Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security and Reliability Analysis of Routing Protocols Under Low Rate Tcp-Target Dos Attack Over Manets

Avineet Saini*
Deptt. of Computer Science and Engg.,
Indo Global college of Engineering, Mohali
Punjab, India

Rubal Jeet
Deptt. of Computer Science and Engg.,
Indo Global college of Engineering, Mohali
Punjab, India

Abstract*— A Mobile Ad hoc Network (MANET) is a dynamic multi-hop wireless network that is established by a group of mobile stations without necessarily using pre-existing infrastructure or centralized administration. It can be easily deployed which makes it very attractive for civilian and military applications. Because of its decentralized property, these nodes relay on each other to store and forward packets. These are characterized by bandwidth constrained links, varying link qualities, and highly dynamic topologies.Security is a very big issue in wireless networks. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other is ready to communicate and to agree on initial sequence numbers for the conversation. Thus, we study the effect of Low rate TCP-target DoS attack. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. To explore low-rate DoS, we consider periodic on-off attacks that consist of short, maliciously-chosen-duration inter-burst bursts that repeat with a fixed, maliciously chosen, slow-time-scale frequency

***Keywords*— MANETS, WLANS, DOS, RRED, TCP, SYN ,ACK , NS-2, CBR traffic**

I INTRODUCTION

One of the most promising and discussed technology in the last decade is the wireless technology which allows users to utilize devices that enable the access to information at any time any place. These needs make wireless networks the best solution for interconnecting devices and people. Wireless networks are comprised of devices that communicate through media such as radio signals and infra-red, and they are generally classified into two categories: Infrastructure-based and ad-hoc wireless networks. Infrastructure-based wireless network consists of base stations localized in convenient places, which provide wireless connectivity to devices within their coverage area. Examples of this category are Wireless Local Area Networks (WLANs) and cellular networks. A WLAN is a flexible data communication system implemented as an extension to a wired LAN within a building or campus. On the other hand, ad hoc wireless networks do not have a pre-established infrastructure.Moreover, nodes connect to each other through automatic configuration when they are in transmission range and willing to forward data for other nodes. In this way, an ad hoc wireless network is formed which is both flexible and powerful. Mobile Ad Hoc Networks (MANETs) can be defined as autonomous systems of mobile nodes connected via wireless links without using an existing network infrastructure or centralized administration. The nodes composing a MANET are free to move and to organize themselves arbitrarily: thus, the topology of the network may change rapidly and unpredictability. In multi-hop ad hoc networks, every node acts as a router and forwards each others' packets to enable the communication between nodes not directly connected by wireless links. Historically, MANETs have been used for tactical network related applications to improve battlefield communications and survivability. The introduction of short range wireless technologies such as Bluetooth and IEEE 802.11 DCF has greatly facilitated the deployment of MANETs outside of the military applications, including personal area networking, sensor networks, vehicular services, location-aware services, emergency services etc. Security is a very big issue in both wired and wireless networks. In a wired network, the transmission medium can be physically secured, and access to the network as well. On the other hand, in a wireless network, security is more difficult to implement, since the transmission medium is open to anyone within the geographical range of a transmitter. One main challenge in design of these networks is their vulnerability to security attacks.

A variety of attacks are possible in MANET. Some attacks apply to general network,some apply to wireless network and some are specific to MANETs. These security attacks can be classified according to different criteria, such as the do-main of the attackers, or the techniques used in attacks. These security attacksin MANET and all other networks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

- **Passive vs. active attacks:** The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Table 1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping,traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Table I: *Classification of security attacks*

Passive Attack	Eavesdropping, traffic analysis,monitoring
Active attack	Jamming, Spoofing, modification, replaying, Denial of Service

- **Internal vs. external attacks:** The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.
- **Attacks on different layers of the Internet model:** The attacks can be further classified according to the five layers of the Internet model. Table 2 presents a classification of various security attacks on each layer of the Internet model. Some attacks can be launched at multiple layers.

