International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

# Design & Implementation of Secure AODV In Multicast Routing To Detect DDOS Attack

Vikram Singh and Vatika

Department Of Computer Science and Engineering
Chaudhary Devi Lal University, Sirsa-125055 Haryana (India)
E-MAIL: arora.vatika@gmail.com
E-MAIL:vikramsinghkuk@yahoo.com

## Abstract

*The wireless ad hoc network is particularly vulnerable to DOS attacks due to its features of open medium, dynamic changing topology, cooperative algorithms, decentralization of the protocols, and lack of a clear line of defense is a growing problem in networks today. In Mobile Ad hoc Networks (MANET), various types of Denial of Service Attacks (DOS) are possible because of the inherent limitations of its routing protocols. In this paper we will secure the MANET from the DDOS attack. DDOS attacks are similar to DOS attacks but there is a difference between them and that is DDOS attacks involve breaking in to hundreds or thousands of machines, so for this reason, this attack called Distributed. Very often, systems that use for attack is a part of the networks and users of these systems don't know about that, their systems used for attack to another systems. This kind of attack, consume more bandwidth and uses more sources in network. . In this work, we study the effect of one of the important attacks that called DDOS in MANET on most vulnerability protocol that named AODV. The product of this study is detection of DDOS attack by using AODV (adhoc on demand distance vector) protocol. Proposed scheme is distributed in nature it has the capability to prevent Distributed DOS (DDOS) as well.*

***Key words**: distributed denial-of-service (DDoS), wireless ad hoc networks, adhoc on demand distance vector protocol(AODV),MANET(Mobile Adhoc Network).*

## 1 Introduction

A wireless ad hoc network is a decentralized wireless network where the network does not depend on a preexisting infrastructure, such as routers in wired networks or access points (AP) in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data to the other nodes, [5] and so the determination of which nodes forward data is made dynamically i.e. the normal nodes are converted to a routers and gateways.

DOI : 10.5121/ijnsa.2011.3504 

A Mobile ad hoc network is a group of wireless mobile computers (or nodes); in which [7] nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. [7] A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links.

There is one attack to be considered on MANET is DDOS attack. This attack is a natural development from the SYN Flood Attack, The idea behind this attack is focusing Internet connection bandwidth of many machines upon one or a few machines. This way it is possible to use a large array of smaller (or "weaker") widely distributed computers to create the big flood effect. Usually, the assailant installs his remote attack program on weakly protected computers (Universities, home users constantly connected etc.) using Trojan horses and intrusion methods, and then orchestrates the attack from all the different computers at once. This creates a brute force flood of malicious "nonsense" Internet traffic to swamp and consume the target server's or its network connection bandwidth. This malicious packet flood competes with, and overwhelms, the network's valid traffic so that "good packets" have a low likelihood of surviving the flood. The network's servers become cut off from the rest of the Internet, and their service is denied. The product of this study is detection of DDOS attack by using AODV (adhoc on demand distance vector) protocol [1].

## 2 Related Works

Dhaval Gada[12] et al have proposed a proactive scheme that could prevent a specific kind of DoS attack and identify the misbehaving node. Since the proposed scheme is distributed in nature it has the capability to prevent Distributed DoS as well. [13]Shiv Mehra have proposed a technique to enhance the capacity of ad hoc networks is implemented. The technique exploits the existing infrastructure by placing gateways at fixed locations in the ad hoc network. They are originally placed to provide Internet access to mobile nodes in an ad hoc network, but they can also be utilized to facilitate communication among nodes in the ad hoc network. Those gateways serve as relay nodes, thus taking responsibility of relaying most of the burden (packets) imposed by the mobile nodes in the network. Bhavana Gandhi[16] have proposed novel framework which deals with proactively mitigating the influence of the attack , characterization of the TCP flows as attack or legitimate, and identification of the path traversed by the flow once it has been characterized as an attack flow. Generation of copies of TCP/IP headers by predefined intermediate routers provides for the dual functionality of proactive mitigation and trace back. Irshad Ullah et al. have presented the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad Hoc on Demand Distance Vector (AODV). Comparative analyses of Black hole attack for both protocols were taken into account.

