



Detection and Prevention of DOS Attacks Using Preventive Approach

Manraj kaur (Mtech scholar) & Parvinder Singh (Associate Professor)

ECE., Rayat institute of engineering & information technology, Rail majra technology, Rail majra

manraj.kaur@bbsbec.ac.in; er.parvinder@gmail.com

Abstract —

Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we will present survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Black hole attack and Gray hole attack which are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols. A malicious node can additionally fluctuate between good and bad behavior by alternating periods during which it forwards the data and stops forwarding them. The packet dropping attacks (Blackhole and Grayhole) may bring great harm to the performance of ad hoc networks and can also convey damage to the network's topology. So, a Novel Preventive based on clustering approach is proposed in this paper. Which will divide the traffic into number of clusters and a certification authority is defined for key distribution.

Keywords— MANETs; DSR; DOS; Preventive approach;

1. INTRODUCTION

A DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network. DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited wireless resources such as bandwidth, storage space,

battery power, CPU, or system memory. Networks and applications can be attacked by modifying routing information or changing system configuration, thereby directly attacking data integrity. DoS attack packets may use spoofed IP addresses, and can occur in different forms including buffer overflow, TCP SYN flooding, Smurf, or Viruses. For example, in TCP SYN flooding, an attacker sends multiple connection requests to a victim, exhausting all of the victim's resources and preventing use by legitimate users. The emergence of new low detection rate DoS attacks, such as low-rate TCP-targeted DoS attacks, brings new challenges to the network services.

In MANETs, nodes act as both routers and ordinary nodes. Due to dynamic network topology and lack of centralized infrastructure, network security has brought a new challenge to networking communities. Unlike traditional networks, MANETs are more vulnerable to DoS attacks due to limited resources that force nodes to be greedy in resource utilization. When there is no cooperation, activities of even a small number of nodes may significantly decrease the performance of the network. For example, a misbehaving node that discards any packets passing through it can result in repeated retransmissions, which in turn cause network congestions. Also, a wireless link does not provide the same protection for data transmissions as does its wired link counterpart. Hence, any user or receiver within the transmissions range can eavesdrop or interfere with data packets or routing information. Battery power is another critical resource for mobile nodes. If the battery power has been used up due to malicious attacks such as the sleep

deprivation attack, the victim will not be able to provide network services. Since all nodes can be mobile, changes in network connectivity and resource availability also expose a network to various attacks. This calls for detection and prevention of attacks in the network.

2. ATTACKS IN MANET

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

- 1) **Availability:** Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.
- 2) **Confidentiality:** Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.
- 3) **Integrity:** Integrity means that assets can be modified only by authorized parties or only in authorized way.. Integrity assures that a message being transferred is never corrupted.
- 4) **Authentication:** Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.
- 5) **Authorization:** This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

6) **Resilience to attacks:** It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

7) **Freshness:** It ensures that malicious node does not resend previously captured packets.

2.1 Classification of security Attacks

The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack.

- 1) **Passive attacks:** A passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.
- 2) **Active attacks:** Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc.

2.2 Types of Active Attacks on Various in Layers:

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay

	attacks, Link Withholding, Resource Consumption Attack, gray hole Attacks.
Data Link	Selfish misbehavior, malicious behavior, traffic analysis
Physical	Eavesdropping, jamming, active interference

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

A. Attacks at Physical Layer: Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

- 1) **Eavesdropping:** It can also be defined as interception and reading of messages and conversations by unintended receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.
- 2) **Jamming:** Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets.

B. Attacks at Data link layer: The data link layer can classified attacks as to what effect it has on the state of the network as a whole.

- 1) **Selfish Misbehavior of Nodes:** The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and to conserve of battery power.
- 2) **Malicious Behavior of nodes:** The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between

neighboring nodes. Attacks of such type are fall into following categories.

3) **Denial of Service:** The prevention of authorized access to resources or the delaying of time-crit(DoS) operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using the desired resources and attempts to “flood” a network, thereby preventing legitimate network traffic.

4) **Misdirecting traffic:** A malicious node advertises wrong routing information in order to get secure data before the actual route.

