# Explicit Query based Detection and Prevention Techniques for DDOS in MANET

Neha Singh
Asst. Professor
IIMT Engineering College, Meerut

Sumit Chaudhary
Asst. Professor
IIMT Engineering College, Meerut

Kapil Kumar Verma
Associate Professor
Dewan V.S. Institute of Engg. & Technology,Meerut

A. K. Vatsa
Asst. Professor
Shobhit University,
Meerut

## ABSTRACT

The wireless adhoc networks are highly vulnerable to distributed denial of service (DDoS) attacks because of its unique characteristics such as open network architecture and shared wireless medium. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its legitimate users. The denial of service (DOS) does not result in information theft or any kind of information loss but can be very dangerous, as it can cost the person a large amount of time and money.

Significant efforts have been made towards making adhoc network secure and free from DDoS attacks. In this paper we study how various detection parameters together work as a single and efficient method to detect various DDoS attacks in Manet. Later in this paper a technique to prevent DDoS attacks in Manet is also presented which help in preventing the attacks to communicate in the network and did not allow them in the network.

**Keywords:** Explicit query, Mobile ad-hoc networks (MANET), Denial of service (DOS), Distributed denial-of-service (DDOS), detection, prevention technique, Blacklist

## 1. INTRODUCTION

MANET is infrastructureless networks composed of a set of wireless mobile nodes. Nodes send packets directly to destinations that are in their coverage zone. When destinations are farther than the coverage range intermediate nodes cooperate to establish the communication path. The ad hoc context increases the number of potential security vulnerabilities. Ad hoc networks can not benefit from the security services offered by dedicated equipment such as firewalls, authentication servers and so on.

MANETs various types of DOS Attacks are also possible because of the inherent limitations of its routing protocols. A DoS attack always attempts to stop the victim from serving legitimate users. A DDoS attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim. There are two types of DDoS attacks i.e. passive and active DDoS attacks. The First type of DDoS attack has the aim of attacking the victim node in order to drop some or all Log files store the Application Programming Interface (API) functions calls that are made by communication applications [1, 2]. Our results show that it is sometimes difficult to distinguish between normal behavior and malicious behavior. The correlation algorithm shows that there are high numbers of correlated events in attack case generated by bots compared to normal users [3, 4]. The new DOS attack, called Ad Hoc Flooding Attack (AHFA), can result in denial of service when of the data packets sent to it for further forwarding even when no congestion occurs, which is known as Passive DDoS attack. The second type of DDoS attack is based on a huge volume of attack traffic, which is known as an Active DDoS attack [4]. 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 an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. Perpetrators of DDoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. Some well-known DoS attacks are SYN Flood, teardrop, smurf, ping of death, land, finger bomb, black holes, octopus, snork, ARP Cache poisoning and the misdirection.

There are various techniques which are proposed to detect and prevent all these DDoS attacks. In this paper a highly powerful approach is used to detect various DDoS attacks with various reliable parameters which can make our network secure and when an attack is easily detectable with this approach then it can easily prevent all these attacks.

### 1.1 Paper Organization

Section II provides the background and related work, Section III deals with the proposed work, Conclusion is stipulated in Section IV. The proposed work may be extended further with reference to the different situations are mentioned in section V under future aspect.

### 1.2 Problem Identification

1. Congestion is created by attackers and legitimate users are unable to successfully send their packets to destination nodes.
2. Various DDOS detection and prevention techniques are not able to completely prevent the users from the malicious nodes.

## 2. BACKGROUND

used against on demand routing protocols for mobile ad hoc networks, such as AODV, DSR. The intruder broadcasts mass Route Request packets to exhaust the communication bandwidth and node resource so that the valid communication cannot be kept [5, 6]. The probability of accidental blacklisting of the node can be reduced by using the concept of delay queue also on the other hand it also delays the detection of misbehaving node by allowing the attacker to send more number of packets until delay queue time out occurs[7 - 9].

