International Journal of Computer Applications (0975 – 8887)
Volume 77 – No.11, September 2013

An Approach to Combat the Blackhole Attack in AODV Routing Protocol

Rohit Pal[1], Mukesh Azad[1], Santosh kumar[2]

ABSTRACT
This article consists of a brief description of various issues on security of Ad hoc networks as well as counter work against Black Hole Attack. A Combat Approach against Black Hole Attack is truly based on Cooperation of individual nodes of MANET. In this Approach each individual node act as *intrusion detection system* and monitors each request that it receives to avoid the attack. For this we use the routing table as well as to authenticate the sender node. We use ns2 for implementation and to simulate the proposed algorithm.

Keywords
Wireless Network, Ad hoc Network, Security Service, Routing Protocols, Routing Authentication, Hash function and Secure Routing Protocols, Attacks, Secure Routing Protocol

1. INTRODUCTION
Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily [3]. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system [1]. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible Technology for establishing communications in situations which demand a fully decentralized Network without any fixed base stations, such as battlefields, military applications, and other Emergency and disaster situations Since, all nodes are mobile, the network topology of a MANET is generally dynamic and may change frequently.

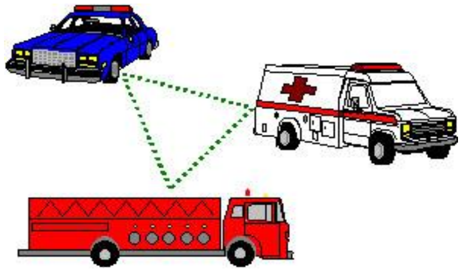

Fig: Ad hoc network in emergency[2]

Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, direct single-hop transmissions between two hosts can require significant power, causing interference with other such transmissions.

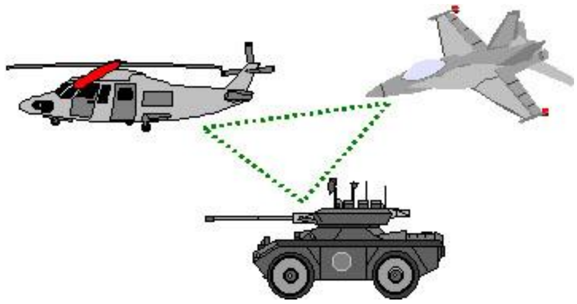

Fig: Ad hoc network in war[2]

Figure 1 and Figure 2 shows three nodes where ad hoc network where every node is connected to wireless, and work as access point to forward and receive data.

2. OVERVIEW OF MANET ROUTING PROTOCOLS
Routing Protocols are classified into following three categories:

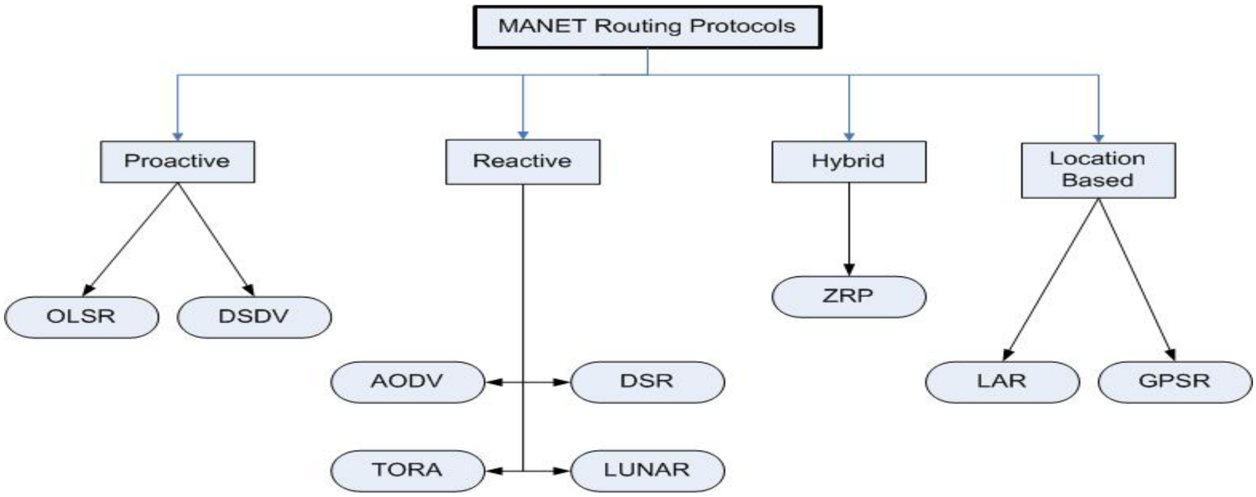

Fig: Classification of MANET Routing Protocols[2]