5) **Attacking neighbor sensing protocols:** Malicious nodes advertise fake error messages so that important links interface are marked as broken.

C. Attacks at Network Layer: The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

1) **Blackhole Attack:** In this type of attacks, malicious node claims having an optimum route to the node whenever it receives RREQ packets, and sends the REPP with highest destination sequence number and minimum hop count value to originator node .whose RREQ packets it wants to intercept.

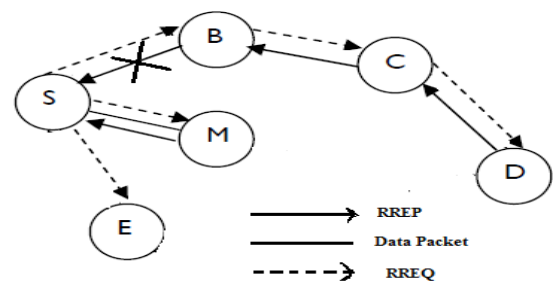


Fig. 1.1: Blackhole Attack

2) **Rushing Attack:** In rushing attacks when compromised node receives a route request packet

from the source node, it floods the packet quickly throughout the network before other nodes.

- 3) **Wormhole Attack:** In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole.

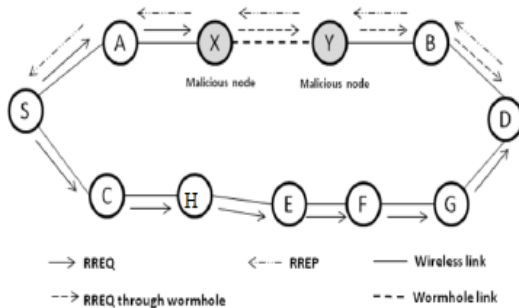


Fig 1.2: Wormhole Attack

- 4) **Greyhole attack:** In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. It is similar to blackhole attack but it drops data packet of a particular node.

D. Attacks at Transport Layer

- 1) **Session Hijacking:** Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup.

E. Attacks at Application Layer

- 1) **Malicious code attacks:** Malicious code attacks include, Viruses, Worms can attack both operating system and user application.

3. PROPOSED WORK

In mobile ad hoc networks, denial of service (DoS) is an attack in which a user is denied of the services of a resource he would normally expect to have. The denial of service can be done at different layers (physical, network, application, etc). At the network level, malicious nodes can perform several types of attacks such as Wormhole and Blackhole/ Grayhole attack, etc. For instance, a node may forward control packets (e.g., RREQ packets) but does not forward data

packets. The aim of this malicious node is to be considered as an intermediate node on the path between source and destination in order to cause a denial of service. A node can also preserve its resources when it does not forward data or control packets. A malicious node can additionally fluctuate between good and bad behavior by alternating periods during which it forwards the data and stops forwarding them. The packet dropping attacks (Blackhole and Grayhole) may bring great harm to the performance of ad hoc networks and can also convey damage to the network's topology. So, a Novel Preventive based on clustering approach is proposed.

