RESEARCH ARTICLE OPEN ACCESS

Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols

Amandeep Kaur[1], Deepinder Singh Wadhwa[2]
[1](Lecturer, Electronics and Communication Department, RIMT, Mandi Gobindgarh)
[2](Assistant Professor, Electronics and Communication Department, BGIET, Sangrur)

ABSTRACT
This Paper focuses on the effects of jelly fish attack on MANET's routing protocols. Here four protocols AODV, DSR, TORA and GRP are used. Performance of the network has been evaluated in terms of Data dropped (buffer overflow), Data dropped (retry threshold exceeded), Load, Media access delay, Retransmission attempts. Simulations were carried out by using OPNET 14.5 simulator.

Keywords – AODV, DSR, GRP, Jelly Fish Attack, TORA

I. INTRODUCTION

MANET is mobile ad-hoc network, which is a group of number of mobile nodes that forms ad-hoc network. Network nodes communicate with each other without the assistance of any centralized authority or management. It is a dynamic topology which forms a temporary network because nodes always move anywhere in the network. It is fast growing technology, whenever the existing technology fails in any area then mobile ad-hoc networks helps to continue the communication among the nodes in that area. Ramanathan and Jason Redi tell about PRNET (packet radio network) which were used. The goal of PRNET was to provide packet switching to mobile battlefields, hostile networks [1]. In 1999, Per Johansson, Tony Larsson and Nicklas Hedman compared three protocols i.e. DSDV, AODV, DSR under two types of simulations–Mobility varied and offered load was kept constant. b) Both offered load and mobility kept constant [2]. In 2003 Sanjay ramaswami , present a technique to identify multiple black hole nodes and a solution is given to find out a safe path or route to avoid cooperative black hole attack. This secured path helps the data packets to travel or transmit from source to destination [3]. The attacker nodes disrupt the route discovery process, hence in 2002, Panagiotis and Zygmunt discovered a route discovery protocol that helps to mitigate or prevent the effects of the malicious node in the network. This proposed protocol provides correct connectivity of links among the nodes. Any two nodes can simply setup a shared key for their communication [4]. Imran Raza and Amjad Ali analyses the congestion behavior of TCP and its variants for AODV and DSR protocols under persistent packet reordering jelly fish attack and proposed a solution for it by adding two new states in this scheme to mitigates the effects of reordering attack in TCPreno [5]. In 2010 multicast routing protocols were studied with capability and security techniques [6]. In 2011, simulation study of black hole attack and jelly fish attack and its impact on open loop and close loop flows and the critical performance of network were measured under these attacks [7]. In 2009, a secured routing protocol was proposed which removes the effect of black hole attack on ad-hoc on demand distance vector routing protocol. This protocol was experimentally show better results than AODV protocol. In this scheme three protocols are taken i.e. AODV, BAODV and SAODV and two scenarios CBR and FTP are taken. The performance of these three protocols were analyzed, compared and the simulation results shows that the secured routing protocol gives better performance then AODV and BAODV [8]. In 2012 a scheme was proposed which prevents the black hole attack, this method uses promiscuous mode to detect black hole node and informs about the attacker node to all the other nodes in the network [9]. After this a method was proposed to prevent both the black and gray behavior i.e. black and gray hole attacks. In this scheme to tackle these attacks extended data routing tables were to be maintained at each node. This method was also helpful in finding the cooperative black hole attacker nodes [10]. It was demonstrated in 2012 that by assigning reputation tables and values to the participating nodes the black hole nodes can be detected. These reputation tables and values assigned to every nodes acts and measured as truth worthiness of that node [11]. In 2012, performance of protocols were compared under jelly fish delay variance attack by using AODV, DSR and TORA routing protocols and average end-to-end delay, network load and Throughput are taken as performance parameters a. Here, TORA was showing better results [12]. Mohammad Wazid, Avita katal and R H Goudar proposed a cluster and super cluster based intrution detection and prevention techniques to prevent jelly fish reorder attack under FTTP (heavy load) traffic using AODV protocol [13].