## 3 Objective and Research Methodology

In this paper we discussed the AODV multicast protocol, which is use to detect the DDOS attack on MANET.

## 3.1 Objective

1. To Study the work of Different MANET Protocols and to study the functioning of AODV protocol.
2. Detection of DOS attack in MANET.
3. Providing the solution of DOS attack as to minimize the packet loss as the DOS attack occurs.
4. To avoid the congestion occurred because of DOS attack.

DDOS attacks that have an important and dangerous effect on Mobile Ad-Hoc Network and cause problems in these networks. In this work, we study the effect of one of the important attacks that called DDOS in MANET on most vulnerability protocol that named AODV. The product of this study is detection of DDOS attack by using AODV (adhoc on demand distance vector) protocols.

## 3.2 Distributed Denial of Service Attack

A DDOS [19] (Distributed Denial-Of-Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. [5] The distributed format adds the "many to one" dimension that makes these attacks more difficult to prevent. A distributed denial of service attack is composed of four elements, as shown in Figure 1.

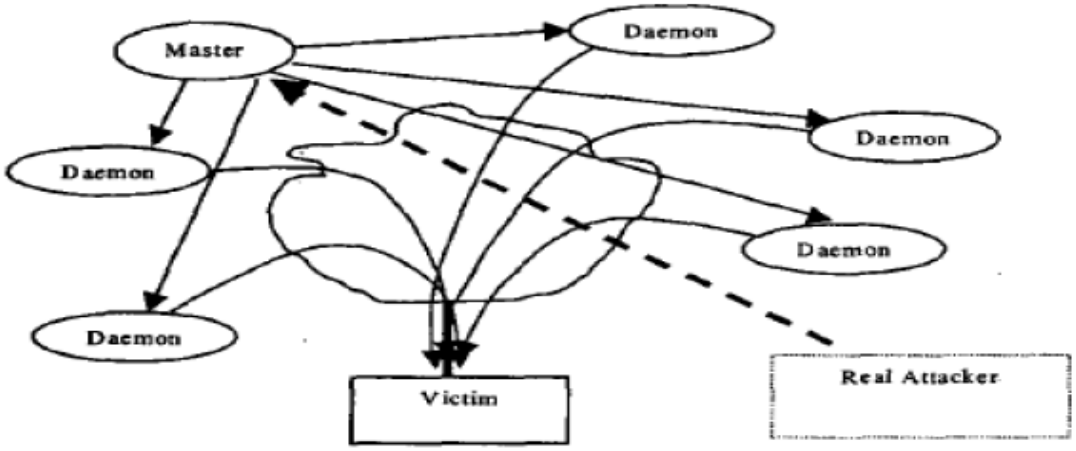



Figure 1 The four components of DDOS attack

First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers.

The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the

control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. [19] By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack:

- The real attacker sends an “execute” message to the control master program.
- The control master program receives the “execute” message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

## 3.3Research Methodology

In this paper we describe the detection system, which is use to detect the DDOS Attack.

### 3.3.1 Detection system location

Detection systems tend to be constructed as either "host based" or "network systems". Each one of these architectures has advantages and shortcomings. Neither one can be defined as "better", yet different protections call for different system architecture.

### 3.3.2 Host based" systems

These systems usually work off audit logs provided by the operating system. The system detects attacks by watching for suspicious patterns of activity on the host. This system can learn quite quickly the different patterns of use in the system and recognize any abnormalities that appear during an attack. The system has the advantage of access to the innermost processes in the host, and can notice any slight change that occurs (for example – access to kernel activities). In addition, since the system sits physically on the host, it can receive real time information about the host's resources during peak activities (such as occurs during an attack). This is important in a situation where due to a crippling amount of packets that arrive to the host, the host discards some of them and responds only to a small amount. The only way to know that the host is discarding some of these packets is by direct access to the innermost processes in the host.

