Investigation on DDOS Attacks Over MANET

Monika Aggarwal[1] Pankaj Kapoor[2]
[1, 2]Computer Science and Engineering Department
[1, 2]SIET, Ambala

Abstract— In recent years, the rapid proliferation of wireless networks, usage of wireless devices and deployment of many mobile computing devices and applications has changed the shape of network security. One field which needs more security is the mobile ad hoc network (MANET). The term "ad hoc" means self-organized nodes that do not have a central entity to govern them. Network security plays a crucial role in this MANET and the traditional way of protecting the networks through firewalls and encryption software is no longer effective and sufficient. Denial of service attacks include deliberately dropping packets instead of forwarding them, as well as actively interfering in the communication of neighbouring nodes. A malicious node could attempt to flood the network with its own unicast data packets, potentially using many different destination addresses. In this paper, we analyze the performance of OLSR routing protocol under two different DDOS attacks namely fake hello link flooding and low rate TCP target attack over MANET. we also evaluate the effect of RED-a defense mechanism, against low rate TCP target attack.

Keywords: MANET, DDOS, TCP, OLSR, RED

I. INTRODUCTION

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. The need for security in MANET is very high because there is no fixed infrastructure for the network and the nodes are mobile with open and dynamic structure. The most important parameters that security depends on are authentication, integrity, confidentiality, availability and non-repudiation [1]. The wireless ad hoc networks need more security because it is more vulnerable to attacks by design. The use of wireless links makes an ad hoc network more susceptible to attacks ranging from passive eavesdropping to active interfering [2]. Unlike in wired networks, where an attacker must gain physical access to the network wires or pass through the several lines of defense like firewalls and gateways. When compared to a wired network, it's easier to attack a wireless network because of its structure and also the attack may come in any direction and any node can be attacked at any point of time. MANETs are more vulnerable to attacks because:

Limited computational capabilities:

Typically, nodes in ad-hoc networks are modular, independent, and limited in computational capability and therefore may become a source of vulnerability when they handle public-key cryptography during normal operation.

Limited power supply:

Since nodes normally use battery as power supply, an intruder can exhaust batteries by creating additional transmissions or excessive computations to be carried out by nodes.

Challenging key management:

Dynamic topology and movement of nodes in an Ad Hoc network make key management difficult if cryptography is used in the routing protocol.

So, that's the reason each and every node in the network has to prepare for attacks at any point of time. And also as there is no central based controlling identity for the participating nodes; the attacks are much easier to launch in MANET. The intruder may insert spurious information into routing packets, causing erroneous routing table updates and thus misrouting [3].

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non- repudiation.

1) Confidentiality is to keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas.
2) Authentication is to be able to identify a node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity.
3) Integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack.
4) Non-repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.
5) Availability is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents.
6) Access control is to prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought

of service in both network communications and individual computer systems.

A. Classification af Attacks

Nodes in MANET can be broken, malicious or selfish. Broken nodes become non-functional due to some link failure so cannot forward the traffic that they earlier agree to forward. Malicious nodes aimed at disrupting the network by dropping the packets or launching denial of service attacks. Selfish nodes hinder the routing by dropping packets in order to conserve their energy and bandwidth. MANET found applications in military, disaster relief operations etc as it is easy to deploy. In order to encourage its use in future it is important to ensure secure and reliable routing in MANET. Before providing security we need to know attacks related to such networks. Security aspects were not considered when adhoc protocols were designed. Later researchers tried to incorporate security mechanisms on existing routing protocols. Attacks can be classified into two broad categories[4]:

1) Passive Attacks

The attacker just snoops the network without disrupting the network operation. These attacks compromise the confidentiality of the data and tell which nodes are working in promiscuous mode.

i) *Eavesdropping:* It is reading or snooping of messages by an unintended receiver. In MANET, the nodes share a wireless medium so nodes can easily overhear communication of the nodes within its transmission range. This attack can be prevented by using encryption.

ii) *Selfishness:* A selfish node in order to save its battery life and resources does not participate in routing either by dropping the packets or not forwarding them.

2) Active Attacks

Attacks in which attacker disrupts the normal operation of the network by fabricating messages, dropping or modifying packets, replaying packets or tunneling them to other part of the network. Basically the content of message is modified. These can be internal attacks and external attacks.

- *External attacks:* In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services [5].