II. RELATED TERMS

1. Jelly fish attack

Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Jelly fish attack is categorized as Jelly fish reorder attack, JF periodic dropping attack and JF delay variance attack. Jelly fish attacks are targeted against closed loop flows. TCP has well known vulnerabilities to delay, drop and mis-order the packets. Due to this nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack [12].

2. Routing protocols

The rules that help the data packets to route from source to destination node are called as Routing protocols. There are three types of protocols reactive, proactive and hybrid protocols.

A. Ad-hoc On-Demand Distance Vector Routing Protocol:

It is a reactive routing protocol which sends route request messages to find out the route to the destination node. When the destination node accept that message i.e. RREQ messages from the source it send RREP message to the source to inform the source node that it has accept the RREQ message and started to set up a link between the nodes. Routing tables are used to update the information about the routes and the nodes. It sends Hello message to detect their neighbors. Hello message is also used to detect the link failure between two nodes [2].

B. Dynamic source routing protocol:

In DSR routes and links are stored in route cache. It also uses route discovery process to find out the specific route for the data packets to send to the destination node. It floods the route request packets to the destination node and as in AODV the destination node reply about the RREQ packet by sending RREP packet or message to the source node. Then this information will be stored in the route cache for future use. If there will be any breakage between the links of the nodes then the nodes send RERR message to the source node. Hence, the source node removes that broken link from its route cache. Then again the route discovery process started [14].

C. Temporally ordered routing protocol:

It is also a reactive protocol. It uses non-hierarchical routing algorithm that is why it attempts to achieve high level of scalability. Unlike, AODV and DSR it built directed acyclic graphs to maintain the routes and links between the nodes. Data packets flow from higher metric node to lower metric node. Route creation, maintenance and erasure are three phases which the TORA protocol follows. Links are assigned on the basis of metrics of the nodes; a node with high degree of metric assigned the link first. It adapts well with limited bandwidth [15].

D. Geographical routing protocol:

GRP is proactive or table driven protocol. The network is divided into quadrants and the information is flows through flooding mechanism. It follows the shortest path to send the packet. When the routes become blocked or there in case of link failure, packets returns to previous hop and then again from that hop new route is found. It broadcast Hello messages to the neighbors to provide them the necessary information about the routes. Hello messages are also used to test the connectivity of local connection from the neighbor nodes. If this hello message will not be received by the neighbor nodes at the specified time then this period is called as “Neighbor expiry time” [16].

III. EXPERIMENTAL DESIGN OF THE NETWORK

SIMULATION SCENARIO

Table 1: Common parameters

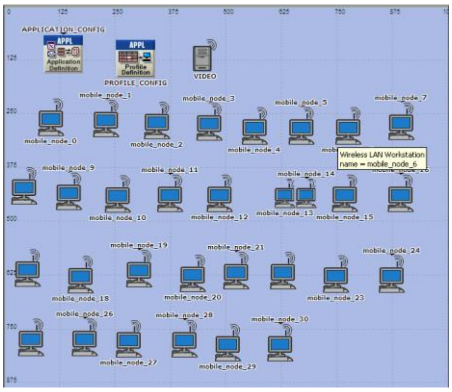
Parameters	Value
Simulator	Opnet modeler 14.5
Area	10x10 km
Network size	30 nodes Scenario 1 and 2
	50 nodes scenario 3 and 4
Mobility model	Random
Topology	Random
Traffic Type	Video (High Resolution Video)
Simulation Time	20 minutes
Address Mode	IPv4
Ad Hoc Routing Parameters	AODV,DSR,TORA,GRP
Jellyfish Attackers	Zero for 1 and 3 scenario
	15 for 2 scenario
	25 for 4 scenario
Forwarding Rate	400000 packets/seconds for honest nodes
	5000 packets/seconds for JF attacker nodes

A. Run time parameters:
Duration- 20 Minutes for all Scenarios
Speed- 128
Value per Statistics- 100
Update Interval- 500000 Events

B. Implementation of Jelly Fish Attack:
In the scenarios of jelly fish attack for all the four routing protocols i.e. AODV,DSR,TORA,GRP the forwarding rate is taken as 5000 packets per second and in the normal flow scenarios of these protocols the value for forwarding rate is 400000 packets per second. In our work, OPNET 14.5 Modeler is used to analyze the effects of jelly fish attack on Mobile ad-hoc network's routing protocol. Here, we use four protocols AODV, DSR, TORA and GRP. In this paper there are four simulation scenarios to analyze our results.

