A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network

Prajeet Sharma
M.Tech Scholar
Computer Science & Engg Dept
RKDF IST, Bhopal M.P, India

Niresh Sharma
Head of Department
Computer Science & Engg Dept
RKDF IST, Bhopal M.P, India

Rajdeep Singh
Assistant Professor
Computer Science & Engg Dept
RKDF IST, Bhopal M.P, India

ABSTRACT
Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

General Terms
Security, algorithms, distributed denial of attack, intrusion detection system.

Keywords
Wireless mobile ad-hoc network, security goal, security attacks, defensive mechanisms, challenges, DDoS attack.

1. INTRODUCTION
Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self routing capability nature, there are many weaknesses in its security. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection [1] and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS[2] is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

2. RELATED WORK
The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV & DSR. Wei-Shen Lai et al [3] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [4] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique. Giriraj Chauhan and Sukumar Nandi [5] proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. Xiapu Luo et al [6] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Xiaoxin Wu et al [7] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification Ping. S.A.Arunmozhi and Y.Venkataramani [8] proposed a defense scheme for DDoS attack in which they use MAC layer information like frequency of RTD/CTS packet, sensing a busy channel and number of RTS/DATA retransmission. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [9] proposed DDoS flooding attack detection through a step-by-step

investigation scheme in which they use entropy-based detection mechanism against DDoS attacks in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu [10] proposed a Confidence-Based Filtering method (CBF) to detect DDoS attack in cloud computing environment. In which anomaly detection is used and normal profile of network is formed at non attack period and CBF is used to detect the attacker at attack period.

3. ATTACK ON AD HOC NETWORK

There are various types of attacks on ad hoc network which are describing following:

3.1 Wormhole

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [11]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

3.2 Blackmail

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [12]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [13].

3.3 Routing Table Poisoning

Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [14]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

3.4 Replay

A replay attack is performed when attacker listening the conversation or transaction between two nodes and put important massage like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender.

3.5 Location Disclosure

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [15] or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

3.6 Black Hole

In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [16]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

3.7 Denial of Service

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [14]. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

3.8 Distributed Denial of Service

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

3.9 Rushing Attack

Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [17]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

3.10 Masquerade

It is an intruder who gain the privilege of any one system as an authenticate user by stolen user password, through finding security gaps in programs, or through bypassing the authentication mechanism.

3.11 Passive Listening and traffic analysis

The intruder could passively gather exposed routing information. Such an attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be

protected. However, the confidentiality of user data is not the responsibility of routing protocol.

4. PROBLEM STATEMENT

DDOS attack is the main problem in all ad hoc scenario i.e. in MANAT and as well as in wireless sensor networks. In the Paper with reference no. [18] Has an intrusion detection system in wireless sensor network which uses the anomaly intrusion detection system in which IDS uses two intrusion detection parameters, packet reception rate (PRR) and inter arrival time (IAT). But only these two parameters are not completely sufficient for intrusion detection in wireless sensor network and as well as in MANET. If we also add other parameters into it to make it works more accurately. So in our proposal we use different intrusion detection parameters in mobile Ad hoc networks. We assume that a mobile ad hoc network contains two or more than two mobile devices that are communicate from each other through intermediate nodes, each node contain routing table , in our proposal we use AODV routing protocol in all normal module attack module and IDS (intrusion detection system) for prevention through attack. In this paper we simulate the three different condition results normal time, Attack time and IDS module time through NS-2 simulator.

5. CRITERIA FOR ATTACK DETECTION

Here we use thirteen mobile nodes and simulate through three different criteria NORMAL case, DDOS attack case and after IDS intrusion detection case.

5.1 Normal Case

We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

5.2 Attack Case

In Attack module we create one node as attacker node whose set the some parameter like scan port , scan time , infection rate , and infection parameter , attacker node send probing packet to all other neighbour node whose belongs to in radio range, if any node as week node with nearby or in the radio range on attacker node agree with communication through attacker node, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the DDOS (distributed denial of service) attack and infect to next other node that case our overall network has been infected.

5.3 IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

6. ALGORITHMS

```
Create node =ids;

Set routing = AODV;

If ((node in radio range) && (next hop! =Null)

        {

                Capture load (all_node)

 Create normal_profile (rreq, rrep, tsend, trecv, tdrop)

                {pkt_type;          // AODV, TCP,
CBR, UDP

                 Time;

                 Tsend, trecv, tdrop, rrep, rreq

                }

 Threshold_parameter ()

     If ((load<=max_limit) &&
(new_profile<=max_threshold) &&
(new_profile>=min_threshold))

         {

        No any attack;

          }

Else {

         Attack in network;

        Find_attack_info ();

    }

   Else {

 "Node out of range or destination unreachable"

        }

Find_attack_info ()

        {

        Compare normal_profile into each trace value

                If (normal_profile! = new trace_value)

                        {

                                Check pkt_type;

                                Count unknown
pkt_type;

                                Arrival time;
```

Sender_node;

Receiver_node;

Block_Sender_node();
//sender node as attacker

}

In our algorithm firstly we create an IDS node in which we set AODV as a routing protocol. Then after the creation, our IDS node check the network configuration and capture lode by finding that if any node is in its radio range and also the next hop is not null, then capture all the information of nodes. Else nodes are out of range or destination unreachable. With the help of this information IDS node creates a normal profile which contains information like type of packet, in our case (protocol is AODV, pkt type TCP, UDP, CBR), time of packet send and receive and threshold. After creating normal profile and threshold checking is done in the network i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold then there is no any kind of attack present. Else there is an attack in the network and find the attack. For doing it compare normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. And after detection of any anomaly in that parameters then block that packet sender node (attacker node).