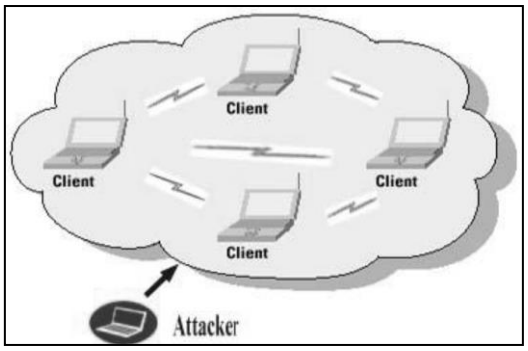

Fig. 1: External attack

- *Internal attacks:* In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a current node and using it as a basis to conduct the attack [6].

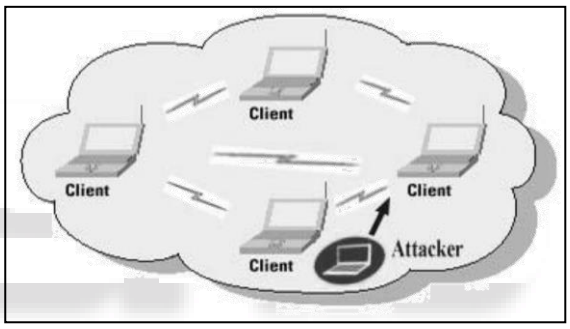

Fig. 2: Internal attack

Active attacks can be further classified corresponding to different layers in MANET.

Fig. 3: Classification of Attacks [7].

II. RELATED WORK

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [8]. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9]. Different kinds of attacks have been analyzed in MANET and their affect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [10].

Security is one of the most primary concerns in MANET for the protection of communication and security of information. For network operation it is necessary to perform routing and packet forwarding. Hence numbers of security mechanisms has been made to counter measure the malicious attacks.

In cryptographic approaches like S-AODV [11] and Adriane [12], the routing packets are encrypted using symmetric or asymmetric algorithm and hence external or inside attacker cannot modify the packets. However the problem with cryptographic approaches
is the increased consumption of processing power and flooding attack can also be launched without forging the packets.

In [13] Dahill, et al. proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN end-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet.

One primitive solution to vanish the RREP forging is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node [14]. This method avoid intermediate node to reply which avoid in certain case the Black Hole and implements the secure protocol. This increase the routing delay in large networks and a malicious node can take advantage by replying message instead of destination node. So for this one or more routes are used by the intermediate nodes which replay the RREQ messages to confirm the routes from intermediate nodes and destination nodes for sending out the data packets. In case if it does not exist, the reply messages is discarded from intermediate node and alarm messages are sent to the network. This method avoids the Black Hole problem thus preventing the network from malicious node. This will result in great delay especially in large networks and in addition the attacker can fabricate a reply message on behalf of the destination node.

In [15] Aleksandar Kuzmanovic and Edward W. Knightly have analyzed several DoS traffic patterns for different TCP Variants such as TCP-Reno, New Reno, Tahoe and SACK (Selective Acknowledgement) and showed that a realistic threat to today's Internet is low-rate DoS attacks and for small Round Trip Time (RTT) flows out of a heterogeneous RTT environment , are more vulnerable to low-rate DoS attacks. RED and RED –PD like mechanisms unable to prevent DoS-initiated synchronization but not eliminate the effectiveness of the attack.

In [16] Ferdous A. Barbhuiya et. al. summarize that Transmission Control Protocol (TCP) is a transport layer protocol which provides flow control, congestion avoidance and error control. TCP is designed to provide the reliable end to end byte stream communication and little or almost no consideration was given to the fact that algorithms used in TCP can be exploited by attackers while designing this protocol. Low rate TCP-targeted denial of service attack is a cleverly crafted attack in which an attacker exploits congestion avoidance algorithm and uniformity of minimum Retransmission Time out period in Transmission Control Protocol. optimistic acknowledgement for any misbehaving TCP receiver is suggested for detection and mitigation of Induced Low rate TCP-targeted attack . This solution mitigates this Induced Low rate TCP-targeted attack by stopping optimistic acknowledgement.

