2016 Symposium on Colossal Data Analysis and Networking (CDAN)

Mitigating Dynamic DoS Attacks in Mobile Ad Hoc Network

Bhavin Joshi
Information Technology Department
U. V. Patel College of Engineering, Ganpat University
Mehsana, India

Nikhil Kumar Singh
Information Technology Department
U. V. Patel College of Engineering, Ganpat University
Mehsana, India

Abstract— **Mobile ad hoc networks operate without any fixed infrastructure and centralized administration. It is an autonomous system of wirelessly connected mobile nodes having the capability to operate as host and router as well. The dynamic nature of ad hoc network increases the topology designing challenges. Security is an important and essential requirement in Mobile Ad-hoc Networks (MANET). MANETs are more vulnerable to security attacks as compared to wired networks due to lack of a centralized authority, dynamic network topology, easy eavesdropping and low bandwidth. Although many types of security attacks have been studied in MANETs, like black hole attack, wormhole attack, jellyfish attack, Denial of service attack, rushing attack, sinkhole attack, Dynamic denial of service attack, but the most pioneered attack is a dynamic denial of services attack (dDoS) because of their potential impact. In dDoS attack, the malicious node continuously sends RREQ to victim node and makes it as busy as possible. So, that node cannot process the legitimate RREQ coming from another node. So, here we have proposed one solution against dDoS attack. The proposed method uses packet delivery ratio, number of route request per unit time to find whether this node is malicious one or not. If the node is found malicious one then node manager will inform to all other node in transmission range.**

Keywords- Manet; ad-hoc network; DOS; DDOS; AODV

I. INTRODUCTION

In the field of wireless networks, Mobile Ad-hoc Network (MANET) is a type of network which operates in the absence of fixed infrastructure [1]. MANET is a collection of arbitrary self-organized nodes which is easy to deploy at any place and at any time. The nodes can communicate directly if they are within the radio range of each other, otherwise communicates with each other using multi-hop routing. Hence, each node in a MANET works both as a router and a host which uses forwarding of packets to the given node in the network, once a route is established. However, MANETs are susceptible to many attacks like black hole attack, gray hole attack, Dynamic denial of service attack and wormhole attack, especially due to their dynamic network topology, easy eavesdropping, Ad-hoc and decentralized nature [2] [3]. All these attacks are targeted at damaging the routing of control and data packets which makes MANETs, insecure and unusable.

978-1-5090-0669-4/16/$31.00 © 2016 IEEE

Reactive routing protocols like Ad-hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance-Vector (DSDV) etc. are susceptible to many attacks [4]. Among these attacks, Dynamic denial of service attack is most severe because of its potential impact [1]. A Dynamic Denial of Service (dDoS) attack is an attack that provides network resources unavailable to legitimate users. The aim of this attack is to exhaust the network resources [5]. In this paper, throughout analysis of this attack, dDoS attack is implemented on AODV and a solution is provided against this attack.

A. MANET Features

In MANET, each mobile terminal functions as both: a host and a router. So usually end user devices and switches are indistinguishable in MANET [6].

Ad-hoc routing algorithms can be single-hop or multi-hop, depending on the link layer attributes and routing protocols. In terms of structure and implementation, Single-hop MANET is simpler than multi-hop. Delivering of data packets from source to destination in the direct wireless transmission range, should be forwarded via one or more intermediate nodes [7].

Due to the mobility of nodes, the topology changes rapidly and unpredictably. MANET needs to adapt the traffic, propagation conditions as well as the moving patterns of the nodes. The mobile nodes dynamically create the route among themselves as they move i.e. they form their own network on the fly [8].

In general MANET nodes are mobile devices with less processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms which reduce computing and communication cost [8].