However, the "Host based" systems have a major shortcoming: they are only aware of what enters the host, and have no clue about low level network events. Since the "Host-based" systems are autonomous, they have no idea regarding the state their neighboring computers are in and rarely share information on a regular basis in order to enable enhanced protection and detection. An example for such correlated detection is several computers noticing a port scan being executed on them (extensive port scanning might warn against an upcoming attack)

### 3.3.3 Network detection

Network systems are driven off interpretation of raw network traffic. They watch traffic on the network and try to detect attacks by watching for specific patterns or abnormalities in network traffic. The systems work by examining the contents of packets transmitted on the network analyzing the types of protocols used and different packet attributes. This is usually done passively by eavesdropping on the network using a stiffer or any similar type of tool. This type of analysis is unobtrusive and at the lowest levels of network operation, extremely difficult to

evade. An installation of such a system does not require any network adjustments and does not degrade the network performance in any way.

Network detection systems are good at noticing low level network manipulations of the network and can identify correlated attacks against several targets. An important advantage is the ability to recognize attacks focused on the network itself and not at a specific target (overloading a network with packets to a nonexistent machine for example [19].

### 3.3.4 Detection Parameters

There are many approaches to identifying a DOS attack and yet after reviewing many of them, one can notice that there are several detection parameters that are considered in the majority of the systems. The weight given to each parameter varies from system to system but important detection parameters are always used. In this part we will review these more common parameters, their strengths and weaknesses. The effectiveness of the detection parameters varies from system to system. Some equipment tends to be more stable than others and at times other equipment might have a better history that enables finer tuning for detection.

### 3.3.5 Load and Traffic Monitoring

Load and traffic volume monitoring at ISPs can provide early warning of attacks. Traffic-limiting IDS can monitor loads of all incoming traffic and search for abnormalities. In addition, the system might also attempt to reframe data communications between two points by asking the sender to slow down the rate of data acknowledgment. Legitimate servers will do so. Those that don't are deemed untrustworthy, so their packets are then filtered out. This method is mainly effective against "script kiddies" who work within Microsoft Windows and download hacking scripts from the Internet. Such hackers don't know sophisticated methods of concealing their IP addresses. In theory, a traffic-limiting device installed outside the firewall should strip out and redirect bad traffic without becoming a choke point for good traffic. It could also deny inbound data from specified IP addresses, either for a set time or until an attack stops. The denial automatically ends when traffic flow returns to normal [19].

### 3.3.6 Latency to Victim

Checking the time it takes the system to respond to requests is a good indicator (assuming otherwise the system works well). The first way to implement such a monitor is to construct an agent placed on a different network from the potential target, and having the agent constantly send requests to the potential target. The agent measures the average time of response, and when a big deviation from this time is identified, the alarms go off. This method is nicknamed 'What's up?'

The second method is to have the potential target send a test packet to some outer agent that simply resends the packet back. [19] When done constantly, the potential target can learn when the inbound bandwidth becomes congested and can sound an alarm.

### 3.3.7 Committed Access Rate (CAR)

This method checks if a specific type of packet uses up more than average amount of bandwidth it usually does. This idea is derived from a defense method, in which the router will limit the bandwidth consumed by certain types of traffic (configurable via an extended access control

list). This can be used to limit the bandwidth consumed by SYN packets, so that non-SYN packets (i.e., legitimate established connections) will have bandwidth available. The downside to this approach is that it will be difficult for a legitimate client to establish a new connection while the target is under attack.

# 4 Simulation of DDOS Attack

This Paper represents the simulation of DDOS attack, which is use to avoid the congestion occurred because of DDOS attack. It describes a study of the Existing System and detection system, which is use to detect the attack.

