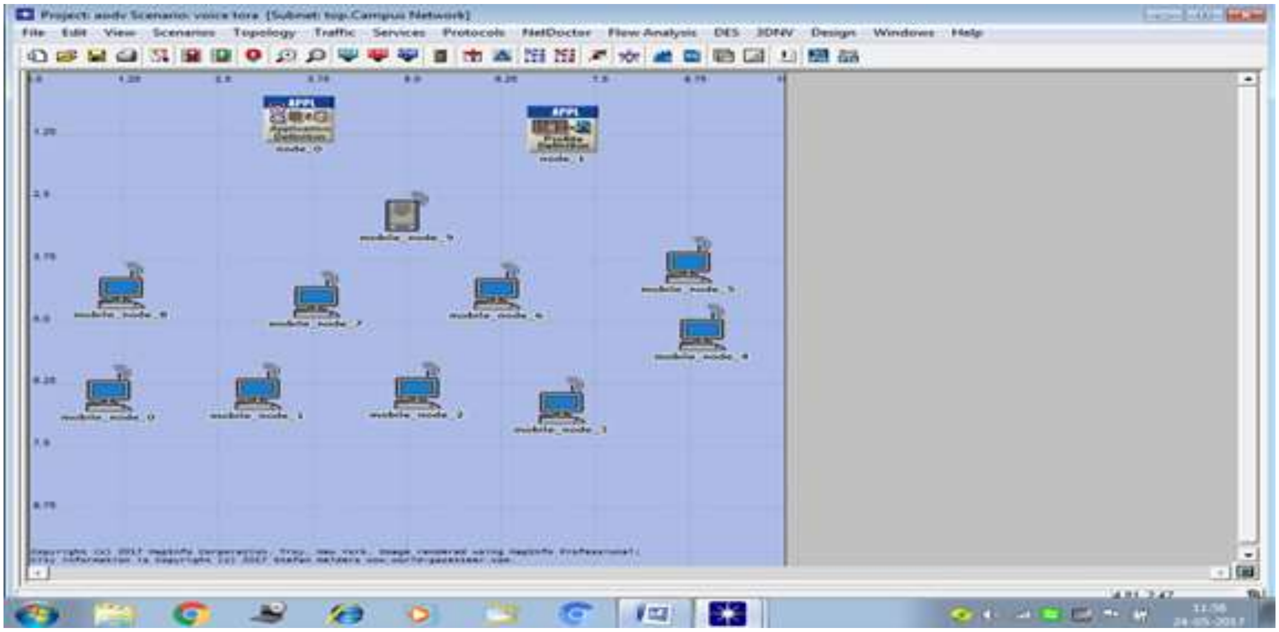

Fig 6: MANET Network

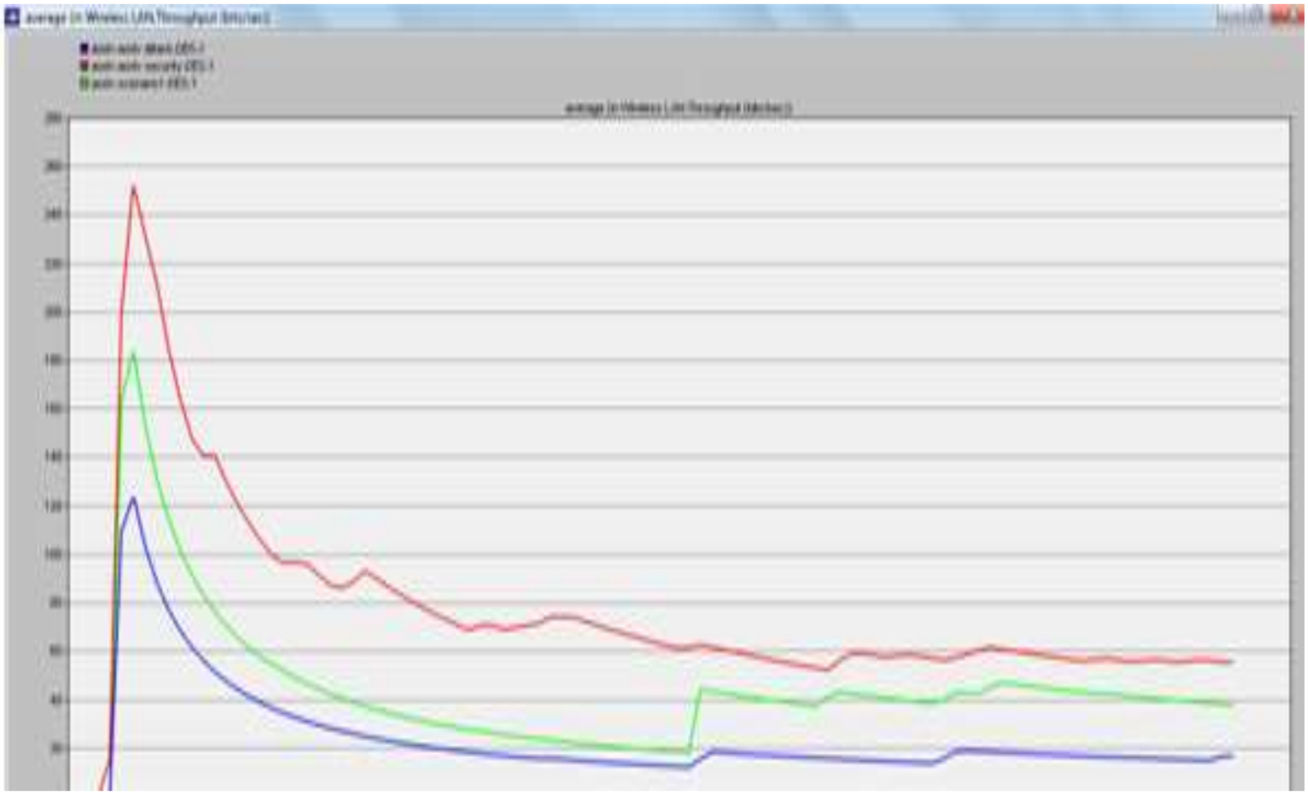

Fig 7: Throughput of Network

As shown in the above fig 7: we see that with the Routing information protocol the Network performance increases to 60 b/s when we apply attack on MANET then it decrease to 20 b/s. The normal performance of the network is 40b/s.

Conclusion: The future of ad- hoc networks is really appealing, giving the vision of ―anytime, anywhere‖ and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. In this paper we see that how gray hole attack effect the MANET network Reduce the Performance of the network. After that when we apply a routing information Protocol the Network Performance increases. Further we apply various Protection schemes to protect the MANET Network

References:

[1]. Pratap K. Meher and P. J. Kulkarni Analysis and Comparison of Performance of TCP-Vegas in MANET. IEEE, 2011, pp.67-70.

[2] Dinesh Singh, Ashish K. Maurya, Anil K. Sarje. Comparative Performance Analysis of LANMAR, LAR1, DYMO and ZRP Routing Protocols in MANET using Random Waypoint Mobility Model. IEEE. 2011. pp62-66.

[3] Xia Wen-jie, Yan Han and Liu Feng-yu. The analysis of M/M/1 queue model with N policy for damaged nodes in MANET. IEEE. 2011. pp289-294.

[4] Sudharson Kumar and Parthipan.V. SOPE: Self-Organized Protocol for Evaluating Trust in MANET using Eigen Trust Algorithm.IEEE. 2011. pp155-159.

[5] FahimMaan, NaumanMazhar. MANET Routing Protocols vs Mobility Models: A Performance Evaluation. IEEE. 2011, pp179-184.

[6] Giuseppe Cardone, Antonio Corradi, Luca Foschini. Reliable Communication for Mobile MANET-WSN Scenarios. IEEE. 2011, pp1085-1091.

[7] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen. CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture. IEEE. 2011, pp1-5.

[8]. Alokpara Band yopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury., Simulation Analysis of Flooding Attack in MANET using NS-3. IEEE. 2011, pp1-5.