B. MANET Applications

With the rapid growth of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance for widespread applications. The applications of MANET are diverse, ranging from large-scale to small scale and mobile to static networks. Besides the legacy applications that move from traditional

infrastructure environment into the ad hoc context, a great deal of new services that can be generated for the new environment are –

1) *Military Battlefield:* Ad hoc networking allows the military to maintain an on demand information network between the soldiers, vehicles, and military information headquarters [9].

2) *Commercial Sector*: In emergency rescue operations where communications infrastructure is damaged or non-existing and rapid deployment of a communication network is needed [10].

3) *Local Level:* Ad hoc networks can be used to spread and share information among participants at temporary multimedia network e.g. conference or classroom. Similarly civilian environments like taxicab, sports stadium, boat, small aircraft etc. are the local level applications of mobile ad hoc communication [10].

4) *Personal Area Network (PAN):* Short-range MANET simplifies the communication between various mobile nodes. Such an ad hoc network can also be extended to the Internet access or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context [10].

C. Mobile Ad-hoc Networking Protocols

The topology of an ad-hoc network is consistently changing which is very difficult for routing process. There are two main approaches for routing process in ad hoc networks. The first approach is a pro-active approach which is table driven and uses periodic protocols. It means every node has table with routing details that are updated in regular intervals. The second one is re-active, source-initiated or on-demand approach in which every time a message is sent, first it has to find a path by searching the entire network. Various protocols have various routing aspects other than finding a short path, which are low communication overhead and load-balancing. The AODV, TORA and DSR are source-initiated or on-demand routing protocols and DSDV is a table driven protocol. Some general ad hoc routing protocols are explained as below-

1) Destination - Sequenced Distance Vector[11]

Destination Sequenced Distance Vector (DSDV) is a type of pro-active routing protocols. It is based on Bell-man-Ford routing algorithm. DSDV also contains the characteristic of distance vector protocol in which each node has a routing table containing the next-hop information for each and every possible destination. Routing information is delivered via broadcast. Any updates in topology are transmitted periodically or immediately. Packets are transmitted between the stations by using routing tables available at each station of the network.

2) Ad-Hoc On Demand Distance Vector Routing

Ad hoc On-Demand Distance Vector (AODV) is a class of reactive routing protocol for mobile ad hoc networks [4, 12, 13, and 14]. This protocol discovers a route to the destination only if it is required. This protocol floods the Route Request packet (RREQ) when the route is not available in its routing table for the desired destination. Their neighbors accept that RREQ and provides the latest path for that node to the destination if they have otherwise they will rebroadcast RREQ. Latest path in the given node has a sequence number (SeqNum) greater than or equal to a SeqNum of RREQ [3]. A node updates its path information in its routing table only if the SeqNum of the current packet received is greater than the last SeqNum stored at the node. This process continues until the RREQ packet reaches the destination node or an intermediate node that has a latest route.

3) Temporally-Ordered Routing Algorithm

Temporally-Ordered Routing Algorithm (TORA) protocol belongs to the class of reactive protocols. TORA is highly adaptive, efficient and is used to maintain the temporal order. This protocol minimizes the reaction of topological changes using temporal order. TORA protocol only needs to maintain the neighboring nodes information. This protocol is source initiated and creates a set of routes quickly to the desired destination. The protocol has basically three functions through the use of three different control packets such as query (QRY), update (UPD) and clear (CLR). The QRY packets are used for creating and maintaining the routes, and CLR packets are used for deleting the routes.

4) Dynamic Source Routing

Dynamic Source Routing (DSR) is a class of reactive protocols which allows us to dynamically explore a route across multiple network nodes to any desired end. The Source routing means that every packet in the header contains the ordered list of nodes across which the packet must pass. In DSR there is no periodic routing of messages, thereby reducing network bandwidth overhead, conserve battery power and avoid large routing updates throughout the ad-hoc network.

The rest of the paper is organized as follows. The following section describes past efforts related to DoS attacks in Mobile ad-hoc networks. In the Section III, we explain our proposed approach. Section IV presents the evaluation results and analysis of the proposed approach. Section V offers conclusions of the paper.