## 4.1 How Detection System works

The following diagram describes the detection system flow indicating inputs, internal information flow and output. Bear in mind that the thread work concurrently and the flow demonstrate only the logical path of the information through the system.

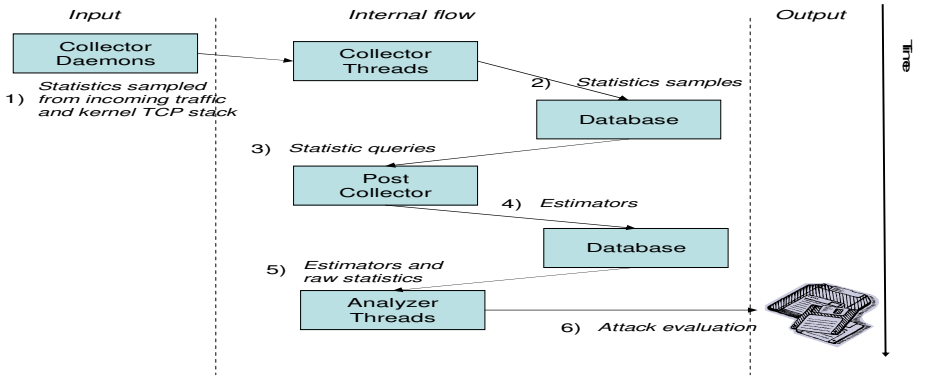



Figure 2 Detection System flow Diagram

System internal flow consists of the following stages:

1) Collector daemons constantly collect incoming statistics. Periodically the collector threads query the daemons for the current statistics.
2) The sampled statistics received by the collector threads are committed to the database, normalized by time.
3) The post collector periodically samples the database for raw statistics samples and estimates the probability for common events such as spoofed traffic or changes in traffic behavior such as changes in packet size, TCP/UDP destination ports distribution and etc.
4) The post collector commits the estimations in the database.
5) The analyzers periodically sample the database for estimations and raw statistics and evaluate the probability for an attack.
6) Attack evaluation are written to log files or printed to the screen upon user request.

## 4.2 Protocol Use in Simulation

In this paper we discussed the AODV multicast protocol, which is use to detect the DDOS attack on MANET.

### 4.2.1 Adhoc On Demand Distance Vector Protocol

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. [3] AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries.

The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors [3] AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. Sequence numbers ensure the freshness of routes and guarantee the loop-free routing.

## 4.3 Algorithm Parameters

With a set of selected detecting paths, the detecting algorithm will probe over each of them. Given a detecting path, there are at least two ways of probing. One way is to probe from the farthest node to the nearest. The other way is to probe from the nearest node to the farthest. Each has its own advantages and disadvantages. Detecting from far to near is better if the detecting path is GOOD since it takes only one probe message and proves the goodness of all the intermediate nodes. But it may take more probe messages if a MALICIOUS node is located near the detecting node. This method can be applied to a network where we have the confidence that the majority of the nodes in the network are GOOD.