Table II: *Security attack on each layer of the internet model*

Layers	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session Hijacking, Syn flooding
Network Layer	Wormhole, Blackhole, Byzantine, flooding, Resource consumption, location disclosure attacks
Data link Layer	Traffic analysis, monitoring, disruption MAC, WEP weakness
Physical Layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the middle

The objectives of TCP-like Transport layer protocols in MANET include setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks. However, a MANET has a higher channel error rate when compared with wired networks. Because TCP does not have any mechanism to distinguish whether a loss was caused by congestion, random error, or malicious attacks, TCP multiplicatively decreases its congestion window upon experiencing losses, which degrades network performance significantly. In the low rate TCP-target attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. In this paper, we sudy low-rate TCP-target DoS attacks, that attempt to deny bandwidth while sending at sufficiently low average rate to elude detection by counter-DoS mechanisms. To explore low-rate DoS, we take a frequency-domain perspective and consider periodic on-off attacks that consist of short, maliciously-chosen-duration inter-burst bursts that repeat with a fixed, maliciously chosen, slow-time-scale frequency.

II. Proposed Methodology

This research work attempts to give a generalized solution to the needs in security for Wireless adhoc Networks. There are different security flaws and attacks on routing protocols in wireless adhoc networks. In this work, Low rate TCP target DoS attack has been researched extensively over wireless adhoc environment and a secure counterpart RRED (Robust Random early detection) which provides security features like erlt notification and integrity. This works aims to prevent low rate TCP-target DoS attack which is difficult to detect over mobile adhoc network. Performance evaluation of OLSR and OLSR with RRED under Low rate TCP-traget multi-layered DoS attack by performing simulation in the NS2 Simulator, to evaluate how RRED could possibly apply for reliable routing messages against security as well as performance.

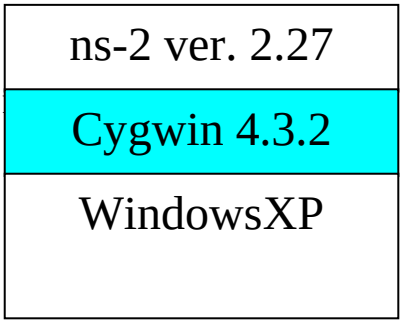
A. Simulation And Results

In this work, main aim is to simulate and analyze performance of OLSR routing protocol under different Low rate TCP-target DoS attack period. Simulations are done considering a hierarchical network consisting of one gateway node that connect two clusters. Constant bit rate (CBR) data sessions among randomly chosen four source-destination pairs are used. However, during this data transfer process, all nodes will operate in the background for providing the necessary support (i.e., routing/forwarding) to the ongoing communication process in the network. The data rate chosen is 2 Mbps

while the data packet size chosen is 512 bytes. The data packets are sent at a rate of 4 packets/sec by each source. Each simulation is executed for 100 seconds. Multiple runs with different seeds have been conducted for each scenario and the collected data is averaged over these runs.

B. **Network Simulator – ns2**

Ns-2 is an open source discrete event simulator used by the research community for research in networking [30]. It has support for both wired and wireless networks and can simulate several network protocols such as TCP, UDP, multicast routing, etc. More recently, support has been added for simulation of large satellite and ad hoc wireless networks. The ns-2 simulation software was developed at the University of Berkeley. It is constantly under development by an active community of researchers.The standard ns-2 distribution runs on Linux. However, a package for running ns-2 on Cygwin (Linux Emulation for Windows) is available. In this mode, ns-2 runs in the Windows environment on top of Cygwin as shown in the figure 1.



NS-2 provides a split-programming model; the simulation kernel is implemented using C++, while the Tcl scripting language is used to express the definition, configuration and the control of the simulation. This split-programming approach has proven benefits over conventional programming methods. Also, NS-2 can produce a detailed trace file and an animation file for each ad hoc network simulation that is very convenient for analyzing the routing behavior.

This simulation process considered a wireless network of 20 nodes which are placed within a 900m x 900m area. CBR (constant bit rate) traffic is generated among the nodes. The simulation runs for 50 Seconds. Table 4.1 shows the important simulation parameters used in the simulation process.

Table III *Salient Simulation Parameters*

Parameter	**Value**
Terrain Area	900×900 m^2
Number of Nodes	20
Propagation Model	Two-Ray Model
Transmission Range of each Node	250 m
Attack Period	2000ms
Attacker Burst Period	300, 800, 1300, 1700 (ms)
Mobility Model	Random-Waypoint
MAC Layer Protocol	IEEE 802.11
Routing Layer Protocols	DSDV, OLSR
Queue Type	DropTail/priqueue, RRED
Simulation Time	100 sec

Here, this performnace is evaluated based on different performance metrics like throughput, routing overhead, average end-to-end delay and packet delivery ratio. This is evaluated against burst period of attacker. The analysis of OLSR routing protocols is disscussed in detail:

Figure 2 illustrates the impact of DoS inter-burst duration on throughput. The simulation graph depicts that throughput under OLSR protocol with RRED active queue management technique is better than OLSR along default droptail queue. To explore low-rate DoS, we take a frequency-domain perspective and consider periodic on-off square-wave shrew or Low rate TCP-target DoS attacks that consist of short, maliciously-chosen-duration bursts that repeatwith a fixed, maliciously chosen, slow-time-scale frequency.As the graph is showing for different burst period of attacker. When burst period is small throuhput for OLSR is low. This goes on increasing as burst period is increased. When the Robust RED techniuques is applied for in simulation under DOS attack scenario. With less burst time, OLSR performs good but as burst time reaches to 600 this goes on decreaing

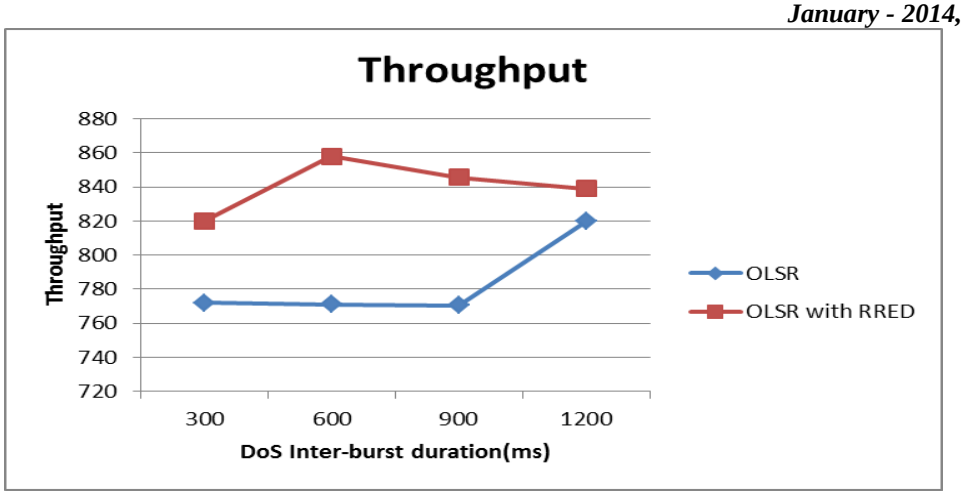


Figure 2: Imapct on throughput for Low rate TCP-target DoS attack with and without RRED on OLSR routing protocol

Figure 3 illustrates the impact of DoS inter-burst duration on routing overhead. As burst period of attacker is increasing firstly this increase very slightly for OLSR without RRED. But with the increase in burst period routing overhead goes on decreasing. When the RRED is applied on it routing overhead for OLSR decreases for less burst period of. At higher burst period scenario routing overhead for OLSR keeps on increasing.

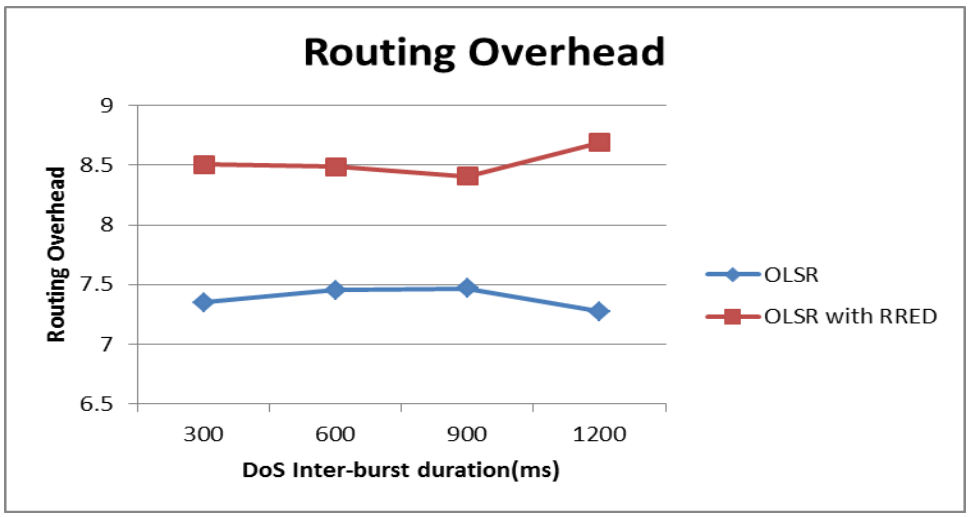


Figure 3: Imapct on routing overhead for Low rate TCP-target DoS attack with and without RRED on OLSR routing protocol

Figure 4, shows the average end-to-end delay for OLSR under TCP SYN DOS attack with and without RRED. The figure depicts that average end to end delay for OLSR goes on decreasing with increase in DoS inter-burst period of attacker and OLSR with Robust RED technique shows better results than OLSR with droptail queue management techniqe.