7. SIMULATION ENVIROMENT

The simulation is implemented in Network Simulator 2.31[19], a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen 35 m/s. A packet size of 512 bytes and a transmission rate of 4 packets/s,

- Performance Metrics**:** In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one [20]. The following metrics were considered for the comparison were

  a) Throughput: Number of packets sends in per unit of time.

  b) Packet delivery fraction *(PDF):* The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

  c) End to End delay*:* - Measure as the average end to end latency of data packets.

  d) Normalized routing load: Measured as the number of routing packets transmitted for each data packet delivered at the destination.

TABLE I Simulation Parameters for Case Study

Examined Protocol	AODV
Number of nodes	13
Dimension of simulated area	800×600
Simulation time (sec)	35
Radio range	250m
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512
Number of traffic connections	TCP/UDP
Maximum Speed (m/s)	35
Node movement	random
Types of attack	DDOS

8. RESULTS AND DISCUSSION

TABLE II Overall summary of Results in all Cases

Parameter	Normal Case	Attack Case	IDS Case
SEND	828	533	844
RECEIVE	804	482	812
ROUTING PACKETS	99	219882	174
PACKET DELIVRY FRACTION	97.1	90.43	96.21
THROUGHPUT	107.815	58.13	87.57
NORMAL ROUTING LOAD	0.12	456.19	0.21
AVERAGE END TO END DELAY	852.04	751.64	830.31
No. Of dropped data(packets)	23	51	29
No. Of dropped data(bytes)	23852	44556	28628

According to performance analysis in normal case, in attack case and in IDS case we observe that DDOS attack definitely affected the network and our scheme is successfully defence the network and also provides the protection against them. In case of attack we observe that the routing load is very high because attacker node are continuously transmit the routing packets to their neighboured and every node in network are reply to attacker node by that heavy congestion is occur. Packet delivery fraction and end to end delay are also goes low, which shows that packets are not deliver accurately and number of dropped data is goes high approximately twice to the normal condition.

8.1 UDP Packet Analysis.

In UDP packet analysis we observe that the packet loss is more in the time of attack. But after applying IDS again the number of packets delivery increases. At the time of attack number of UDP packet received is near about 24 but at the time of normal and IDS time it is 37, 35 respectively.

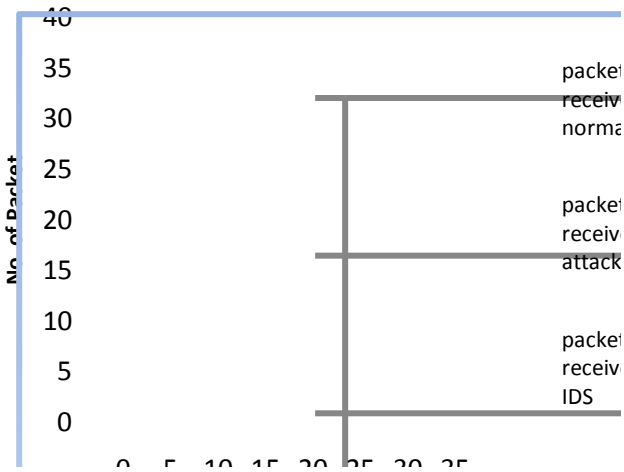

Fig. 1 UDP packet analysis

8.2 UDP Packet loss Analysis

This graph shows the loss of UDP packets in all three cases. At the normal time UDP packet loss is near about negligible and at the time of attack it goes very high, where at the time of IDS it only goes to 2 packets.

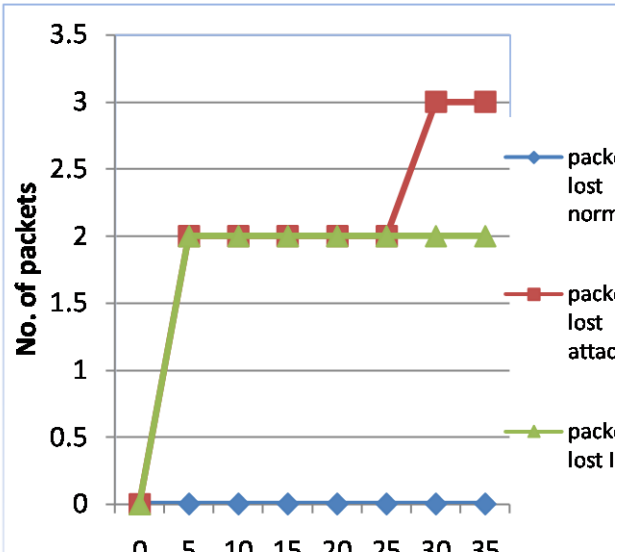

Fig. 2 UDP Packet loss Analysis

8.3 TCPP Packet Analysis

This graph represents the loss of TCP Packets in the time of attack. But after applying IDS the packet loss is minimizes and packet delivery increases. At normal time receiving of TCP packet is near about 34 packet and at IDS time it goes to near about 27 packets but at the time of attack it goes very low i.e. 2 packets.