II. LITERATURE SURVEY

Here we have discussed the various approaches proposed by authors to mitigate various possible attacks in mobile Ad-Hoc networks.

In paper [15] the authors Ramratan Ahirwal and Leeladhar Mahour presented a method for determining intrusion or misbehave in MANET using intrusion detection system and protect the network from distributed denial of service (DDOS). They analyzed the result on the basis of actual TCP flow monitoring, routing load, packet delivery ratio and average end-to-end delay in normal, DDoS attack and IDS time. The advantage of this approach is their IDS has recovered the data.

In [16] Minda Xiang et. al have provided a solution for mitigating dynamic denial of service attack. They are using hierarchical structure for preventing network from DDOS attack. It uses two monitor nodes called RPN (Remote Protection Node) the node that is the first hop from the source node will be assigned as a protection node and LPN(Local Protection Node) is protecting destination from the bogus packet. Here each higher level node is protected by each lower level node. When any source node sends packet for particular node at that time each packet will go through the LPN. So, if any malicious activity found by the LPN then it will discard those packet and notify about it by Attack Notification Message (ANM) to the higher level node. Then, higher level node notifies to RPN about that node by broadcasting an Attack Information Message (AIM) packet. So, all the RREQ coming from this node will be dropped by RPN. Hence, it prevents against DDOS attack in network [16].

In [17] Rizwan Khan and A. K. Vatsa has implemented new architecture of Detection and control of DDoS attacks in MANET. This architecture consists of Monitor, Reputation System, Trust Manager/Co-operation system and Path Manager. Advantage of this approach is that it improves the overall network performance and functionality by prevention, detection and control of DoS and DDoS attack [18].

The authors Hwee-Xian et. al. have compared the statistical filtering defense mechanism for DDOS attack on wired and wireless network in paper [19]. They have discussed the framework of statistical filtering. The advantage of this method is packet delivery ratio is increased and average end-to-end delay is decreased. A limitation of this method is cluster-based routing protocol filtering mechanism [19].

In [20] the authors S. A. Arunmozhi and Y. Venkataramani proposed a new defense mechanism in which each node contains a flow monitoring table (FMT). An advantage of this scheme is to improve the performance of Ad-hoc network, high bandwidth, high packet delivery ratio, reduced packet drop for legitimate users [20].

The authors in [21] proposed a traceable overlay network with relatively stable topology support for trackback based on identity replacement mechanism. They have proposed an Identity Replacement (IR) mechanism to give a more stable topology support for trace back. The advantage of this method is trackback performance is improved.

In [22], the authors have proposed an approach for detection of malicious nodes and protection against DOS attack in AODV protocol. This approach maintains record of all nodes present in the network.

In [23], the authors have provided a survey of possible solutions for Intrusion Detection System (IDS) against DDoS attacks. According to this, the perfect IDS will have the coverage of 100% and false positives rate of 0 %. In addition to these two metrics, the intrusion detection time should be as short as possible. The advantage of this approach is to minimize false positive.

III. PROPOSED ALGORITHM

Here, we propose a new defense mechanism against Dynamic Denial of Service (dDoS) attack which consists of a node manager, RREQ (Route request), time and nodes of network. Node manager know about the nodes which are within its transmission range and for that, it is maintaining a table. The selection of node manager would be on the basis of energy level it has. Now, to find the attack we are using RREQ which is coming from any node.

Here we have defined the RREQs limit per unit time which is coming from any node. If RREQs coming from any node is exceeding than the limit then node manager will inform to all other node in network using alert message.

A. Performance Evaluation Metrics:

Three metrics are adopted to conduct a comparison study between our node manager-based Dynamic DoS attack mitigation approach and the original AODV protocol. The main purpose is to check how much overhead has been caused in order to mitigate the Dynamic DoS attacks.

a) Packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets sent.

b) Network Routing Load: The number of other control packets that transmitted for transmit one data packet.

c) End-to-End Delay: Average time difference (in seconds) between the time of the packet receipt at the destination node, and the packet sending time at the source node.