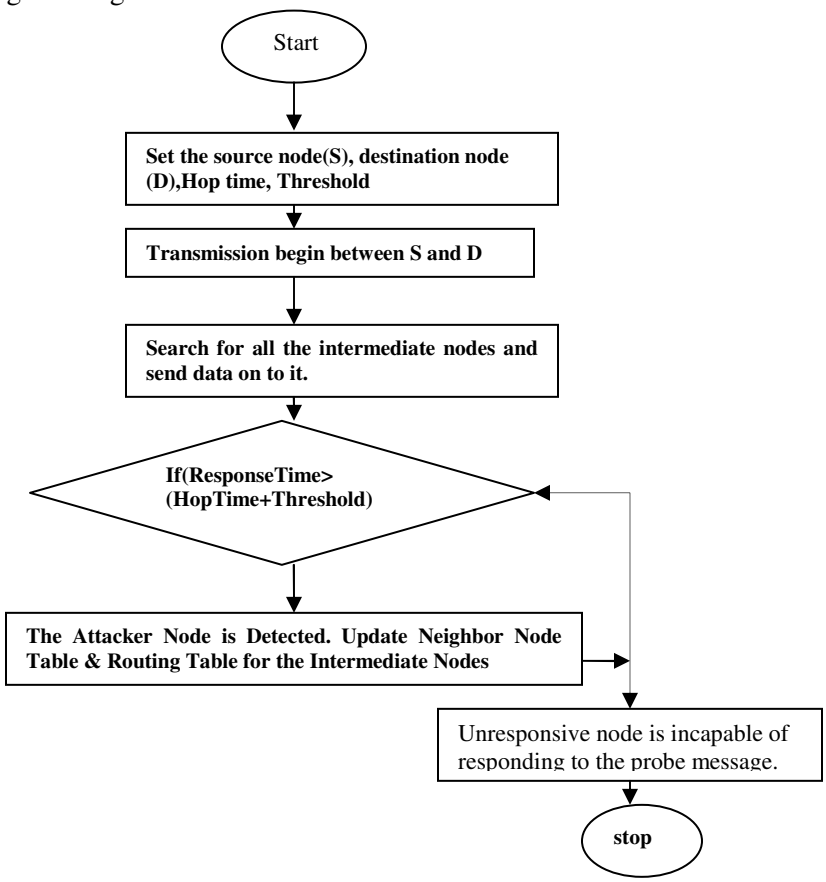
The advantage of probing from near to far is that it generates smaller number of probing messages to detect a MALICIOUS node located near the probing node. Another advantage is that we have the prior knowledge of the states of all the intermediate nodes along the path to the probed node except its immediate predecessor node. The disadvantage is an intelligent attacker may be able to avoid detection by forwarding all packets for a certain period of time immediately after receiving a probe message for itself. A received probe message therefore serves as a signature to an attacker that a diagnosis process is ongoing, and it would start to behave normally for a short period of time. Other search strategy (e.g., binary search) can also be deployed to reduce network overhead.

In this paper, we present the algorithm for the first method, probing from the farthest nodes to the nearest, since it is stronger than the other alternatives in detecting malicious nodes. For a probing path, the probing node sends a probe message to the farthest node. If an acknowledgment message is received within a certain period of time, all the intermediate nodes are shown to be GOOD. Otherwise, a probe message is sent to the second farthest node. This

process is repeated until one node responds to the probe message or the nearest node (a neighbor node) is probed and it is not responsive. In the latter case, we know that the neighbor node in the probed path either is DOWN or has moved out to another location. Since the neighbor node is not responsive, there is nothing we can do to monitor the rest nodes in the path. Therefore, probing over this path is stopped. If an intermediate node is responsive but a node subsequent to it is not, it is possible:

**Steps:-**

DOSDetect(S,D)
/* S is the source node and D represents the Destination Node over the network*/
{
1) As transmission begins it will search for all the intermediate nodes and send data on to it.
2) The intermediate node failed forwarding the probe message to the next node;
3) It will check the RESPONSE time for the intermediate node
    If (Response Time> HopTime +Threshold)
    {
    The Attacker Node is detected.
    Update Neighbor Node Table & Routing Table for the Intermediate Nodes
    }
4) the unresponsive node is incapable of responding to the probe message.
5) The diagnosis algorithm will then be called to decide which one is the case.
}




In this flowchart, it compares the response time to hop time and threshold time. If it is greater, then attacker node id detected. Then update Neighbor Node able & Routing

Table for the Intermediate Nodes .Otherwise unresponsive node is incapable of responding to the probe message.

## 5 Experimental Results

Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize the simulations. Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. We have to choose NS2 for simulation test scenario.