2.1 Proactive Routing Protocol

A Proactive (Table-driven) Routing Protocol attempts to allow each node using it to always maintain an up-to-date route to each possible destination in the networks, the protocol periodically exchanges routing information with other nodes in order to allow new route to be discovered and existing route to be modified if they break due to factors such as node mobility and environmental changes [2].

2.2 Reactive Routing Protocol

A Reactive (On Demand) Routing Protocol only attempts to a discover a route to some destination when it has a packet to route to some destination when it has a packet route to that destination and does not already know a route there; the protocol catches known routes and uses a flooding based discovery protocol when a needed route is not found in the cache [2, 20].

3. SECURITY ATTACK & CHALLENGES

We have to consider external as well as internal attack on MANET. The nature of wireless ad hoc networks makes them very vulnerable to attack. First of all, the mobile nodes are independent and their movements are not controlled by the system, so they can easily be captured, compromised and hijacked. Secondly, since in wireless networks there are no physical obstacles for the adversary, attacks can come from all directions and target any node. Third, in wireless ad hoc networks adversaries can exploit the decentralized management for new types of attack designed to break the cooperative algorithms. Thus following are the ways by which security can be breached [2, 5].

Table I describes various Routing Attack at NETWORK Layer for MANET. In this article Black Hole attack is focus for Combat Approach.

TABLE I Various Routing Attacks with brief description

S. No	Routing Attack	Brief Description
1	**Location Disclosure**	Location disclosure is an attack that targets the privacy requirements of an ad hoc network [9].
2	**Black Hole**	Malicious node injects false route replies to the route requests it receives, broadcasting itself as having the shortest path to a destination.[10]
3	**Replay**	An attacker that performs a replay attack injects into the network routing traffic that has been captured previously [9].
4	**Wormhole**	The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [11].
5	**Blackmail**	This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [12].
6	**Denial of Service**	Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [12].
7	**Routing Table Poisoning**	In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [14].
8	**Rushing Attack**	Rushing attack is the results in DoS when it used against all previous AODV routing protocols [14, 13].

9	**Masquerading**	During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system [12].
10	**Passive Listening and traffic analysis**	The intruder could passively gather exposed routing information. Such a attack can not affect the operation of routing protocol, but it is a breach of user trust to routing the protocol [13].

4. SECURITY SOLUTIONS FOR MANET

In a secure wireless ad hoc sensor network, a node is authorized by the network and only authorized nodes are allowed to access the network resources. The generic process to establish such a network consists of bootstrapping, pre-authentication, network security association establishment, authentication, and behavior monitoring and security association revocation. Among these, authentication is of the utmost importance and is an essential service in network security. Other basic security services like confidentiality, integrity and non-repudiation depend on authentication. The main requirements of a routing protocol are quick convergence, scalability, consistency, robustness etc. Additionally to provide extra security guarantees, the routing protocol should also provide, amongst other things, Data Integrity, Origin Authenticity, Non-Repudiation, Timeliness and Ordering. Various solutions have been proposed in literature to deal with many of these security problems. All the schemes can be broadly categorized into the following three groups based on their functionality.

- *Routing Information Technique:* In these techniques, digital signatures are used to provide Origin authenticity and to an extent data integrity also by having the sender signs the routing messages. This can protect against modified or fabricated routing messages and enables attack detection due to subverted links but not due to subverted routers themselves [2].
- *Routing Protocol Techniques:* Several changes have been proposed to the routing protocols and Messaging formats to provide additional security benefits. These methods help in preventing looping, malicious distance vector updates cannot be detected using these techniques. Sequence Numbers are used in along with the routing messages to protect against replay attacks and also to provide orderliness and detection of lost routing messages. But it does not provide any other security guarantees [2].
- *Intrusion Detection Techniques:* These techniques are used to detect anomalous behavior in the routers, assuming that intrusion detection devices are available in the network.