[9] Adnan Nadeem member IEEE and Michael P.Howarth, "A Survey of MANET Intrusion
Detection & Prevention Approaches for Network Layer Attacks", Communication survey Tutorials, IEEE Volume: 15, Issue: 4, 2013.

[10] Behrouz A Forouzan, Data Communications and Networking‖, Special Indian Forth Edition, 2006

[11] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and Devaraju J.T,"Scenario Based Study of on demand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards", ISSN: 2249-57 Vol 1(2), Oct-Nov 2011, pp.128-135

[12] Naveen Bilandi and Harsh K Verma, "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET", International Journal of Electronics and Computer Science Engineering 1660 ISSN- 2277-1956.

[13] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad-hoc Networks: A Survey", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[14] Sinem Coleri, Ergen, ZigBee IEEE 802.15.4‖. LAN-MAN Standards Committee of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification, IEEE, New York, NY, USA, IEEE Std802.11-1997 edition,1997 .Wireless Communication, Sept 10, 2004 pp. 35 – 54, ISBN 9781420045474.

[15].Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks" ,Tseng et al. Human centric Computing and Information Sciences 2011, a Springer open journal.

[16] Wu, Bing, "Simulation Based Performance Analyses on RIP, EIGRP and OSPF Using OPNET"

[17] Vishal sharma, Rajneesh Narula and Sameer khullar "Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols" International Journal of Computer Applications (0975 – 8887) Volume 44– No13, April 2012

[18] Ittiphon krinpayorm and Suwat Pattaramalai,"Link Recovery Comparison Between OSPF & EIGRP ", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012).

[19] Mr. R. M. Pethe, Miss S. R .Burnase technical era language of the networking - EIGRP International Journal of Engineering Science and Technology (IJEST) NCICT Special Issue Feb 2011

[20] Mehboob Nazim Shehzad, Najam-Ul-Sahar, "Simulation of OSPF Routing Protocol Using OPNET Module"(A Routing Protocol Based on the Link-State Algorithm)

[21] Bernard Fortz, Jennifer Rexford and Mikkel Thorup., Traffic Engineering With Traditional IP Routing Protocols." IEEE Communications Magazine. October 2002, pp. 118-124.

[22] Ahmad Karim, Minhaj Ahmad Khan "Behaviour of Routing Protocols for Medium to Large Scale Networks", Australian Journal of Basic and Applied Sciences, 5(6):, 2011,pp1605-1613.

[23] Amandeep Singh, Amandeep Singh Bhandari, "To evaluate and improve TDMA based MAC protocol for clock synchronization in WBAN", International Journal in Applied Studies and Production Management, IJASPM, Volume2, Issue 3, 15 May 2016- 15 August 2016, pp. 32-41

[24] Arjun Kumar, Amandeep Singh Bhandari, "Symbol Detection in MIMO Systems Using PSOGSA Optimization Algorithm", International Journal of Research, IJR, e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015, pp. 801-808.

[25] Amandeep Singh Bhandari, Charanjit Singh, "Performance Analysis of Cyclostationary Spectrum Sensing Over Different Fading Channels", International Journal of Computer Applications (0975 – 8887) Volume

129 – No.1, November2015, pp. 27-31.

[26] Sehleen Kaur, Amandeep Singh Bhandari, “Frequency estimation of ECG signals using FIR filter”, International Journal of Research, IJR, e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015, pp. 786-793.

[27] Khera, Ishan, and Ajay Kakkar. "Comparative study of scheduling algorithms for real time environment." International journal of computer applications 44, no. 2 (2012): 5-8.

[28] Kakkar, Ajay, M. L. Singh, and P. K. Bansal. "Dynamic Path Management Scheme for Multinode Network", International Journal of Communication Engineering Applications-IJCEA, Vol 02, Issue 03; July 2011, pp: 117-122.

[29] Sharma, Amandeep, Ajay Kakkar, and Sandeep Sachdeva. "Optimized WDM network with consideration of lesser blocking probability & shortest path selection." In Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on, pp. 1-6. IEEE, 2012.