3.1 Basic Design of Proposed Work:

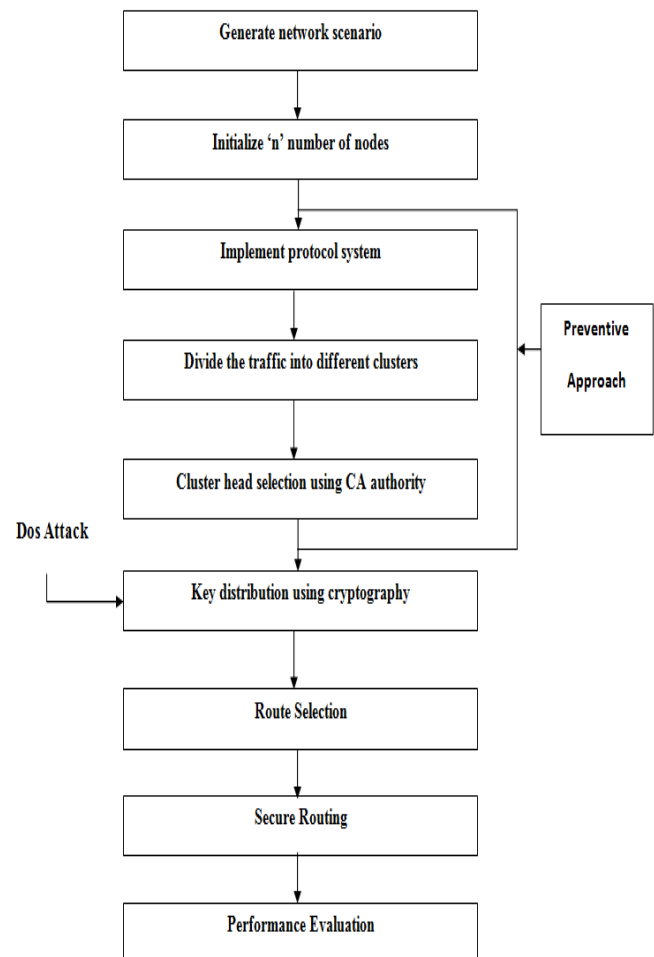


Figure 1.3: Flow chart of proposed work

3.2 Proposed Algorithm:

Input: no_of_nodes, no_of_clusters, CA

Output: Secure_data_transmission

Start

{

Initialize network with 'n' no_of_nodes

Size_network = area of network

no_of_clusters = 3

Size_of_cluster=

size_of_network/no_of_clusters

cluster_formation

{

Divide the network into different clusters

According to size_of_cluster;

}

Initialize CA

cluster_head_selection

{

CA checks the Trust_value of nodes of a particular cluster

Trust_value = previous transmission of nodes

CH $\leftarrow$ Max(Trust_value)-node

}

Key_distribution

{

CH gets certificate from CA

CH generate keys by using certificate distribute to each node of cluster

The following is the algorithm for key distribution

Node(i) $\leftarrow$ key(i)

Transmission

{

If within the clusters

Check key

If found in CH data

Then

Check key

If found in CH data

then

start

else

check neighbour cluster

if found

then

start

else

stop

}

In this approach, nodes are divided into number of clusters named as 0,1 and 2. One of the node is provided with the authority of certification which means that this node will distribute the encryption keys to all other nodes in the network. This key will help to distinguish between the honest node and malicious node. If any of the node will try to enter in the defined clusters there will be a key check point to enter. No malicious node would be allowed to interrupt the network. Cluster heads are declared on the basis of trust values which is calculated with keeping in account last transmission records. Now, three of the clusters have respective cluster channels for controlling their cluster member nodes. Malicious nodes would be detected with the help of key check. This is how our approach will gain more packet delivery ratio because there will be no loss of any

message in the network. More PDR will result in less delay and better throughput.

4. IMPLEMENTATION

To implement this proposed solution we used Network Simulator 2. We test this proposed algorithm to different network scenario but here only discussed the scenario of 50 nodes with 1800x1400 areas. Manet scenario is generated by using NS-2 with this defined configuration using DSR protocol and comparison of existing work with the proposed work. The network setup is defined below in table 1.

Table 1: Simulation Setup

Network Parameters	Values
Channel	Wireless
Radio propagation model	Two ray ground
Network interface type	Physical/wireless physical/802_15_14
MAC type	802.11
Interface Queue Type	Droptail/Priority queue
Link Layer Type	LL
Antenna Model	Omni Antenna
Queue length	50
No.of nodes	50
Routing protocol	DSR
Area	1800*1400
Simulation time	100s

Implementation in ns-2

NS-2 is used to simulate the real moving behaviours of the nodes in a mobile ad hoc network. The evaluation will be conducted with some specific number of nodes that will be randomly scattered in a specific region with specific number of connections. Figure 4.1 shows the MANET Environment generated by using NS-2.