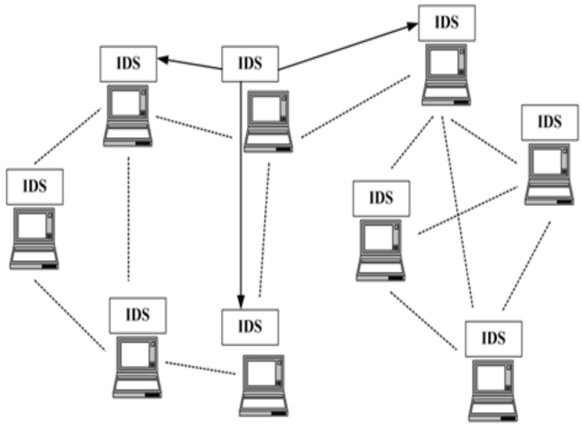

Fig: IDS Architecture[1]

But the problems associated with these schemes are precise characterization of what exactly constitutes anomalous behavior, as subtle changes made over time could possibly bypass these filters. Also these mechanisms only help in identifying the anomalous behavior but cannot avoid the attack [2].

5. COMPARISON OF PREVIOUS WORK AGAINST BLACKHOLE ATTACK

Black Hole attack always attract researcher for its scope as well as potential challenges of cope up MANET Protocol. In Table II summarized in brief previous work done against Black Hole Attack.

Table II Comparison of work against Black Hole Attack

Schemes Against Black Hole	Routing protocol	Simulator Used	Year of Publication	First Author's Name	Results	Defects	Citation
DRI and cross checking	AODV	No simulator	2003	Ramaswamy S	No simulation results	-	[15]
DRI table and cross checking using FREQ and FREP	AODV	-	2007	Weerasinghe H	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route request	[16]
DCM	AODV	NS-2	2007	Yu CW, Wu T-K	The PDR is improved from 64.14 to 92.93% and the detection rate is higher than 98%	A higher control overhead than AODV	[17]
Hash based	DSR	-	2009	Wang W	No simulation results	-	[18]
MAC and Hash	AODV	NS-2	2009	Min Z	The PDR is higher	The malicious node is	[19]

based PRF scheme					than 90% when AODV is inaccessible 50%	able to forge a reply to dodge the detection scheme	
BBN and RIP	AODV	-	2010	Vishnu KA	No simulation results	-	[20]
BDSR	DSR	QualNET	2011	Tsou P-C	The PDR of BDSR is always higher than 90%	The overhead is minimal higher than DSR, but lower than WD approach	[21]

6. COMBAT APPROACH AGAINST BLACK HOLE ATTACK

To protect MANETs from outside attacks, the routing protocols must fulfill certain set of requirements to guarantee the correct functioning of all the paths from source to destination. These are:

- Only the authorized nodes shall be able to execute route discovery processes
- Negligible exposure of network topology
- Early detection of distorted routing messages
- Avoiding formation of loops
- Avert redirection of data from broken paths

For this purpose to protect against Black Hole Attack we have to cross check shortest as well as fresh path for destination by IDS. Table III shows all technical aspect of combat approach.

Table III Algorithm for implementing proposed intrusion detection system [1]

1	Source node broadcasts RREQ to neighbors
2	Source node waits till it receives RREP from its all neighbors
3	Source node selects shortest and next shortest path based on timestamp and the no. of hops
4	Source node checks its routing table for single hop neighboring nodes only
5	If the neighbor node is in its routing table then route data packet. Else the node is malicious with count 1 and sends false packets to that node
6	Invoke the route discovery. Inform all the neighboring nodes about the stranger
7	Add the status of stranger to the routing table of source node
8	Again send packet to neighboring nodes
9	If step 5 repeats then broadcast the malicious node as black hole
10	Update the routing table of the source node after every broadcast
11	Repeat step 4 to 10 until packet reaches the destination node correctly

7. SIMULATION ENVIRONMENT

For simulation, we set the parameter as shown in Table IV. Random Waypoint Model (RWP) [1] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destination with a random velocity.