**We have worked with different scenarios to test the above work.**

Scenario-1

| Parameter | Value |
|---|---|
| Number of Nodes | 10 |
| Topography Dimension | 670 m x 670 m |
| Traffic Type | CBR |
| Radio Propagation Model | Two-Ray Ground Model |
| MAC Type | 802.11.Mac Layer |
| Packet Size | 512 bytes |
| Mobility Model | Random Way Point |
| Antenna Type | Omni directional |
| Protocol | AODV |

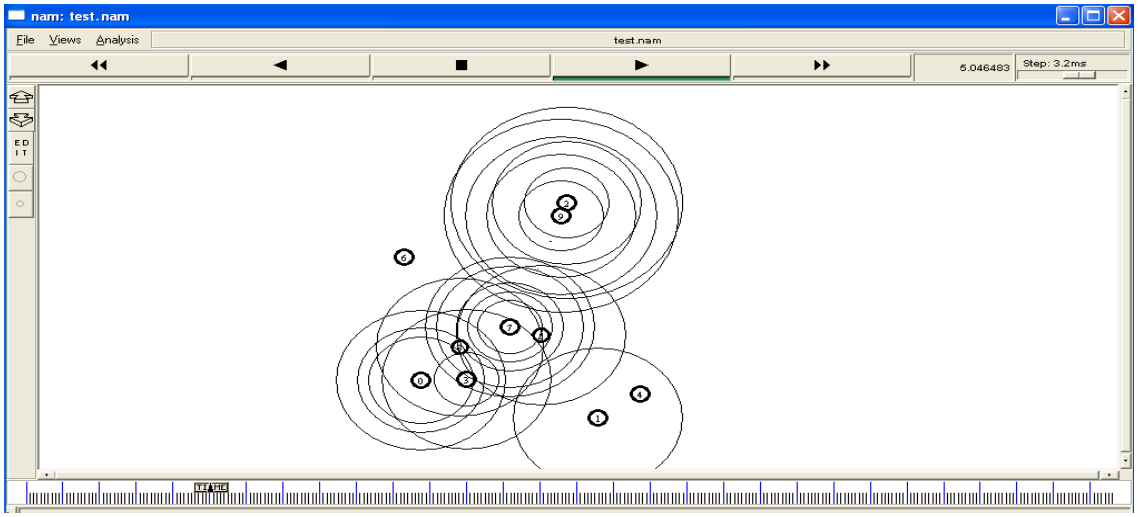



Figure 3 Scenario 1 to test communication between nodes

The mobile adhoc network comprising of 10 mobile nodes are constructed in the NS-2 simulator with the use of TCL script in the topological boundary area of 670 m x 670 m. The position of the mobile nodes is defined in terms of X and Y coordinates values and it is written in the movement scenario file.

**Scenario 2**

| Parameter | Value |
|---|---|
| Number of Nodes | 23 |
| Topography Dimension | 670 m x 670 m |
| Traffic Type | CBR |
| Radio Propagation Model | Two-Ray Ground Model |
| MAC Type | 802.11.Mac Layer |
| Packet Size | 512 bytes |
| Mobility Model | Random Way Point |
| Antenna Type | Omni directional |
| Protocol | AODV |