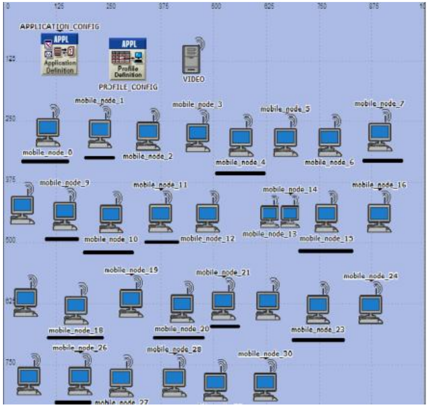
IV. SIMULATION SCENARIOS

In scenario 1, the traffic is without any JF attacker node. The traffic is running smoothly with 30 wireless mobile nodes. This scenario shows the normal flow of information between the nodes.



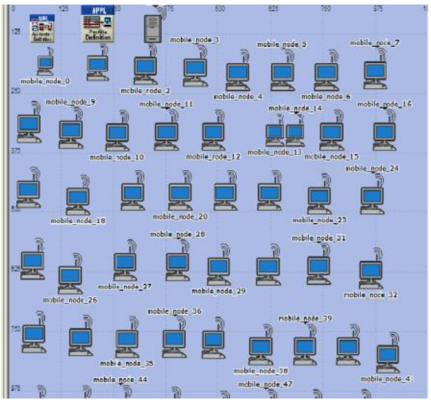
Scenario 1: Normal flow with 30 nodes

In scenario 2, the traffic is flowing with some JF attacker nodes. Black underlined nodes are the JF attacker nodes. Here 0, 1, 4, 7, 9, 10, 11, 15, 18, 20, 21, 23, 26, 27, 29 are the attacker nodes.



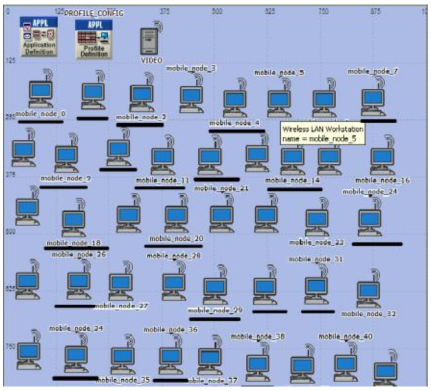
Scenario 2: JF attack with 30 nodes

Scenario 3 is showing the normal functioning of the network with 50 nodes.



Scenario3: Normal flow with 50 nodes

Here, 50 nodes are taken with black underlined nodes showing JF attacker nodes in scenario 4. These nodes disrupt the normal behavior of the network. 0, 1, 2, 4, 7, 9, 10, 11, 12, 14, 18, 20, 24, 26, 29, 30, 31, 34, 36, 38, 40, 41, 43, 44, 46 are the JF attacker nodes.



Scenario 4: JF attack with 50 nodes

Each protocol used in this paper has all these four scenarios.

V. V SIMULATION RESULTS:

Performance Metrics:

Following are the metrics from which we calculate the performance of the network:
Data dropped (Buffer overflow) (b/sec), Data dropped (retry threshold exceeded) (b/sec), Load (b/sec), Media Access Delay (sec), Retransmission of packets (packets).

A. Data Drop (Buffer Overflow)

This metric reports the number of the higher layer packets that are dropped because the MAC could not receive any acknowledgement for the retransmission of those packets or their fragments.