Table IV Simulation Parameters

Parameters	**Values**
Simulation Time	500 (s)
Number of Mobile Nodes	20
Topology	1600 *1600 (M)
Routing Protocol	AODV and IDSAODV
Traffic	Constant Bit Rate (CBR)
No. of black hole nodes	1
Pause Time	10 (S)
Max Speed	20 (M/S)
Transmission range	250m
Observation parameters	PDR,Minimum,Maximum And Average Delay ,Throughput And Jitter
Data packet size	512 byte

8. SIMULATION RESULT

To analysis quality of service of Combat Approach against Black Hole attack, Static Scenario simulated with the help of NS2.35.

Figure 5 shows maximum delay under Black Hole attack with combat approach and without combat approach.

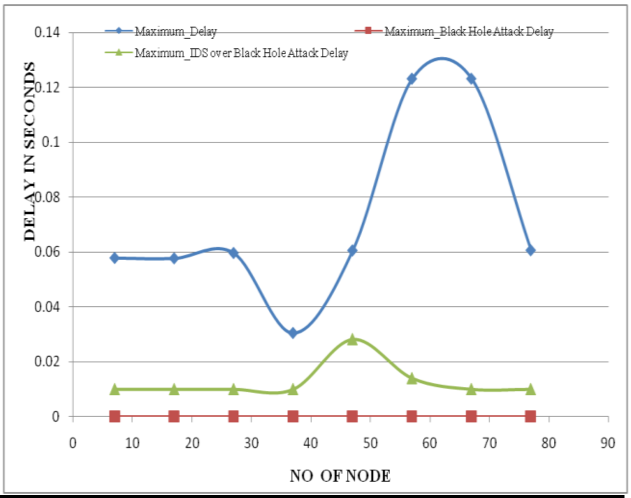

Fig: Maximum Delay VS. No Of Nodes

Figure 6 represents minimum delay under Black Hole attack with combat approach and without combat approach.

Fig: Minimum Delay VS. No Of Nodes

In Figure 7 Average delay under Black Hole attack with combat approach and without combat approach are shown.

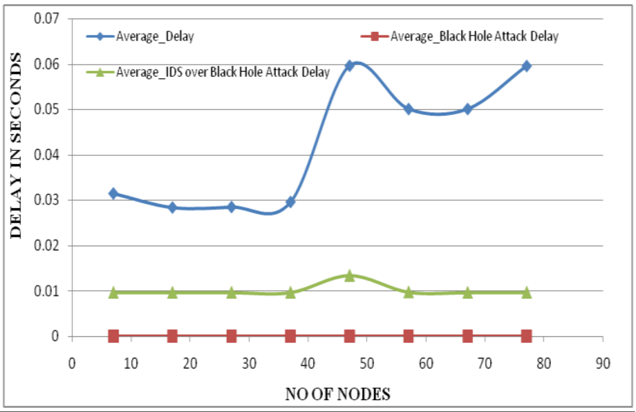

Fig: Average Delay VS. No Of Nodes

In Figure 8 minimum Jitter under Black Hole attack with combat approach and without combat approach are shown.

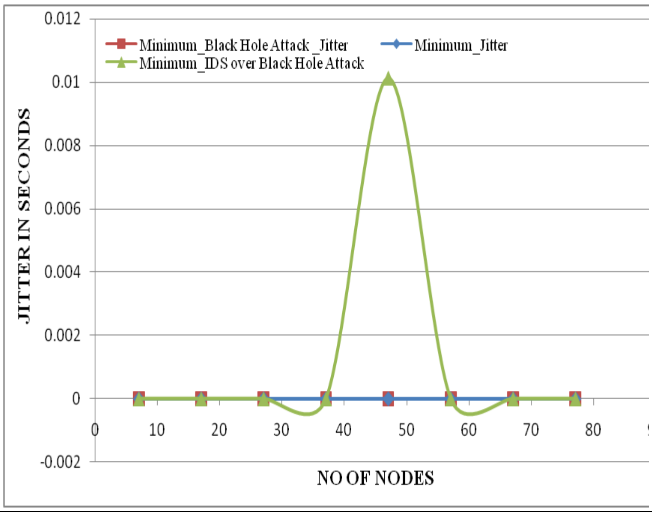

Fig: Minimum Jitter VS. No Of Nodes

Figure 9 represents maximum Jitter under Black Hole attack with combat approach and without combat approach.