Node Placement

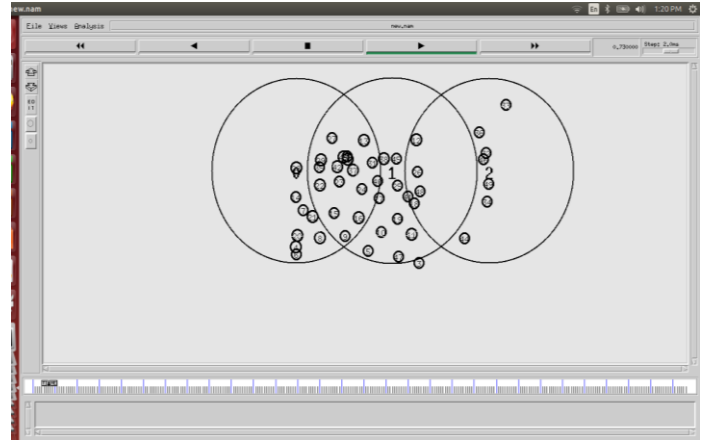


Figure 1.4 This shows how nodes are placed in ns-2

Key distribution of CA authority

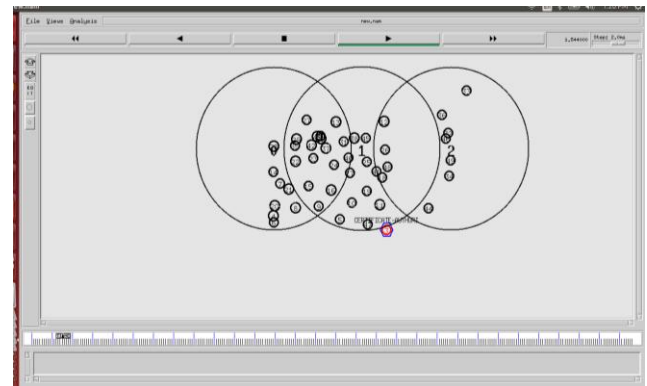


Figure 1.5 Cluster authority is given to one node in the network of 50 nodes.

Cluster heads

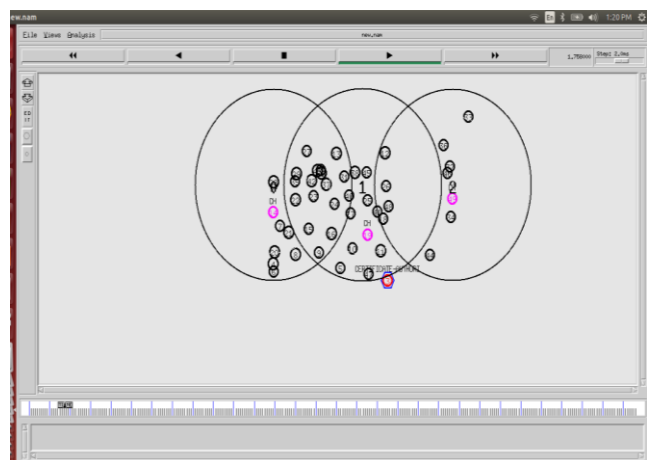


Figure 1.6 In all three clusters their cluster heads are defined which are of pink color.

5. Results & Discussion

To simulate the real moving behaviours of the nodes in a mobile ad hoc network a simulation tool will be used. The evaluation will be conducted with some specific number of nodes that will be randomly scattered in a specific region with specific number of connections. This simulation evaluates the protocol using the following performance metrics:

- Packet delivery Ratio
- Throughput
- End to End Delay

Packet Sent: It is the number of packets sent by the application layer of source nodes.

Packet received: It is the number of packets received by the application layer of destination nodes.

Routing Overhead: The total number of routing control packets generated by all nodes to the total data packets during the simulation time.

Network Load: It is the total traffic received by the network layer from the higher MAC that is accepted and queued for transmission. It is measured as bits per second.

Packet delivery Ratio (PDR): It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

$$PDR = (P_r / P_s) * 100$$

Where, P_r is total packet received and P_s is total packet sent.