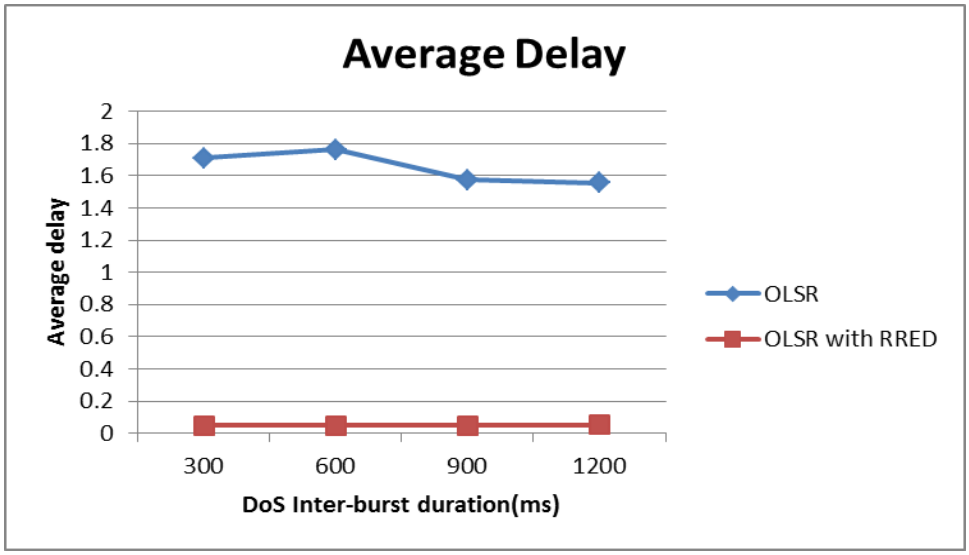


Figure 4: Imapct on average end to end delay for DOS attack with and without RRED on OLSR routing protocol

Figure 5 depicts the packet delivery ratio for OLSR under TCP SYN DOS attack with and without RRED.In this case, packet delivery ratio for OLSR with droptail is better than OLSR with RRED. This is because in this attacker send the synchronization request in unperiodic manner. The Robust RED quality of service policy enabled gateway to notifies most frequent connection consisting attacker and some other nodes that communicated through gateway. So the gateway have to discard the packets form attacker and other lower priority nodes which degrade the overall packet delivery ratio.

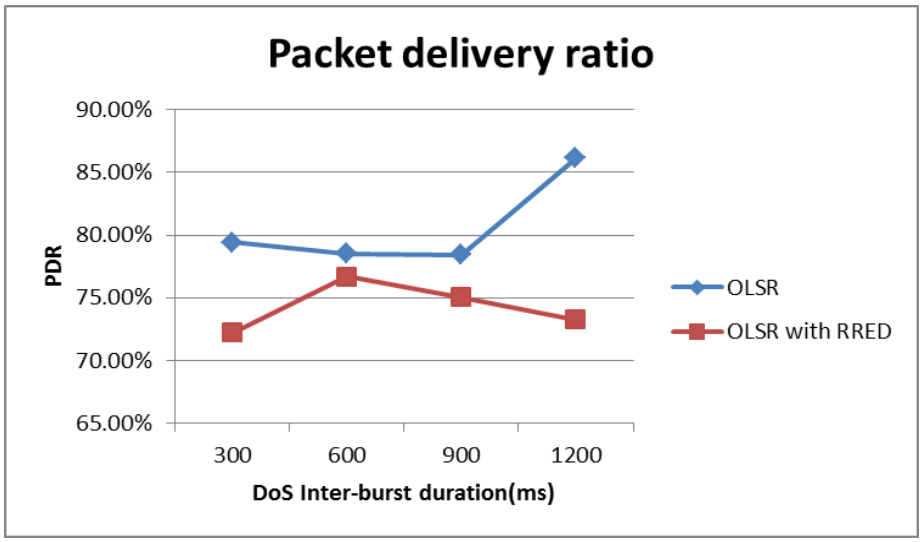


Figure 5: Imapct on packet delivery ratio for DOS attack with and without ARED on DSDV and OLSR routing protocol.