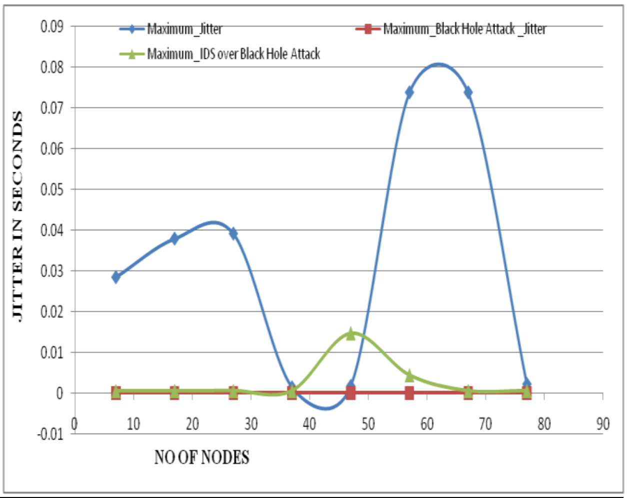

Fig: Maximum Jitter VS. No Of Nodes

In Figure 10 average Jitter under Black Hole attack with combat approach and without combat approach are shown.

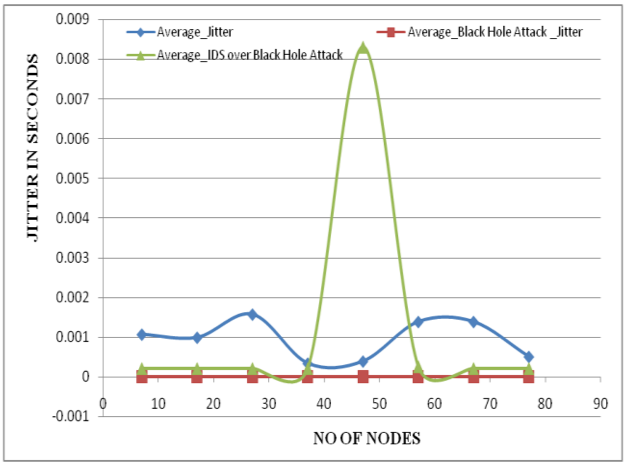

Fig: Average Jitter VS. No Of Nodes

Figure 11 represents minimum throughput under Black Hole attack with combat approach and without combat approach.

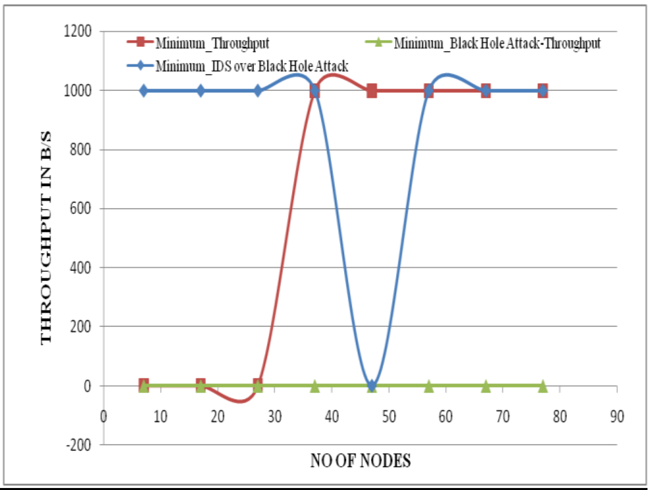

Fig: Minimum Throughput VS. No Of Nodes

In Figure 12 maximum throughput under Black Hole attack with combat approach and without combat approach are shown. In Figure 13 average throughput under Black Hole attack with combat approach and without combat approach are shown. Figure 14 represents packet drop ratio under Black Hole attack with combat approach and without combat approach.