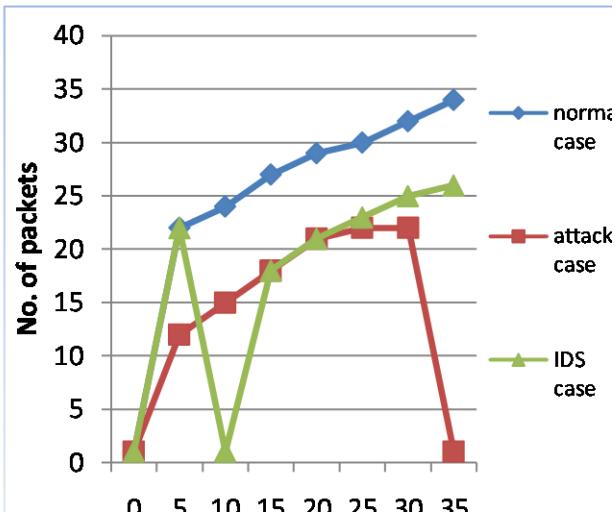

Fig. 3 TCP congestion window analysis.

8.4 Throughput Analysis

At the time of attack throughput decreases due to congestion in network. This graph represents after applying IDS throughput increases. At the normal time and at IDS time throughput is near about 107 and 85 respectively. But at attack time it goes down near about 50.

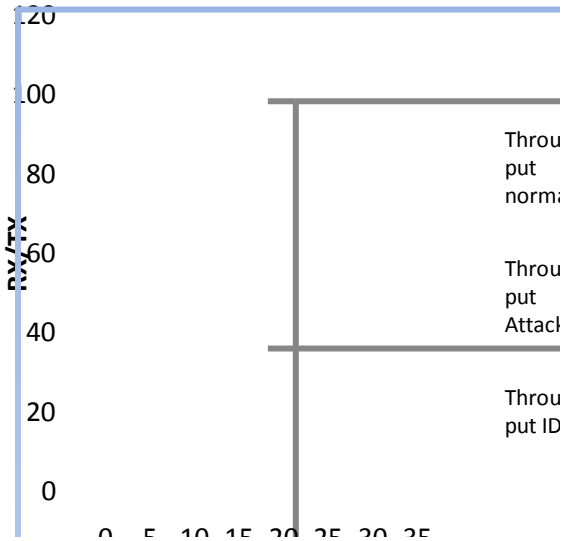

Fig. 4 Throughput Analysis

8.5 Routing load Analysis.

This graph represents the routing load; in case of attack it is very high this is the main reason of congestion occurs in the network. After applying IDS routing load is in under control. At normal and IDS time routing load is approximately negligible but at the time of attack it goes to near about 15000 packets.

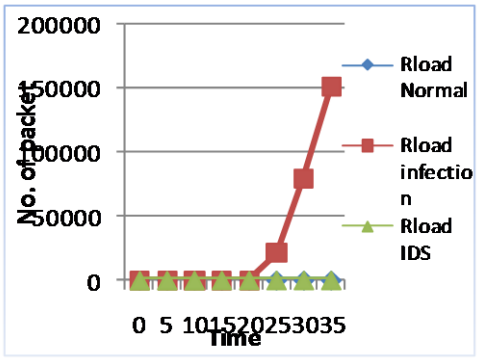

Fig.5 Routing load analysis

9. CONCLUSION

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

10. ACKNOWLEDGMENTS

It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed Mr. Rajdeep Singh, and Niresh Sharma HOD (CSE) R.K.D.F.I.S.T., Bhopal. His invaluable guidance, inspiration, constant encouragement sincere criticism and sympathetic attitude could make this paper possible.

11. REFERENCES

[1] F. Anjum, D. Subhadrabandhu and S. Sarkar. Signaturebased intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[2] D. E. Denning, An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[3] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[4] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008)

[5] Giriraj Chauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[6] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)

[7] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)

[8] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[9] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim "DDoS flooding attack detection through a step-by-step investigation" 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011

[10] Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu " CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4.2011

[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003

[12] Patroklos g. Argyroudis and donal o'mahony, "Secure Routingfor Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.

[13] Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1): Issue (1) 56

[14] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of ServiceResilience in Ad Hoc Networks," Proc. MobiCom, 2004.

[15] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[16] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.

[18] Ponomarchuk, Yulia and Seo, Dae-Wha, "Intrusion Detection Based On Traffic Analysis in Wireless Sensor Networks" IEEE 2010.

[19] Network Simulator- ns-2. http://www.isi.edu/ nsnam /ns/.

[20] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004), Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications, 11(1), 38-47.