B. Experimental Setup

AODV, DSDV and DSR routing protocols can be implemented using Network Simulator 2.35. NS is a discrete event simulator targeted at networking research. It provides substantial support for TCP routing and multicast protocols over wired and wireless networks. Using Xgraph (A plotting program) we can create graphical representation of simulation results. All the work is done under Linux platform, preferably ubuntu.

C. *Implementation Methodology*

Here the following algorithms are proposed to mitigate the Dynamic DoS Attack in Mobile Ad-Hoc network. is the stepwise guide for implementing new protocol in ns-2

a) Dynamic Dos Attack generation algorithm

This algorithm is used to generate the dynamic dos attack in MANET using Ns-2. Steps of the algorithm is as given below-

1. Add the flood timer functionality below Broadcast timer in AODV.cc file. So, it needs to add fttimer cunstructor in the AODV.cc file.
2. Declare the nodes who will flood the RREQ
3. Define the FLOOD_INTERVAL.
4. Open AODV.h file to define the flood interval at very begining for aodv.h file, as given below -
   # define FLOOD_INTERVAL 0.09
   Here flood timer is 0.09 sec i.e. in every 0.09 second attacker will send the request packet to his neighbor.
5. In AODV.cc file, we have code for different type of packets like, send packet, receive packet, broadcast packet, etc. So, we have to add these codes for flooding RREQ packets by setting the parameters for it as in step 6 and step 7.
6. For flooding RREQ packets, declare following parameters –
   i. *Packet *p = Packet::alloc();*
   ii. *struct hdr_cmn *cm = HDR_CMN(p);*
   iii. *struct hdr_ip *ih = HDR_IP(p);*
   iv. *struct hdr_aodv_request *rq = HDR_AODV_REQUEST(p);*
   v. *aodv_rt_entry *rt = rtable.rt_lookup(dst);*
7. Initialize the above structures as below –
   i. *cm->ptype() = PT_AODV;*
   ii. *cm->size() = IP_HDR_LEN + rq->size();*
   iii. *cm->iface() = -2;*
   iv. *cm->error() = 0;*
   v. *cm->addr_type() = NS_AF_NONE;*
   vi. *cm->prev_hop_ = index;*
   vii. *ih->s_addr() = index;*
   viii. *ih->d_addr() = IP_BROADCAST;*
   ix. *ih->s_port() = RT_PORT;*
   x. *ih->d_port() = RT_PORT;*
   xi. *ih->ttl_ = NETWORK_DIAMETER;*
   xii. *rq->rq_type = AODVTYPE_RREQ;*
   xiii. *rq->rq_hop_count = 1;*
   xiv. *rq->rq_bcast_id = bid++;*
   xv. *rq->rq_dst = dst;*
   xvi. *rq->rq_dst_seqno = num;*
   xvii. *rq->rq_src = index;*
8. Now these packets will be used to flood the victim node.

b) Node Manager Selection Algorithm

Here we have used the node energy concept to select a node as manager. Steps of the algorithm is as below-

1. In AODV.cc file add the following code.
   i. #include <mobilenode.h>
   ii. iNode= (MobileNode *) (Node::get_node_by_address(index));
2. Execute the below code for each node to get the highest energy node
   Void AODV:: get_energy() {
   iEnergy = iNode->energy_model()->energy();}
3. Make the highest energy node as node manager.
4. Now compile ns-2.

c) Algorithm to enable the hello packet

This algorithm is needed to enable the Hello packet to get the information about the nodes present in their transmission range. Steps of the algorithm is as given below-