An ad hoc network is the collection of cooperative wireless nodes without the existence of any access point. The presence of malicious nodes in an ad hoc network deteriorates the network performance. Number of packet drops increases proportionally with the number of malicious nodes. As the packet drop increases, it also affects the packet delivery ratio, routing load and throughput etc [10, 12]. Packet flow is monitored and when packet drops increases, it causes a frequent change in sequence number and when it crosses a threshold limit, then alarm is raised and finally malicious nodes are removed from network on the basis of losses caused by them [11, 14]. One of the major reasons to address the security aspects in MANETS is the usage of wireless transmission medium, which is highly susceptible or vulnerable to attacks. These attacks throttle the tcp throughput heavily and reduce the quality of service (QoS) to end systems gradually rather than refusing the clients from the services completely. The status values from MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and the number of RTS/DATA retransmissions [13, 15, 16]. A approach that can accurately identify DDoS attack flows and consequently apply rate-limiting to the malicious network flows.

A DDoS attack is a coordinated attempt made by malicious users to flood the victim network with the large amount of data such that the resources of the victim network are exhausted resulting in the deterioration of the network performance. The DDoS attacks in MANETs are implemented by taking advantages of the weaknesses of the routing protocols, operating systems and security schemes applied on systems. But the results of these types of attacks may lead to degrade the performance of systems/sites or break the services to legitimate users. Reduction of Quality (ROQ) attack is one of the Denial of Service (DoS) attacks which affect the MANETs [17 - 19]. Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems [20]. The Ad hoc On-Demand Distance Vector (AODV) routing protocol, designed for mobile ad hoc networks, offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization. However, without keeping in mind the security issues in the protocol design, AODV is vulnerable to various kinds of attacks [21, 22].

# 3. PROPOSED WORK

## 3.1 Architecture of explicit query based detection and prevention technique for DDoS in Manet

These are the various parameters which help in the detection and prevention technique for DDoS in Manet-

- **Sequence number:** Various sequence numbers are assigned to each and every node with the help a random number generator.
- **Parameters:** Manet consist of various parameters like battery power, RTT, threshold values, packets forwarded at each node, total time taken by any packet.
- **Response of each node:** With the help of various parameters used attacker is detected.
- **BlackList:** A blacklist is created which store the information of all the nodes which are detected as an attacker and that node is allowed to communicate over the network.
- **Limit of Processing:** Attacker is detected by using the RTT threshold value and with the help of that ratio of clost/csent is calculated.
- **Threshold Parameters:** Threshold values of friend, acquaintance and stranger nodes are used to detect the attacker.
- **EAN:** A notification is send to sender node by destination node i. e. Explicit Attacker Notification to give it information of attacker and ask it to slow down its packet sending rate.

## 3.2 Working Principle

### Detection

The working of DDoS detection proposed architecture model illustrated in Figure -1, which starts working by randomly generate sequence to each and every node with the help of random number generator. The availability of response from node is checked with help of various parameters used i.e. battery power, RTT, total time taken by packets, total number of packets forwarded, blacklist used for attackers. By checking the response from nodes attackers are detected and then these attackers are sent to the blacklist and not allowed to communicate over the network. In next step limit processing is checked with the help of RTT threshold value and with that ratio of clost/csent is calculated and if attacker is there it is sent to blacklist and packet is dropped.

### Prevention

The working of DDoS prevention proposed architecture is illustrated in figure-2 which starts working by categorizing the nodes in three categories friend, acquaintance and stranger. The attacker is detected by setting different threshold values for each category. These threshold values are compared with number of packets delivered and node is also checked if it is in blacklist or not. If both conditions satisfied then a notification is send to sender node to slow down its sending rate and if after this also sender node does not slower down its sending rate then it is termed as attacker and sent to blacklist and not allowed to communicate over the network.