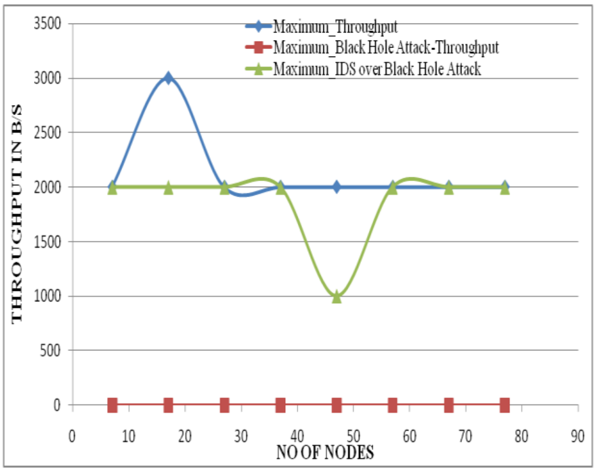

Fig: Maximum Throughput VS. No Of Nodes

Figure 15 represents packet drop ratio under Black Hole attack with combat approach and without combat approach.

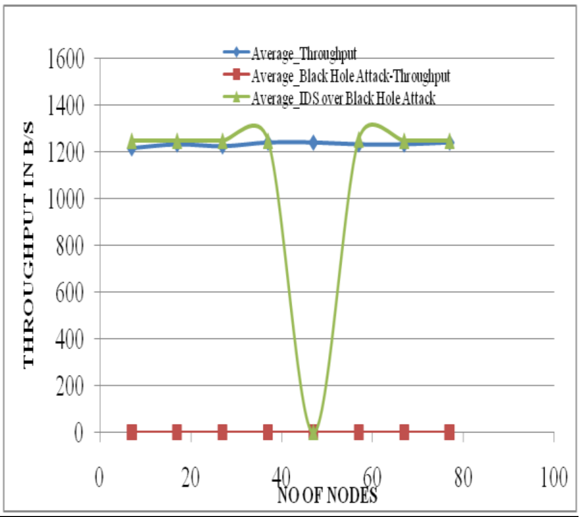

Fig: Average Throughput VS. No Of Nodes

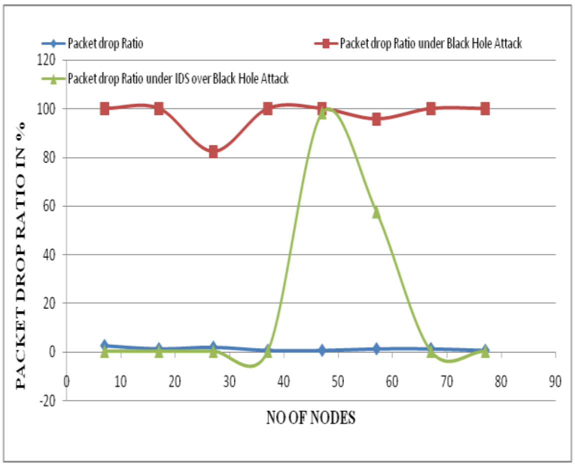

Fig: Packet Drop Ratio VS. No Of Nodes

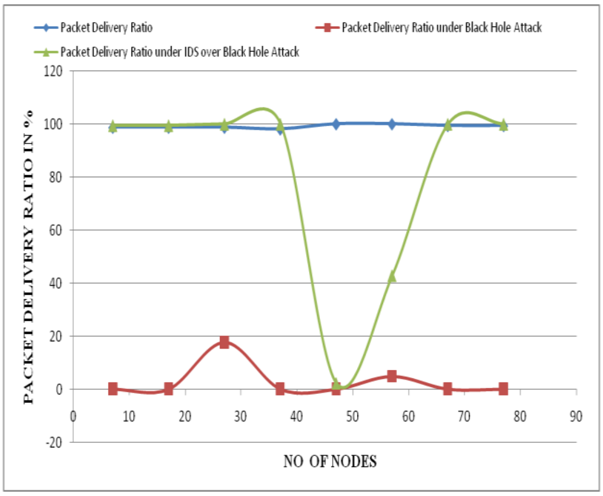

Fig: Packet Delivery Ratio VS. No Of Nodes

9. CONCLUSION

Mobile ad hoc networks present different threats and vulnerabilities due to their nature of openness and its various properties. These properties bring in various different security risks from conventional wired networks, and each of them affects and gives a challenge that how security is provided and maintained. All types of threats identified above give rise to different security requirements, several of which apply to ad hoc routing.