1. Node manager will get the information of other nodes using Hello Packet.
2. In the ns-2 by default HELLO packet in AODV is not enable. When we just fresh install NS2, AODV come with no prior HELLO packet, We have to make enable HELLO packet explicitly.
3. For that we have to make following changes in aodv.cc file.
4. We have to comment following two lines present in aodv.cc
   - #ifndef AODV LINK LAYER DETECTION
   - #endif LINK LAYER DETECTION
5. After that we need to just recompile ns-2.

d) Algorithm to add new type of packet called alert

This proposed algorithm is used to add a new packet called alert in packet.h file. Steps of the algorithm is as given below-

1. Alert message will be sent by the node manager when RREQ packets are more than the limit.
2. To add new packet type, we have to make two file with .cc file and .h file. Let's say alert.cc and alert.h.
3. In alert.h we provide structure of packet data and offset of it. Offset points to the position in the NS-2 byte array, where the header is stored.

4. Now in alert.c create a static class myheader. Now in packet.h add our new packet type. Then you can use it where ever you want in Ns-2.

c) MDDaMAN Algorithm to Prevent Dynamic Dos attack:

Here we have proposed MDDaMAN Algorithm for Mitigating Dynamic DoS Attack in Mobile Ad-Hoc Network. Steps of the algorithm is as given below-

1. Create cache table with aodv_rreqcnt in aodv_rtable.h.
2. For that we make friend class with aodv and aodv_rt_entry.
3. Then initialize following field for it.
   u_int32_t RREQentry=0;
   u_int32_t RREQatmpt=0;
4. Count the number of request coming from and then take decision.
5. For that we need to add following code to it.
   i. aodv_RREQID *id = aodvrreqcnt_lookup(rq->rq_id);
   ii. aodv_RREQcount *ct = cnt++;
   iii. if(id->RREQentry > peak_value){
   iv. Generate the alert msg;
   v. Broadcast the alert msg;}

IV. Result and Analysis

We have performed set of experiments to perform dynamic DoS in network simulator under the AODV routing protocol.

All the results are obtained using Ns-2.35. Following parameters are observed to evaluate performance of the proposed scheme.

TABLE I
PARAMATERS

Parameters	Values
Simulator	NS2
Number of Nodes	50
Area Size	1000×1000
MAC	802.11
Simulation Time	125sec
Traffic Source	CBR
Packet Size	1000
Routing Protocol	AODV
Transmission Protocol	UDP

A. End-To-End Delay

It is the average time difference (in seconds) between the time of packet receipt at the destination node, and the packet sending time at the source node.

As we know that, when any discrepancy occurs across the network then packet would be delayed for the destination. Here, in dynamic dos scenario malicious node floods the victim node with route request and do not get the destination. So, we get the more delay from source to destination.

With our proposed solution when Dynamic DoS attack is applied, end-to-end time delay is decreased as compared to without applying our approach.

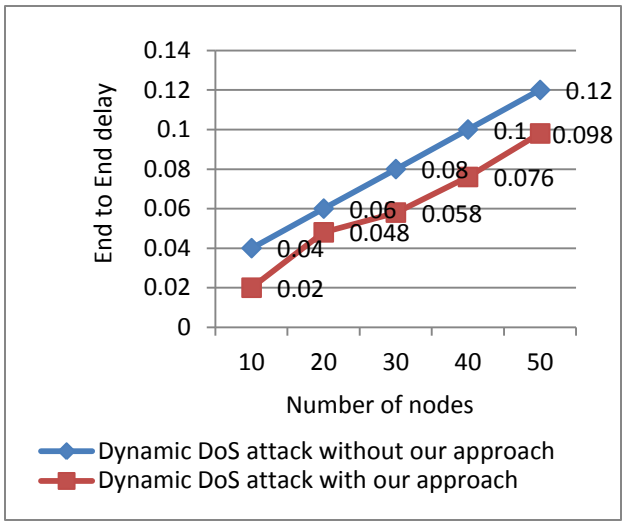

Fig. 1. End-to-end delay

B. Packet Delivery Ratio

It is the ratio of the number of packets received successfully to the total number of packets sent.