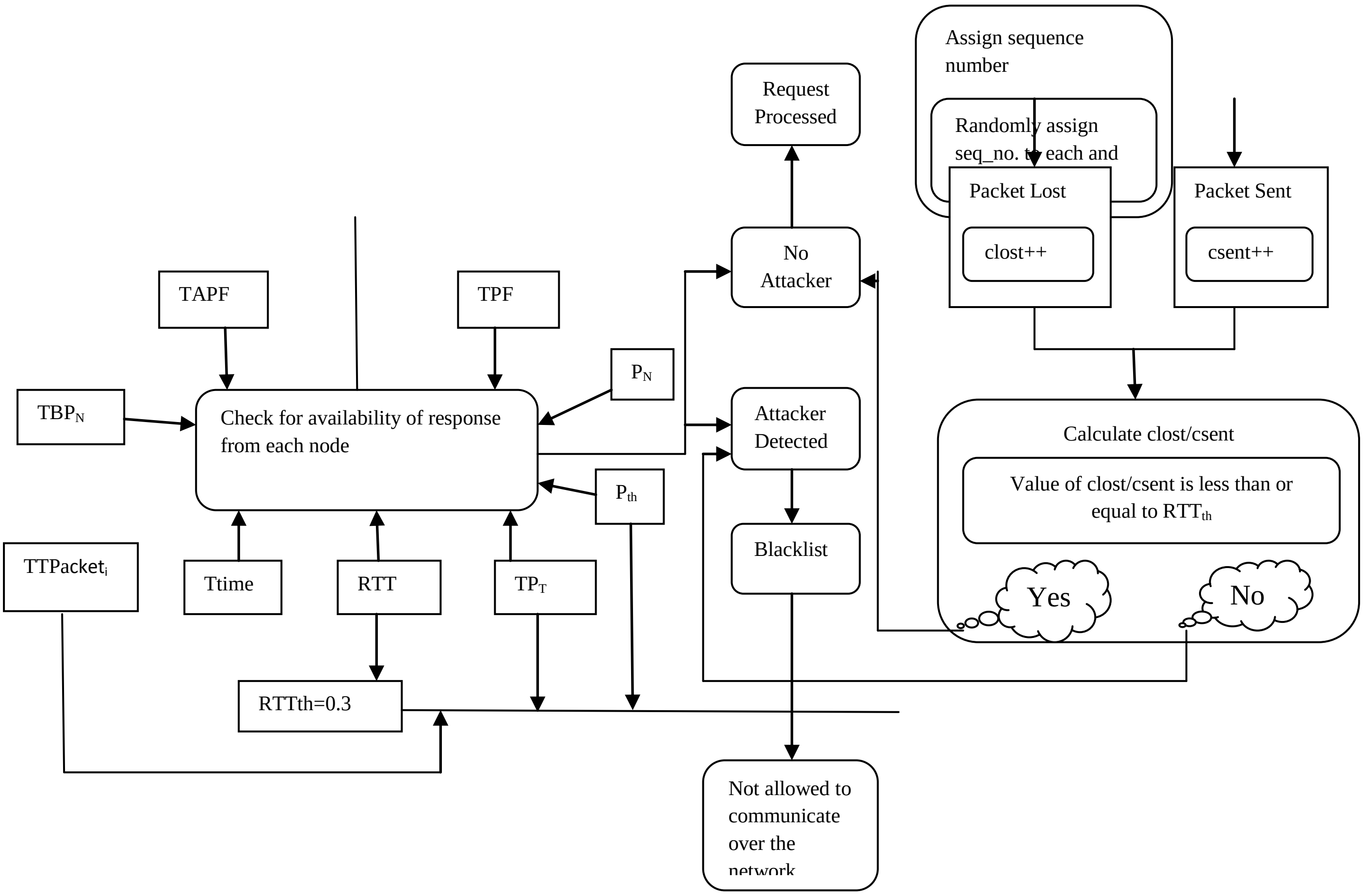

**Fig 1: Architecture of detection of DDOS attack in MANET**

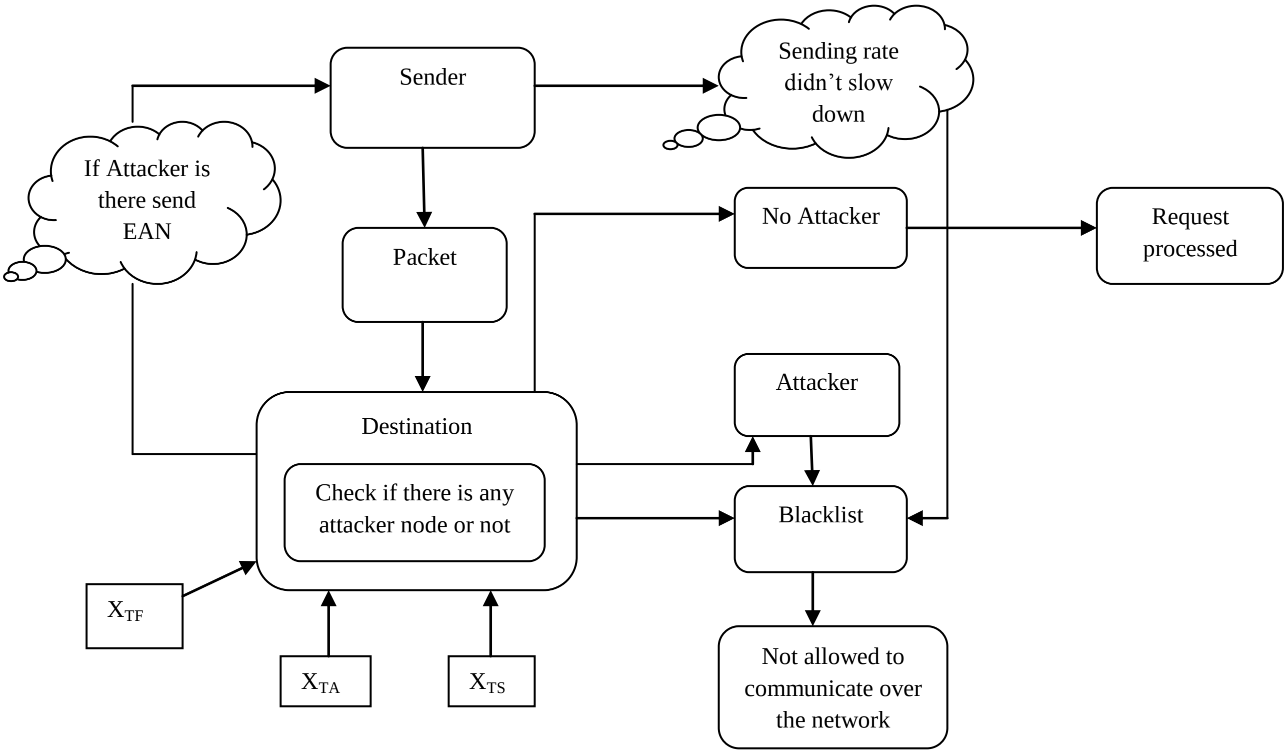
Sender
Sending rate didn't slow down
If Attacker is there send EAN
Packet
No Attacker
Request processed
Attacker
Destination
Check if there is any attacker node or not
Blacklist
XTF
XTA
XTS
Not allowed to communicate over the network

**Fig 2: Architecture of prevention for DDOS attack in MANET**

## 3.2 Mechanism

**PHASE I -Detection Techniques for DDoS:**

**Step 1- Assign sequence number for each node of MANET**

```
Number of node = N
For (i=0; i<N; i++)
{
Nseq_no = RandomNoGenerator( ); //Nseq_no is node sequence number
}
```

**Step 2- Check Response message**

```
Response ( )
{
For (Nseq_no = 0; Nseq_no<N; Nseq_no++)
{
If($TP_T$>$P_{th}$&&$T_{time}$>RTT||$P_N$<$TBP_N$&&TAPF>TF)
          //$TP_T$=Total no. of packets over time T
          //$P_{th}$=Threshold value for packet sending
          //TAPF=Total actually packet forwarded
                  at node i
          //TPF=Total packet to be forwarded at `node i

          //$T_{time}$=Total time of packet forward and acknowledgement

          //RTT=Round Trip time of a node

          //$TBP_{N=}$Threshold battery power of node

{
          Node will be detected as an attacker;
          Send it to black List
}
```

```
**int AttackerNode (node_i)**
{
For($Node_1$ to $Node_n$)
{
If(BlackList[i]==$Node_i$ && $Node_{req}$<$NodeRate_{limit}$)
{
 Request is processed;
}
else
{
 Node is attacker Node and No further available over network
}

IdentifyBlackListNode ( )
{
int i,BlackList[n];
for(i=0;i<n;i++)
{
BlackList[i]==AttackerNode($Node_i$);
If(BlackList[ i]==$Node_i$)
{
Node won't be allowed for any further communication over Network
}
}
}
```