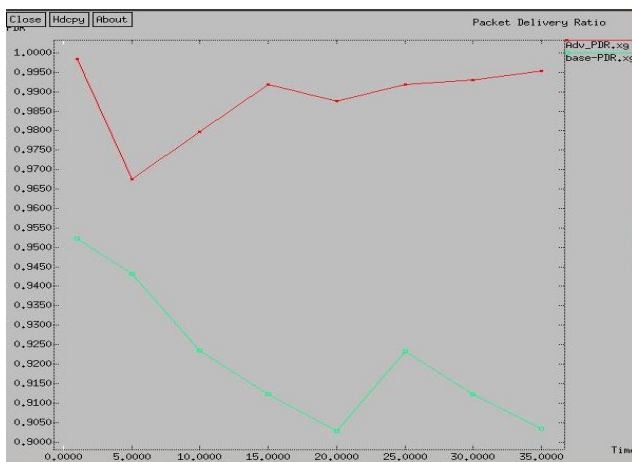


Figure 1.7: Packet delivery ratio is more for the improved scenario.

If any of the node will try to enter in the defined clusters there will be a key check point to enter. No malicious node would be allowed to intrude the network. Cluster heads are declared on the basis of trust values which is calculated with keeping in account last transmission records. Now, three of the clusters have respective cluster channels for controlling their cluster member nodes. Malicious nodes would be detected with the help of key check. This is how our approach will gain more packet delivery ratio because there will be no loss of any message in the network.

Throughput: It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation .

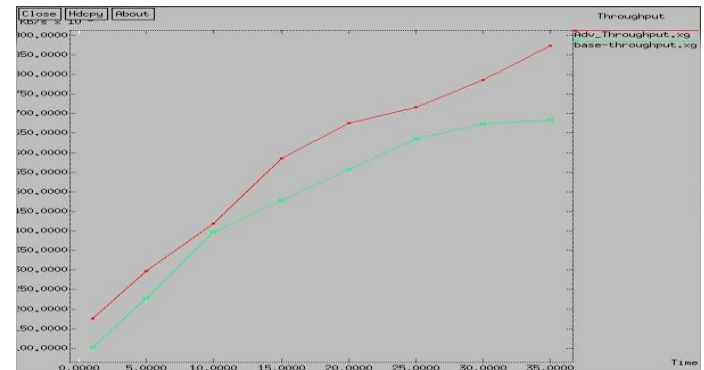


Figure 1.8: Throughput is more for the improved scenario.

Improved packet delivery ratio stands for more transmission of packets across the network as in the last graph our results ensured the improved PDR which will definitely help in increasing the over all throughput of our system.

End to End Delay: This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D = (T_r - T_s)$$

T_r is receive time and T_s is sent time of the packet.

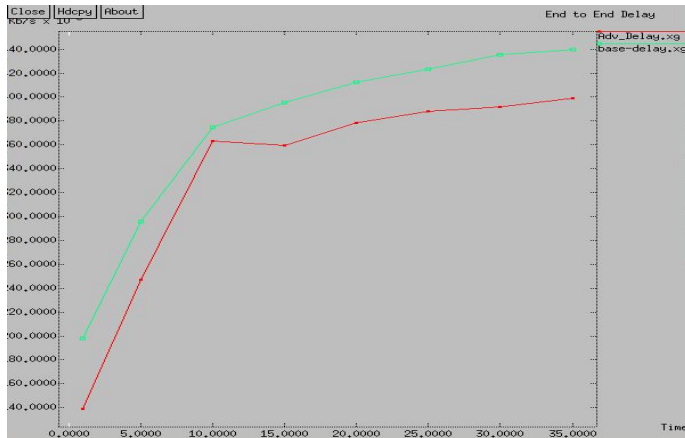


Figure 1.9: Delay is less in Improved approach.

5. CONCLUSION

In this paper, we proposed a preventive approach for detecting and preventing DoS attacks in MANETs. A clustering architecture was proposed for performing reputation data management in a localized and distributed manner. DoS attacks were detected through collaborative monitoring and information exchange. Reputation rating was carried out using neighbourhood and cluster level information with more weight given to a node's own observation. In this mechanism, selections are made probabilistically among the eligible nodes that are on the path to the destination. We used the simulation technique to evaluate network performance in the presence of misbehaving nodes. Our simulation results indicated that the preventive approach is effective in tackling DoS attacks that occur due to selfish and malicious nodes. Future work includes the investigation of Distributed Denial of Services (DDoS) in MANET and integrated wireless networks. In future study we will try to invent such security algorithm will be installed along with routing protocols that helps to reduce the impact of different attacks.