In [17], the author disscuses the two type of attack on adhoc network. The first on is Jelly Fish and second one is Black Hole attack.Significant progress has been made towards making ad hoc networks secure and DoS resilient. In this paper, the author made the design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. JellyFish attack, is targeted against closed-loop flows such as TCP. This attack is protocol-compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. These attacks are studied in a variety of settings and have provided a quantification of the damage they can inflict. As such a partitioned system is clearly undesirable, author also considered fairness measures and the mean number of hops for a received packet, as critical performance measures for a system under attack. The main guidelines are provided for protocol designers who are developing DoS-resilience mechanisms: with a better understanding of the key attack factors and how to evaluate the impact of an attack, protocol designers can better determine if the overhead of deploying a counter-strategy is merited given the damage that an attack can inflict.

III. PROPOSED METHODOLOGY

Mobile Ad hoc Networks (MANET) is new paradigm of wireless networks providing unrestricted mobility to nodes with no fixed or centralized infrastructure. Each node participating in the network acts as router to route the data from source to destination. This characteristic makes MANET more vulnerable to routing attacks. The various authors have given various proposals for detection and prevention of DDOS in MANET but every proposal has some limitations. In this paper, the behavior of two DDOS attacks and the performance impact of these attack on OLSR

protocol is studied. An Active queue management scheme is proposed that can prevent the effect of low rate TCP-SYN attack without causing much overhead. The NS2 network simulator is used for evaluation.

A. Research Methodology

Ns2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (NAM) is use to visualize the simulations. Ns2 fully simulates a layered network from the physical radio transmission channel to high-level applications.

Ns2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols.

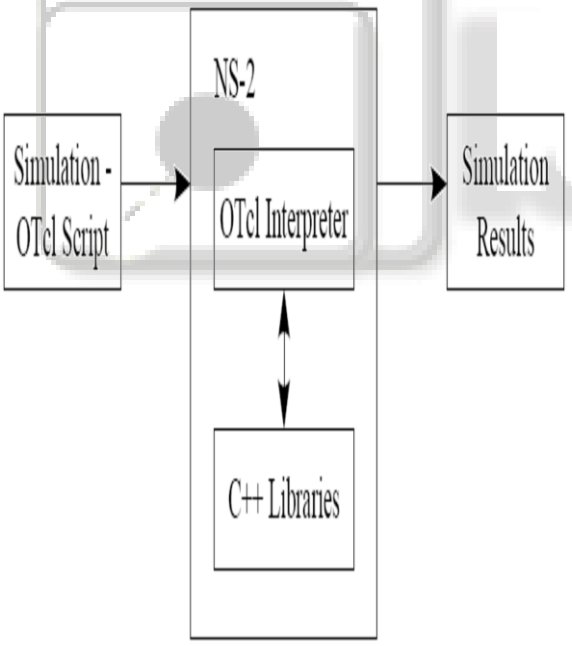

Fig. 4: data flow for one time simulation

As Figure 4 shows, for the data flow of one time simulation in ns-2, the user input an OTcl source file, the OTcl script do the work of initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. And then, this OTcl script file will be passed to ns-2, in this view, we can treat ns-2 as Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup module libraries. And then the detail network construction and traffic simulation will be actually done in ns-2. After a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, and the data can be used for simulation analysis .

Parameter	Value
Simulation time	150 Sec
Simulation area	1500m x 300m
Antenna	Omni antenna
No. of nodes	30
Traffic	CBR
Routing protocol	OLSR
Mobilty Model	Random Waypoint Model
Security attacks	Fake-hello flooding, low rate TCP-SYN attack
Active queue scheme	DropTail, RED
Pause time	5, 10, 15, 20, 25, 30

Table. 1: Salient Simulation Parameters

There are many parameters which can be used to evaluate the performance of routing protocols. Performance metrics are considered as follows**:**

Throughput: The ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Figure 5, shows the effect of two different DDOS attacks on throughput when pause time is varied.

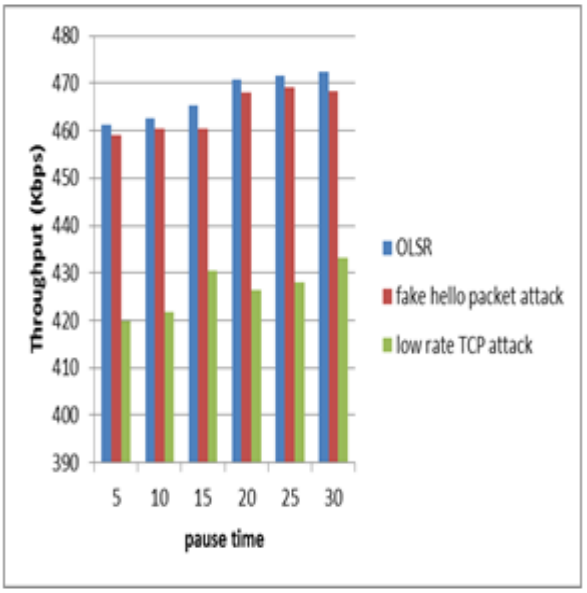

Fig. 5: Throughput versus pause time

Figure 6, shows the effect of active queue management technique under low rate TCP-SYN attack on throughput when pause time is varied.