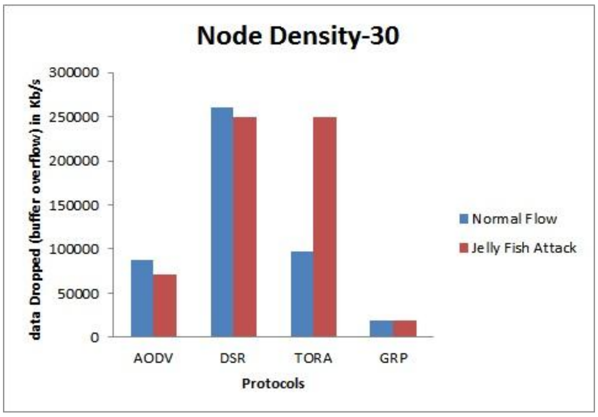


Figure 1: Data Dropped (Buffer overflow)

Table 2: Data dropped (Buffer overflow) (kb/sec)

Node Density	30 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	88000	260000	97000	18500
Jellyfish Flow	71000	250000	250000	18900

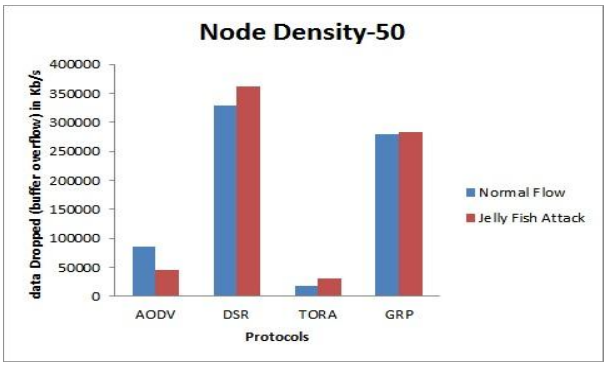


Figure 2: Data Dropped (Buffer Overflow)

Table 3: Data dropped (Buffer overflow) (b/sec)

Node Density	50 Nodes			
Protocols	AOD V	DSR	TORA	GRP
Normal Flow	85100	329000	18000	279000
Jellyfish Flow	45100	361000	31500	284000

B. Data Dropped (Retry Threshold Exceeded):

The total size of higher layer data packets dropped by all the Wireless LAN MAC's in the network due to:-

a) Full higher layer data buffer.

b) The size of the higher layer packet which is greater than the maximum allowed data size defined in the IEEE 802.11 standard.

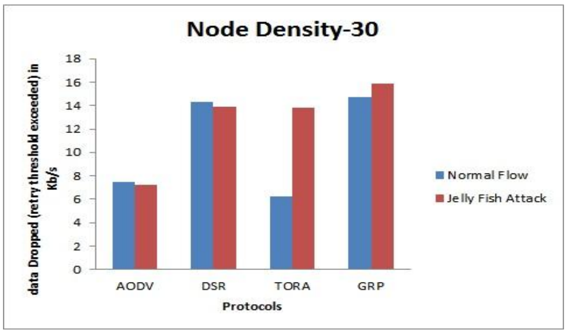


Figure 3: Data Dropped (Retry Threshold Exceed)

Table 4: Data dropped (Retry threshold exceed) (kb/sec)

Node Density	30 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	7.5	14.3	6.28	14.7
Jellyfish Flow	7.2	13.9	13.8	15.9

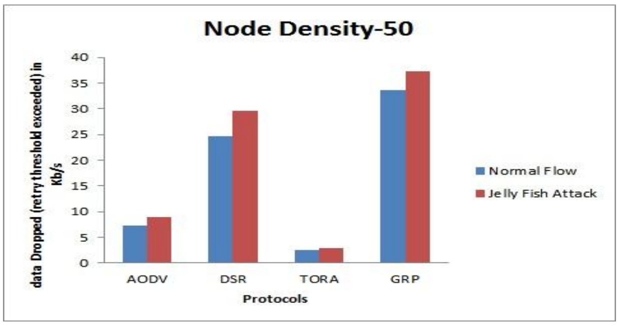


Figure 4: Data Dropped (Retry Threshold Exceed)

Table 5: Data dropped (Retry Threshold Exceed (b/sec)

Node Density	50 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	7300	24600	2570	33700
Jellyfish Flow	9000	29600	2830	37300

C. Load:-

It represents the total load submitted to Wireless LAN layer by all higher layers in all WLAN nodes of the network.