**Step 3-Check for Limit of Processing**

A threshold value for RTT is set to 30ms.If any packet is exceeding the set time limit then it is assumed that packet is lost. Two counters are parallelly executed csent(packet sent i.e. not exceeding time limit) and clost(packet lost i.e. exceeding time limit). A ratio of (clost/csent) is calculated. Threshold value for this ratio is set to 30% i.e. 0.3 which is termed as limit of processing.

```
for(i=0;i<n;i++)
**(i)-**
Set $RTT_{th=}$30ms;          //$RTT_{th}$=Round Trip Time
                              threshold value
{
If ($TTPacket_i$> $RTT_{th}$&& $TP_T$>$P_{th}$)
                    //$TTPacket_i$=Total Time taken by any
                    Packet at node i
                    //$TP_T$= Total no. of packets over time T
                    //$P_{th}$=Threshold value for packet sending
{
Packet is lost;
clost++;            //clost=counter for lost packet
}
else
{
csent++;            //csent=counter for sent packet
}
}
**(ii)-** Calculate ratio of clost/csent
{
if(clost/csent<=0.3)
Request is processed;
else
{
Node is termed as Attacker;
Send it to BlackList;
}
```

**Phase II- Prevention Technique**

```
Relation (ni →nj) = $F_N$          when T ≥ Tfri
               //ni,nj=neighboring nodes to each other

               //T=Trust level, Tfri=Trust level of friend
Relation (ni →nj) =$A_N$           when Tacq ≤ T < Tfri
               //Tacq=Trust level of          acquaintance
Relation (ni →nj) =$S_N$           when 0 < T < Tacq
Begin
For (i=0; i<N; i++)
               //An intermediate node receives flooding packet
               from node i
{
if(Node(i)=$F_N$&&Z[i]=0&&Node(i)=$A_N$&&Z[i]=0
        &&Node(i)=$S_N$&&Z[i]=0)
        //$F_N$=Friend node, $A_N$=Acquaintance node, $S_N$= Stranger node
        //Z[i]=Boolean array to activate or stop the process
{
  X[i] ++;
        //X[i] = No. of packet delivered from neighboring node (i)

}
If(X[i]>($X_{TF}$&&$X_{TA}$&&$X_{TS}$))||(check whether  packet at node i is in BlackList or not)
        //$X_{TF,}X_{TA,}X_{TS}$ =Flooding threshold of friend, Acquaintance& Stranger nodes
{
elseif (both conditions are satisfied then destination node
        sends an EAN to sender node)
        //EAN=Explicit Attacker Notification
{
Drop the packet and set Z[i] = 1;
Sender node should slow its sending rate;
If(sender node=!slow packet sending rate)
Block that sender node in the network;
Send it to BlackList;
}

else
{
Forward the packet;
}
```

# 4. CONCLUSION

The DDoS attacks in MANETs are implemented by taking advantages of the weaknesses of the routing protocols, operating systems and security schemes applied on systems. But the results of these types of attacks may lead to degrade the performance of systems/sites or break the services to legitimate users. To avoid such types of attacks there is need to develop more powerful security schemes. In this paper a powerful detection and prevention technique for DDoS attacks in MANET is proposed. An algorithm is presented that is capable of detecting the suspicious or attacker nodes by detecting the nodes which misbehave by dropping significant percentage of packets and an algorithm for prevention of such DDoS attacks is also presented which helps in providing a highly secure and reliable mobile Adhoc network.