We have considered two scenarios for packet delivery ratio, first for dynamic dos attack without any prevention scheme and second for dynamic dos attack with our prevention scheme. When dynamic DoS attack occurs at that time one victim will be flooded by the RREQs. So, when any other legitimate RREQ come to that node, then it cannot process that request. Consequently, packet delivery ratio is 0.45 which is very low.

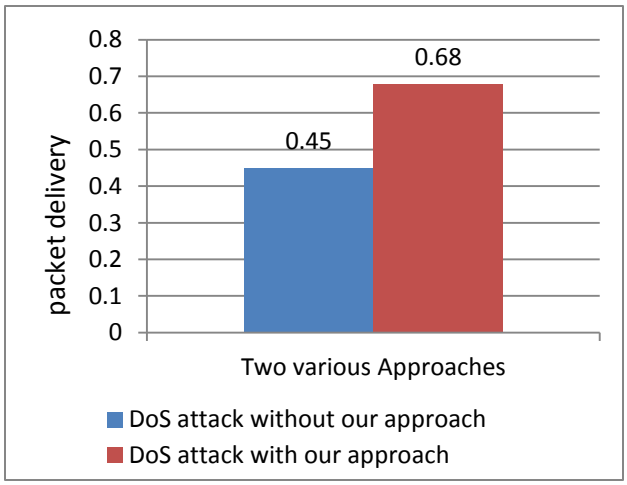

Fig. 2. Packet Delivery Ratio

During the protect action against dynamic dos attack, we have protected RREQ flood. Therefore, now we get the packet delivery ratio 0.68 by using our proposed approach which is higher than without using it in dynamic dos scenario.

C. Network Routing Load

It is the number of other control packets that are transmitted to transmit one data packet. We have measured the network routing load in AODV protocol with dynamic dos attack for two scenarios: without our approach and with our approach. In first case i.e. dynamic DoS attack without our approach, we haven't added any protection scheme yet, so there are no extra control packets. Therefore, network routing load which is 0.061 is very low.

In second case i.e. dynamic DoS attack with our approach there are some changes in AODV protocol and also added protection mechanism against dynamic dos attack. So, some control packet would be transmitted across the network.

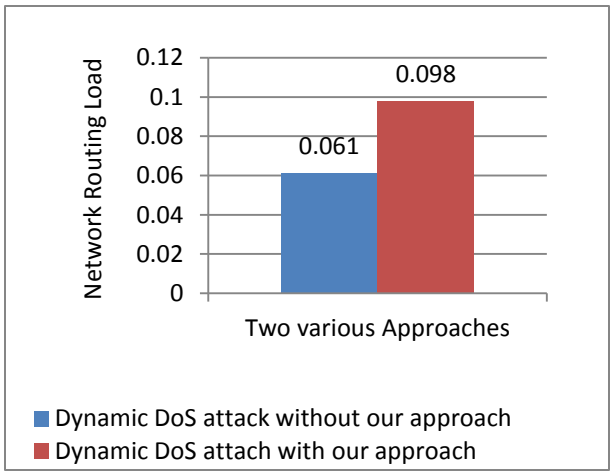

Fig. 3. Network Routing Load

Therefore, routing load is increased slightly in the network which is 0.098.

V. Conclusion

Proposed scheme describes the mitigation of dynamic DoS attack which is done by counting the route request coming towards the victim node. In this, if route requests are more than the threshold then we will declare this node as malicious one. For that, we just maintain one table at the node manager that contains the information about the node within its range. To select the node manager we have considered the energy of the node. To protect a network, proposed scheme requires managing the node manager and counting the route request.