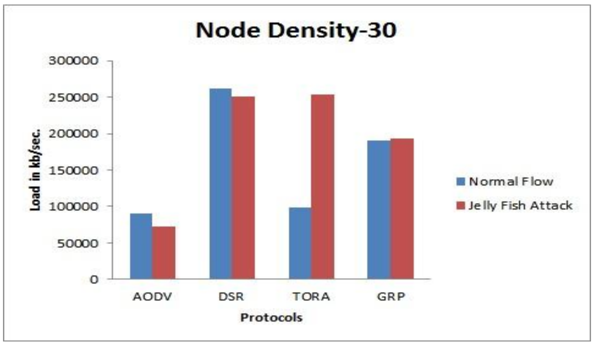


Figure 5: Load

Table 6: Load (kb/sec)

Node Density	30 Density			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	90000	262000	99000	190000
Jellyfish Flow	73000	251000	254000	193000

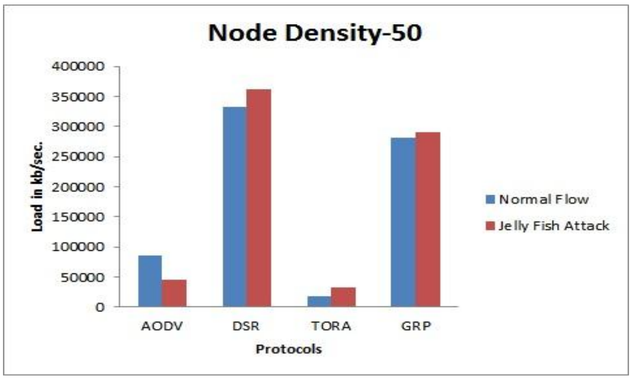


Figure 6: Load

Table 7: Load (b/sec)

Node Density	50 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	85300	332000	18200	282000
Jellyfish Flow	45900	361000	31800	290000

D. Media Access Delay:

It represents the global statistics for the total queuing and contention delays of the data, management, delayed block-ACK and block-ACK request frames transmission by all WLAN MACs in the network. For each frame, this delay is calculated as the duration from the time when it is inserted into the transmission queue, which is arrival time for higher layer data packets and creation time for all other frames types, until the time when the frame is sent to the physical layer for the first time.

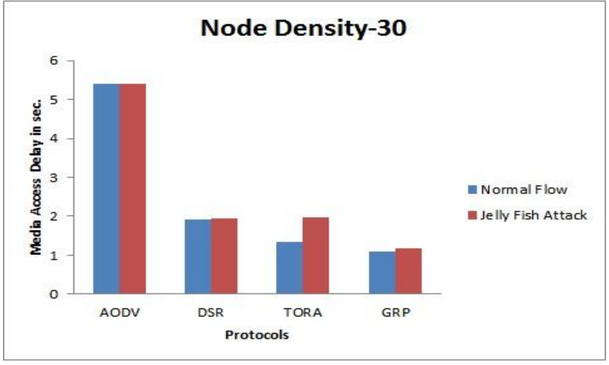


Figure 7: Media Access Delay

Table 8: Media Access Delay (sec)

Node Density	30			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	5.4	1.92	1.34	1.08
Jellyfish Flow	5.4	1.95	1.97	1.18