# 5. FUTURE SCOPE

The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. Constant researches are going on in field of Manet for detecting and preventing DDOS attacks. The techniques proposed in this dissertation are reliable for a small area of network and more research work can be done in this for a large network as the network is scalable, heterogeneous, mobility- used approach and is fully composite with respect to the ongoing advancement in this field.

# 6. REFERENCES

[1] Yousof Al-Hammadi and Uwe Aickelin, "Detecting Botnets Through Log Correlation**"**, volume 1, pp 1-4, January 2010.

[2] Ms.Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", IJCTEE ,volume 1, Issue 3, pp 68- 72, November 2011.

[3] Shishir K. Shandilya and Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications, volume 5, Issue 12, pp 4-8, August 2010.

[4] Kanchan and Sanjeev Rana, "Methodology for Detecting and Thwarting DoS in MANET", IJCA, volume NSC, Issue 1, pp 31-34, December 2011.

[5] Mansoor Alicherry, Angelos D. Keromytis and Angelos Stavrou, "Deny-by-Default Distributed Security Policy Enforcement in Mobile Ad Hoc Networks", SpringerLink, volume 19 part 1 , pp 41-50, 2009.

[6] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, volume 2, Issue no. 5, pp 815-818, October 2010.

[7] S.A.Arunmozhi and Y.Venkataramani, "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", IJNSA, volume 3, Issue no. 3, pp 182-187, May 2011.

[8] Quan Jia,Kun Sun and Angelos Stavrou, "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET", ICCN, August 2011.

[9] Gurjinder Kaur,Yogesh Chaba and V. K. Jain, "Distributed Denial of Service Attacks in Mobile Adhoc Networks", World Academy of Science, Engineering and Technology, volume

[10] Syed Atiya Begum, L.Mohan and B.Ranjitha, "Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks", IJECCE, volume 3, Issue no 1, pp 152-156, March 2012.

[11] S.Venkatasubramanian and N.P.Gopalan, "A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET", IJCA, volume 21, Issue no. 1, pp 7-10, May 2011.

[12] Adnan Nadeem and Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs", IWCMC, pp 926-930, June 2009.

[13] Yaser Khamayseh, Ruba Al-Salah and Muneer Bani Yassein, "Malicious Nodes Detection in MANETs: Behavioral Analysis Approach", Journal of Networks, volume 7, Issue no. 1, pp 116-125, January 2012.

[14] Vikram Singh and Vatika, "Design & Implementation of Secure AODV in Multicast Routing To Detect DDOS Attack", IJNSA, volume 3, Issue no. 5, pp 43-57, September 2011.

[15] S.Kannan,T.Maragatham,S.Kartik and V.P Arunachalam, "A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols", Medwell Journals, volume 5, issue no. 3, pp 178-183, 2011.

[16] Venkatesan Balakrishnan and Vijay Varadharajan, “Packet Drop Attack: A serious threat to operational Mobile Ad hoc Networks”, IJSER, pp 1-7, 2005.

[17] Prajeet Sharma, Niresh Sharma and Rajdeep Singh, “A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network”, IJCA, volume 41, Issue no. 21, March 2012.

[18] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod,Zalak ,Dedhia and Nirali Mody, “Security Scheme for Distributed DoS in Mobil Ad Hoc Networks”, volume 2, May 2010.

[19] Wei Ren,Dit-Yan Yeung,Hai Jin and Mei Yang, “Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks”, International Journal of Network Security,volume 4, Issue no. 2, pp 227-234, March 2007.

[20] Ujwala D. Khartad and R. K. Krishna**, “**Route Request Flooding Attack Using Trust based Security Scheme in Manet”, IJSSAN, volume 1, Issue no. 4, pp 27-33, 2012.

[21] S.Gopinath, S.Maragatharaj and C.Rajalingam, “ The Modified Routing Protocol for Defending against Attacks in MANET”,International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, Issue no. 1, pp 1-4, January 2012.

[22] Rizwan Khan and A.K Vatsa, “Detection and Control of DDOS Attacks over Reputation and Score Base MANET”, Journal of Emerging Trends in Computing and Information Sciences, volume 2, Issue no. 11, pp 646-655, October 2011.