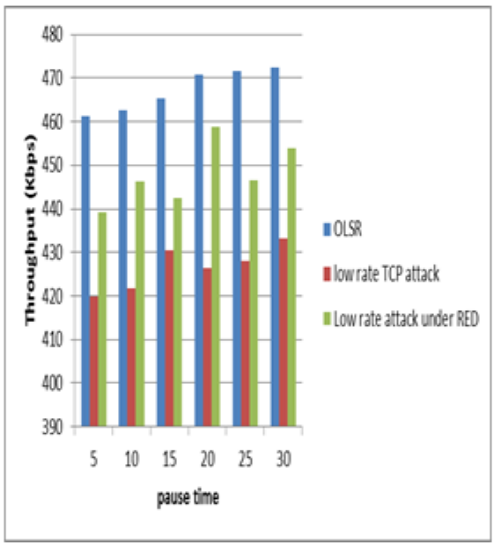

Fig. 6: Throughput versus pause time

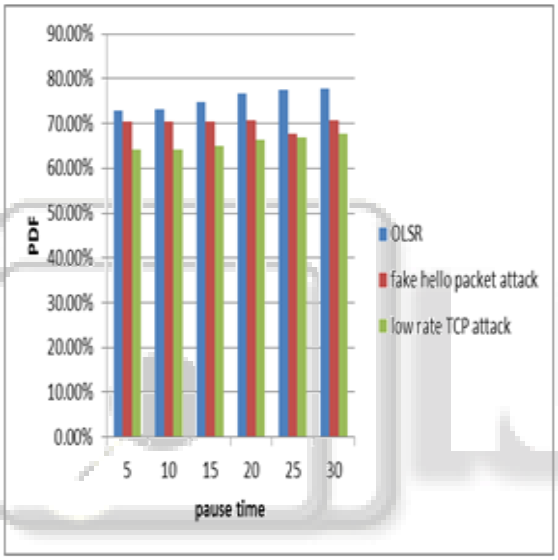

Fig. 7: PDR versus pause time.

Figure 7, shows the pachet delivery ratio for OLSR under TCP SYN DOS attack with RED

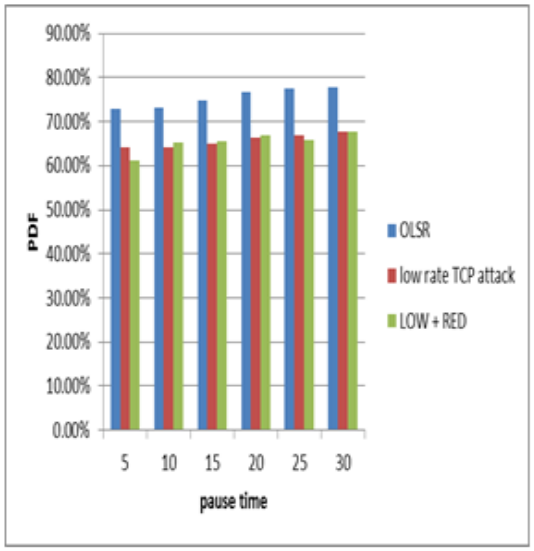

Fig. 8: PDR versus pause time

Average Delay

The average delay a data packet takes to travel from the source to the destination node. The figure 9 shows the impact of fake hello flooding and low rate TCP-SYN attack on the average end to end delay for OLSR.