REFERENCES

- [1] M. Rmayti, Y. Begriche and R. Khatoun, L.Khoukhi, D. Gaiti" Denial of Service (DoS) Attacks Detection in MANETs Using Bayesian Classifiers" 978-1-4799-8030-7/14/\$31.00 ©2014 IEEE.
- [2] Yajuan Tang, XiapuLuo, Qing Hui, and Rocky K. C. Chang" Modeling the Vulnerability of Feedback-Control Based Internet Services to Low-Rate DoS Attacks" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 3, March 2014.
- [3] Wei Liu, Member, IEEE, and Ming Yu, Senior Member" Aasr: Authenticated Anonymous Secure Routing For Manets In Adversarial Environments" IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.
- [4] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member" Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" IEEE Stems Journal, Vol. 9, No. 1, March 2015.
- [5] AvitaKatal, Mohammad Wazid , R H Goudar, and D P Singh" A Cluster Based Detection and Prevention Mechanism against Novel Datagram Chunk Dropping Attack in MANET Multimedia Transmission" 978-1-4673-5758-6/13/\$31.00 © 2013 IEEE.
- [6] AlbandariAlsumaytand John Haggerty" A survey of the mitigation methods against DoSattacks on MANETs"Science and Information Conference 2014\ August 27-29, 2014 | london, UK.
- [7] QuanJia, Kun Sun and AngelosStavrou" CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET" " 978-1-4673-5758-6/13/\$31.00 © 2011 IEEE.
- [8] SoufieneDjahel, FaridNa"it-abdesselam, and Zonghua Zhang" Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges" IEEE CommunicationsSURVEYS &TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.
- [9] YinghuaGuo and Matthew Simon" Network forensics in MANET: traffic analysis of source spoofed DoS attacks" 978-0-7695-4159-4/10 \$26.00 © 2010 IEEE.
- [10] Jieying Zhou, Jianfeng Chen, WeicongXie, and Jing Li" Improved Weight Clustering Algorithm for IDS in Mobile Ad hoc Network" 1-4244-1312-5/07/\$25.00 © 2007 IEEE.
- [11] Yongjin Kim, Vishal Sankhla, and AhmedHelmy" Efficient Traceback of DoS Attacks using Small Worlds in MANET" 0-7803-8521-7/04/\$20.00 © 2004 IEEE.
- [12] L. Buttyan and J. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).
- [13] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks," <http://www.stanford.edu/~yl31/adhoc> (2001).
- [14] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks," <http://www.stanford.edu/~yl314/adhoc> (2002).
- [15] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheatproof, credit-based system for mobile ad-hoc



networks,” Technical Report 1235, Department of Computer Science, Yale University (2002).

[16].S. Marti, T.J. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” In: Mobile Computing and Networking. (2000) 255–265.

[17] S. Buchegger and J.Y.L Boudec, “Performance Analysis of the CONFIDANT Protocol: Cooperation Of Noes — Fairness In Distributed Ad-hoc NeTworks,” In Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, IEEE (2002) 226– 236.

[18] P. Michiardi and R. Molva, “Making greed work in mobile ad hoc networks,” Technical report, Institut Eur’ecom (2002).

[19] A. Kuzmanovic and E.W. Knight, “Low-Rate TCP-Targeted Denial of Service Attacks,” SIGCOMM’03, August 25-29, 2003.

[20] A.D. wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” IEEE October 2002.

[21] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy efficient communication protocol for wireless micro-sensor networks”, In Proc. of IEEE Hawaii Int. Conf. on System Sciences, pages 4-7, January 2000.

[22] S. McCanne and S.Floyd., Network Simulator. [Http://www.mash.cs.berkeley.edu/ns/](http://www.mash.cs.berkeley.edu/ns/).

[23] M.K. Denko, “An Incentive-Based Service Differentiation in Mobile Ad Hoc Networks”, In Proc. IEEE International conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005), pp. 197-204, August 2005, Montreal, Canada.

[24] M.K. Denko, “A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks”, In Proc. IFIP INTELLCOMM’05, Montreal, Canada.