Any protocols and simulations to test them should include the capability to handle each type of node and hattack. In this paper, an attempt is made to discuss various attacks and vulnerabilities that exist in ad hoc networks with their techniques and solutions that how the security can be provided without hampering the performance of the network.

10. FUTURE WORK

It is demand of time that we have to implement secure reliable as well as efficient routing protocol which is capable enough to provide QOS without compromising security as well as high availability. We are more concern about enhancement of security in AODV. In future we simulate various cases with the help of NS2 and try to overcome possible threats.

11. REFERENCES

[1] Jaspal Kumar, M. Kulkarni, Daya Gupta," Effect of Black Hole Attack on MANET Routing Protocols" , I. J. Computer Network and Information Security,Volume-5,pp-64-72, April 2013

[2] Mukesh Azad, Rohit Pal, Jyoti Nautiyal, Mukesh Panday, Kuldeep Kumar ―Review of Emerging Threats, Vulnerabilities and Techniques of Security on Mobile Ad hoc Networks‖ UACEE International Journal of Advances in Computer Networks and its Security - Volume 2: Issue 3 [ISSN 2250 - 3757]

[3] Lidong Zhou , Zygmunt J. Haas, "Securing Ad Hoc Networks," Cornell University Ithaca, NY 14853

[4] William Stallings, *Cryptography and Network Security Principles and Practices*, 4th Ed

[5] Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks," IEEE 2004.

[6] Zhou, Z.J. Haas, "Securing ad hoc networks," IEEE NetworkMag. 13 (November/December 1999) 24–30.

[7] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks," in: SixthInternational Conference on Mobile Computing and Networking (MOBICOM'00), August 2000,pp. 275–283.

[8] Lakshmi Venkatraman and Dharma P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," Journal of Parallel and Distributed Computing - Special issue on Routing in mobile and wireless ad hoc networks, Volume 63 Issue 2, February 2003, Pages 214 - 227

[9] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , ―A Survey on Attacks and Countermeasures in

Mobile Ad Hoc Networks ,‖ Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[10] Payal N. Raj and Prashant B. Swades, ―DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET‖ , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[11] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", Master Thesis, Thesis no: MCS-2007:07, March 22, 2007.

[12] Jain, S., Jain, M., and Kandwal, Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Computer Applications, 2010, Vol. 1, No. 7, pp. 37-42.

[13] Baadache, and Belmehdi, Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, J. Comp. Sci. and Info. Security, 2010, Vol. 7, No. 1, pp. 10-16.

[14] Vaithiyanathan, Gracelin Sheeba.R, Edna Elizabeth. N, Dr.S.Radha, ―A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm‖, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[15] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International

[16] Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007

[17] Yu CW, Wu T-K, Cheng RH, Chang SC, A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007

[18] Wang W, Bhargava B, Linderman M, Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.

[19] Min Z, Jiliu Z, Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009

[20] Vishnu KA, Paul J, Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks. International Journal of Computer Applications,2010, 1(22):38–42. doi: 10.5120/445-679

[21] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011

[22] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, IETF Network Working Group, January 1999.

[23] E. C. H. Ngai, J. Liu, and M. R. Lyu. "On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC 06), Istanbul, Turkey, June 2006.

[24] M. Zorzi and R.R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Trans. Mobile Computing, vol. 2, no. 4, Oct.-Dec. 2003.

[25] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communications Review (MC2R) Volume 1, (2002).

[26] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS'02).

[27] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05).

[28] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM, 47(6):53-57.

[29] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[30] Roberta, Bragg, Mark, Rhodes-Ousley, Keith Strassberg, *The Complete Reference Network Security*

[31] E. A. Mary Anita and V. Vasudevan, "Black Hole attack on multicast routing protocols," JCIT, Vol.4, No.2, pp. 64–68, 2009.

[32] Y. C. Hu, A. Perrig and D. B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol"; Proceedings of ACM WiSe2003, Sep, 2003.

12. ACKNOWLDGEMENT

We are highly thankful to Mr. Sanjay Bansal, Chairman of DBGI Group Dehradun, for providing us the research environment with highly advance lab.

We also thankfull to Editorial Board of IJCA for their motivation, support and consistent communication.