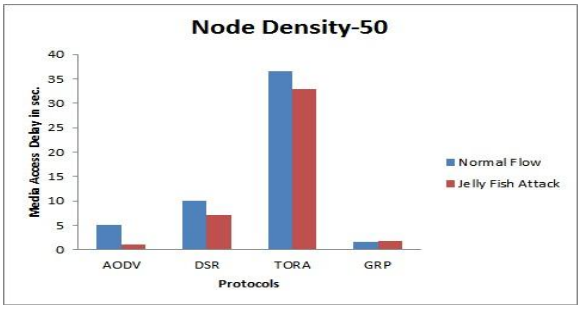


Figure 8: Media Access Delay

Table 9: Media Access Delay (sec)

Node Density	50 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	5	10	36.6	1.7
Jellyfish Flow	1.13	7.1	32.8	1.75

E. Retransmission Attempts:-

Total number of retransmission attempts by all WLAN MAC's in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limits. It also includes retry count increments, due to internal collisions.

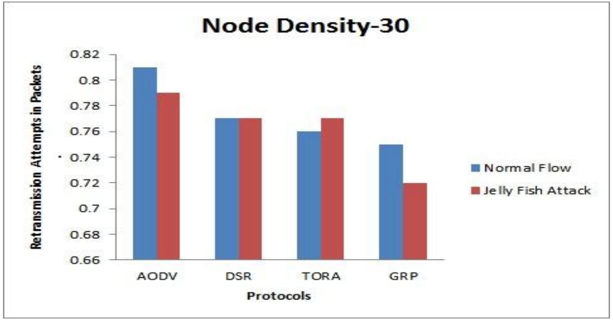


Figure 9: Retransmission Attempts for Thirty Nodes

Table 10: Retransmission of Packets (Packets)

Node Density	30 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	0.81	0.77	0.76	0.75
Jellyfish Flow	0.79	0.77	0.77	0.72

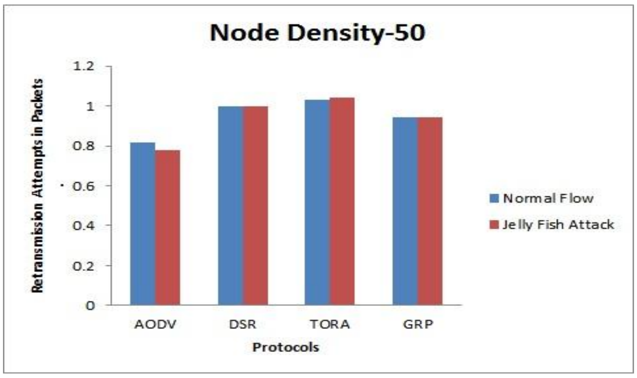


Figure 10: Retransmission Attempts

Table 11: Retransmission Attempts (Packets)

Node Density	50 Nodes			
Protocols	AODV	DSR	TORA	GRP
Normal Flow	0.819	1	1.03	0.94
Jellyfish Flow	0.78	1	1.04	0.94

VI. OBSERVATIONS

Some of the observations for this paper are as follows:

- If we increase the node density then data dropped due to buffer overflow is low in TORA and at node density 30, GRP has lower data dropped in Normal flow as well as jelly fish flow scenario. This drop of data is due to number of higher layer packets that are dropped because the MAC layer could not receive any acknowledgement for the retransmission of those packets that are dropped.
- Data dropped (retry threshold excceed) is due to the reason that the size of the higher layer packets is greater than the maximum allowed data size defined in IEEE 802.11 standard. At node density 30 and 50 TORA has lowest data dropped due to retry threshold only in normal flow but in jelly fish scenario with node density 30, AODV has lower data drop.
- Delay is low in GRP if we increase the node density. It is the delay produced during transmission and reception of data packets. Load is less in case of AODV and TORA.
- For lower density of nodes i.e. 30, GRP performs better for Media Access Delay and Retransmission Attempts and when we increase the density up to 50 nodes, AODV performance is good. DSR performs worst.
-

VII. CONCLUSIONS AND FUTURE SCOPE

If good time services and no loss of information needs then we have to choose TORA and if we want low delay produced during transmission and reception of information and data then we go for AODV. GRP is used as optional at the place of AODV. As compare to other three protocols the performance of DSR is poor. If we increase node density, forwarding rate of packets, use diferent protocol and introduced JF periodic dropping attack the performance may vary.This work can be further extended to calculate the performance of Mobile ad-hoc networks.