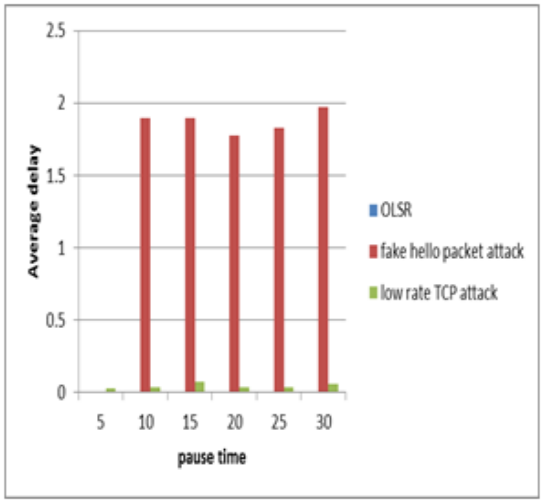

Fig. 9: Average delay versus pause time

Figure 7, shows the average end to end delay for OLSR under TCP SYN DOS attack with RED.

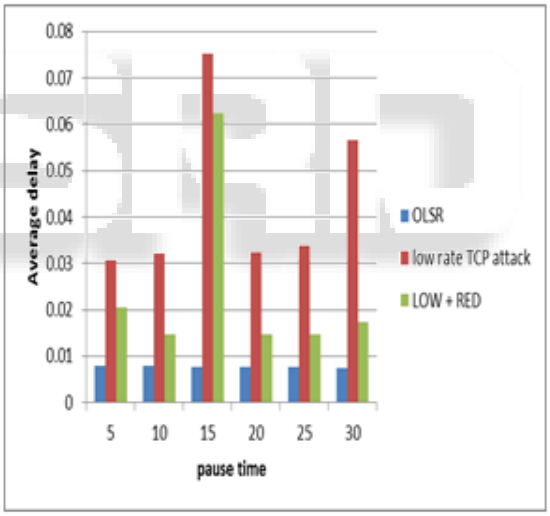

Fig. 10: Average delay versus pause time

IV. Conclusion and Future Work

In this paper, We simulated the fake hello flooding anf low rate TCP-SYN attacks in the Ad hoc Networks and investigated its affects for OLSR routing protocol. Having simulated the low rate TCP-SYN attack, we saw that the performance is much decresed in the ad-hoc network as compare to other DDOS attack namely fake hello flooding attack. This also shows that low rate TCP-SYN attack affects the overall network than fake hello flooding attack. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency for low rate TCP-SYN attack. Our proposed solution tries to reduce the effect of low rate TCP-SYN attack by using a probability scheme. In our study, we used the OLSR routing protocol. But the other routing protocols

should be tested as well to see the effect of these DDOS attack.

REFERENCES

[1] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST,2(4).
[2] I. Noman and Z. A. Shaikh, "Security Issues in Mobile Ad Hoc Network," Wireless Networks and Security, Springer Berlin Heidelberg, pp. 49-80, 2013.
[3] Rai, Abhay Kumar, Rajiv Ranjan Tewari, and Saurabh Kant Upadhyay. "Different types of attacks on integrated MANET-Internet communication." International Journal of Computer Science and Security 4.3 (2010): 265-274.
[4] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management 11 (2011): 32-37.
[5] Shanthi, N., L. Ganesan, and K. Ramar. "STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK." Journal of Theoretical & Applied Information Technology 6.4 (2009).
[6] Pani, N. K., Mishra, S., Secure Hybrid Routing for MANET Resilient to Internal and External Attacks, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India, Springer International Publishing, 2014, pp. 449-458.
[7] Tarunpreet Bhatia and A.K. Verma, "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms", International Journal of Advanced Research in Computer Science and Software Engineering, 3 (6), June - 2013, pp. 1382-1394.
[8] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.
[9] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
[10] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".
[11] S. Yi and R. Kravets, Composite Key Management for AdHocNetworks.Proc. Of the 1st Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.
[12] Hu, Y., Perrig, A., & Johnson, D. (2002). Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta
[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.
[14] Hongmei Deng, Dharma P. Argawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, October 2002.
[15] Aleksandar Kuzmanovic and Edward W. Knightly, "Low Rate TCP Targeted Denial of Service Attacks" SIGCOMM'03, August 25-29, 2003.
[16] Ferdous A. Barbhuiya, Vaibhav Gupta, Santosh Biswas and Sukumar Nandi, "Detection and Mitigation of Induced Low Rate TCP-Targeted Denial of Service Attack" IEEE Sixth International Conference on Software Security and Reliability, Oct. 2012.
[17] Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly , "Impact of Denial of Service Attacks on Ad Hoc Networks, " IEEE/ACM transactions on networking, VOL. 16, NO. 4,pp no 791-802, Aug 2008.