IV. Literature Review

In [1] Yih-Chun Hu, et al. had given a survey of secure wireless ad hoc routing. This paper reviews routing attacks on ad hoc networks, security in routing Protocol and discussed current approaches for establishing cryptographic keys in ad hoc networks and describes the state of research in secure ad hoc routing protocols and its research challenges

In [2] 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 [3] Rejo Mathew and Vijay Katkar analyzed that existing denial of service defense mechanisms anticipates simple attacks such as a flood of packets but Low rate denial of service attacks are difficult to detect ,which exploit the vulnerabilities of the system. Low rate DOS attacker periodically sends short burst of packets to overflow a target's source queue due to which source TCP back off to recover from congestion and retransmit after one Retransmission Time Out. Various Low rate DOS Detection methods such as dynamic detection method, periodic attack detection & modelled attack detection method , packet percentage and threshold at cache queue of target router investigation method, buffer size and shrew sending rates, detection of attacks at the edge routers, rto randomization and detection based on self- similarity, are compared under Effectiveness, Overhead, Scalable, and no impact on the legitimate traffic.

In [4] 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 heterogenous 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 [5] a survey on MANET routing protocols has been done categorizing unicast, multicast and broadcast routing algorithms. Unicast algorithms are further categorized as reactive, proactive and hybrid routing algorithms. If source and destination mobile nodes are within each other's transmission range, they can communicate with each other directly; otherwise, the intermediate nodes in between have to forward the packets for them. In such a case, every intermediate mobile node has to function as a router to forward the packets for others. Thus, routing is a basic operation for the MANET.

In [6] Z. J. Hass and others summarized the ad hoc networks routing, MAC and transport issues and explained the state-of-art of ad hoc networking technology in four areas: routing, medium access control, multicasting and security which help to understand Wireless Ad hoc Networks.

In [7], 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.

V Conclusion And Future Work

Wireless telecommunications is the transfer of information between two or more points that are not physically connected. It is having various types of fixed, mobile, and portable, cellular telephones, personal digital assistants (PDAs), etc. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometers for deep-space radio communications. A mobile Ad hoc network (MANET) is a kind of wireless Ad hoc network and is a self configuring network of mobile routers connected by wireless links the union of which forms an arbitrary topology. Security is major concern in case of MANETs. There are different security flaws and attacks on routing protocols in MANETs. In this work, reliability of OLSR under low rate TCP target Denial of Service attack is analyzed. Simulation is performed for evaluating the reliability of OLSR under different burst period of attacker scenarios with DropTail or with Robust RED active queue management technique. This is performed using performance metrics like throughput, average delay, packet delivery ratio and routing overhead. Throughput for OLSR protocol under RRED is better than OLSR with droptail technique. Average end to end delay for OLSR is much less along with RRED and also goes on decreasing with increase in burst period of attacker.Thus the results shows that robust random early detection improve the performance of mobile ad-hoc network under low rate TCP-target DoS attack.

In future other performance metrics like hop count, no of packet dropped, hop count etc. as well as other active queue management technique such as stochastic fair blue, weighted fair blue queue etc. are still to be considered for research in security area.

References

[1] Y.C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security and Privacy*, vol 2, no 3, pp 28–39, 2004.

[2] 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.

[3] Rejo Mathew and Vijay Katkar, "Survey of low rate DoS attack detection mechanisms *," Proceedings of the International Conference & Workshop on Emerging Trends in Technology,* 2011.

[4] Aleksandar Kuzmanovic and Edward W. Knightly, "Low Rate TCP Targeted Denial of Service Attacks" *SIGCOMM'03,* August 25-29, 2003

[5] H. Zhou, "A survey on routing protocols in MANETs," Technical report: MSU-CSE-03-08, March 2003.

[6] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos and S. Sajama, "Wireless Ad Hoc Networks," Encyclopedia of Telecommunications, Wiley Interscience, December, 2002.

[7] 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.

[8] Principles of wireless networks a unified approach by Kaveh Pahlavan and Prashant Tyagi, pearson education.

[9] C Siva Ram Murthy and BS Manoj "Ad hoc Wireless Networks architectures and protocols", Pearson education.

[10] K. Fall and K. Varadhan, "*The NS Manual"*, The VINT Project, UC Berkeley, January 2002.