Therefore it does not give more overhead across the network. When the dos attack is performed on any node of the network then, the victim node loses its energy, processing power and storage space. Here, we have measured packet delivery ratio, end-to-end delay and network routing load under the dynamic dos attack in the network. From the results obtained it can be claimed that packet delivery ratio is 0.45 which is very low and delay is slightly increased in the network.

From the results of our proposed scheme for mitigating dynamic dos attack, the packet delivery ratio is 0.68, network routing load is increased to 0.098 and end-to-end delay is decreased compared to network with the dynamic dos attack.

References

[1] Kasturiniva Das and Amar Taggu "A comprehensive analysis of DoS attacks in Mobile Adhoc Networks." In proceeding of International Conference on Advances in Computing, Communications and Informatics, pp. 2273-2278, IEEE, 2014.

[2] Lu Jin Zhongwei Zhang David Lai and Hong Zhou. "Implementing and evaluating an adaptive secure routing protocol for mobile ad hoc network." In Wireless Telecommunications Symposium, pp. 1-10, IEEE, 2006.

[3] Rajesh Yerneni, and Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc." In Proceeding of Third International Conference on Computing Communication & Networking Technologies (ICCCNT), pp. 1-5, IEEE, 2012.

[4] Perkins C, Belding E. Royer, and Samir Das, "Ad hoc on-demand distance vector (AODV) routing,". IETF, RFC 3561, July 2003. http://www. 1eft. o. 2003 Feb.

[5] Y. Liu and L. Shen, "Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks," In proceeding of Computer Knowledge and Technology 2007 Vol. 3 No. 16, 2007.

[6] RENU MISHRA,DR. SANJEEV SHARMA, DR. RAJEEV AGRAWAL,"Vulnerabilities and security for ad-hoc networks" 2010 International Conference on Networking and Information Technology.

[7] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 2009.

[9] Pramod Kumar Singh, Govind Sharma,"An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET",IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications-2012.

[10] Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra: "Security Issues in MANET: A Review" 978-1-4244-7202-4/10/$26.00 ©2010 IEEE.

[11] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, "Performance Comparison of AODV,DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Journal of Scientific Research, pp.566-576, 2009

[12] C. Perkins, E. Belding-Royer, and S. Das,"Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.

[13] "Charles E Perkins" ,"Elizabeth M.Royer", "Ad hoc OnDemand Distance Vector Routing"

[14] Peng Ning , Kun Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols", Ad Hoc Networks, Vol. 3, No. 6, pp. 795-819, 2006

[15] Ramratan Ahirwal, Leeladhar Mahour," Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network", International Journal on Computer Science and Engineering (IJCSE)-06 June 2012

[16] Minda Xiang,Yu Chen,WeiShinn Ku,Zhou Su," Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks", In Procedding of Global Telecommunications Conference (GLOBECOM 2011), p.p. 1- 6 , 2011.

[17] Rizwan Khan,A. K. Vatsa"Detection and Control of DDOS Attacks over Reputation and Score Based MANET", Journal of Emerging Trends in Computing and Information Sciences-oct2011.

[18] S.A.Arunmozhi,Y.Venkataramani,"DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", International Journal of Network Security & Its Applications (IJNSA)-2011

[19] Hwee-Xian Tan,Winston K.G.Seah,"Framework for Statistical Filtering Against DDoS Attacks in MANETs",Proceedings of the Second IEEE International Conference on Embedded Software and Systems, 2005.

[20] 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.

[21] Yinan Jing, Xueping Wang, Lili Zhang, Gendu Zhang, Stable Topology Support for Tracing DDoS Attackers in MANET, 2011 IEEE.

[22] Kanchan, Sanjeev Rana, "Methodology for Detecting and Thwarting DoS in MANET", IJCA,2011.

[23] Mirjana Stojanovic,Valentina Timcenko, Slavica Boštjancic Rakas, Intrusion Detection Against Denial Of Service Attacks In Manet Environment, XXIX Simpozijum, 0, decembar 2011.