VIII. ACKNOWLEDGEMENTS

We are thanking to our management for their continuing support and encouragement for completing this work and we are thanking our head of the department for his valuable suggestion.

REFERENCES

[1] Ram Ramanathan and Jason Redi, “A brief overview of Ad-hoc networks: Challenges and direction”, IEEE Communications magazine 50 Anniversary commemorative Issue/May 2002.

[2] Per Johnson, Tony Larsson, and Nicklas Hedman, “Scenario based performance analysis of routing protocols for Mobile ad-hoc network”, Mobicom ’99 Scattle Washington USA, copyright ACM 1999 1-58113-142-9/99/08.

[3] Sanjay Ramaswami, Huirong Fu, Manohar sreekantaradhya John Dixon and Kendall Nygard, “Prevention of cooperative Black hole attack in wireless ad-hoc networks”, 2003.

[4] Panagiotis papadimitratos and Zygmunt Haas, “Security routing for Mobile ad-hoc networks”. In proceedings of CNDS 2002, San Antonio, TX, January 27-31, 2002.

[5] Imran Raza, S.A.Hussian, Amjad Ali, Muhammad Hassan Raza“Persistant packet reordering attack in TCP based Ad-hoc wireless network”, IEEE, 978-1-4244-8003-6/10-2010.

[6] Ahmed.M.Abdel Mo’men, Haitham.S .Hamzas and Iman.A.Saroit, “A survey on security enhanced multicast routing protocol in mobile ad-hoc network”, IEEE, 978-1-4244-8003-6/10-10-2010.

[7] Nidhi Purohit, Richa Sinha and Khushbu Maurya, “Simulation study of black hole and jelly fish attack on MANET using NS-3”, Institute of technology, Nirma University, Ahmedabad-382481 08-10 December, 2011.

[8] Songbai Lu Longxuan Li Lingyan Jia, “SAODV: A MANET Routing protocols that can withstand black hole attack”, International Conference on computational Intelligence and Security, 2009.

[9] Pramod Kumar Singh, Govind Sharma, “An efficient prevention of black hole problem in AODV routing protocol in MANET”, IEEE11th Conference on Trust, Security and Privacy in Computing Communication, 2012.

[10] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, “Detection and Removal of co-operative black hole attack and gray hole attacks in MANET”, International Conference on System Engineering and Technology, Bandung, Indonesia, September 11-1-2012.

[11] Shinni Mittal,Harish Taluja, “Analysis of co-operative black hole attack using Dynamic source protocol”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8,August 2012.

[12] Mohammad Wazid, Vipin Kumar, RH Goudar, “Comparative performance analysis of routing protocols in mobile ad-hoc network under Jelly fish attack”, 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.

[13] Mohammad Wazid, Avita Katal, RH Goudar,“Cluster and Super cluster based Intrution Detection and Prevention Techniques for Jelly fish reorder attack”, 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.

[14] Md.Anisur Rahman, Md.Shohidul Islam, Alex Talevski, “Performance Measurement of various routing protocols in Ad-hoc network”, In the proceedings of International Multi Conference of Engineers and Computer Scienstists, Hong Kong, Volume 1, IM ECS 2009, March 18-20-2009.

[15] Saleh Ali, K.AL-Omari and Putra Sumari, “An overview of mobile ad-hoc network’s for the existing protocols and applications”, Journal on Application of Graph Theory in Wireless Ad-hoc Networks and sensor network’s (J GRAPH-HOC) Vol.2, No. 1, March 2010.

[16] Takagi, H.Kleinrock, L, “Optimal transmission ranges for randomly distributed packet radio terminals”, IEEE Transactions on communications, (32)3:246-257, March, 1984.