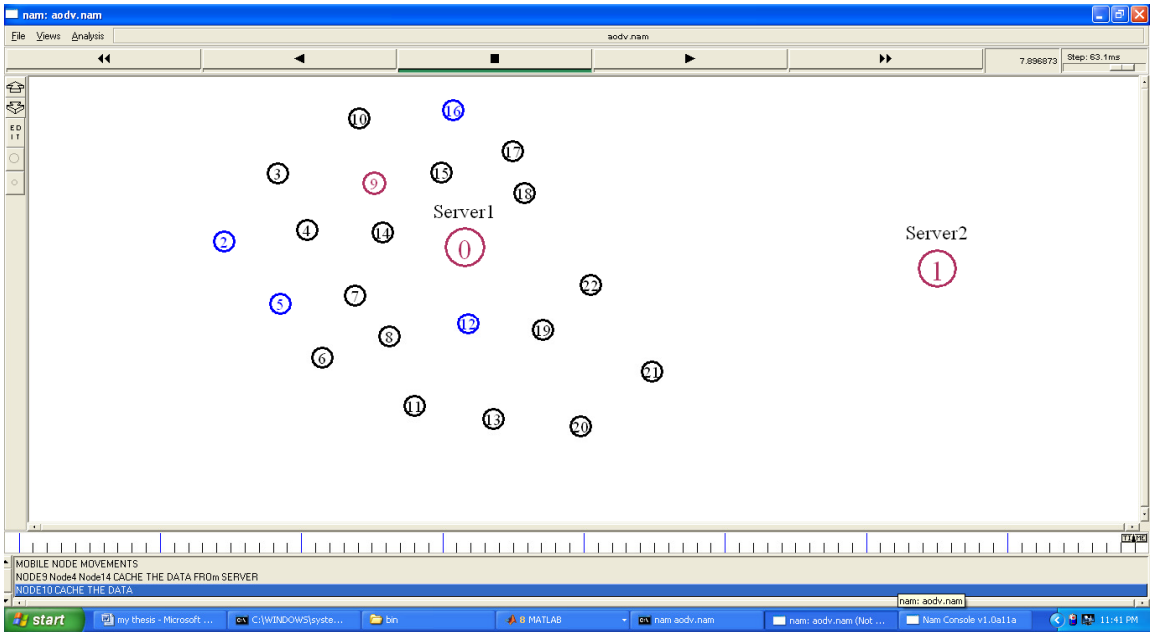



Figure 4 Scenario 2 to test the DDOS Attack

The mobile Adhoc network comprising of 23 mobile nodes are constructed in the NS-2 simulator with the use of TCL script in the topological boundary area of 670 m x 670 m. We have used two servers to manage the node movement over the network. One is a head for all node transferring data and other for monitoring the packet loss etc. In this figure the blue nodes represents all the nodes that are detected as the victim nodes i.e. where most of the time the packet is being lost more then threshold value.

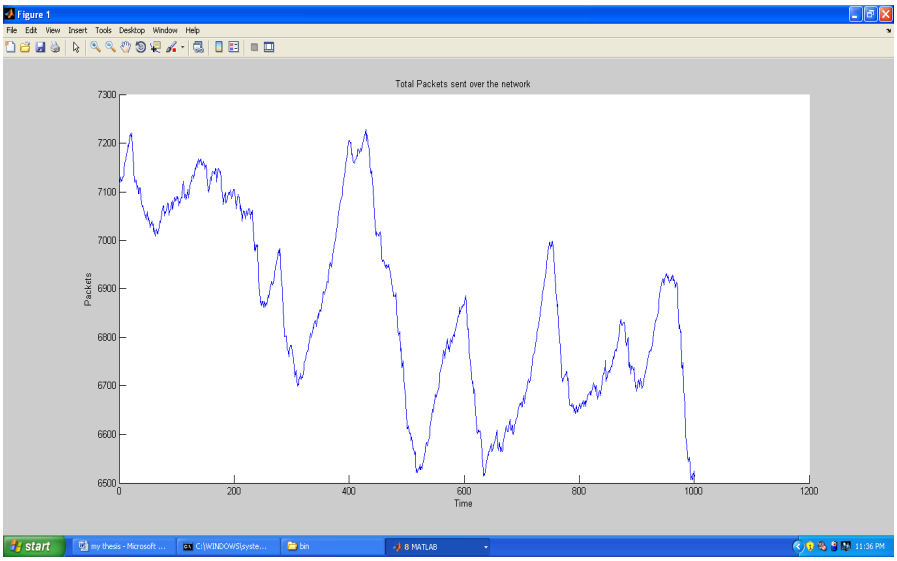



Figure 5 Number of packets being transferred over the network.

This graph represents the how many packets have been transferred from source to destination. It represents that how packets being transferred over the network according to time.

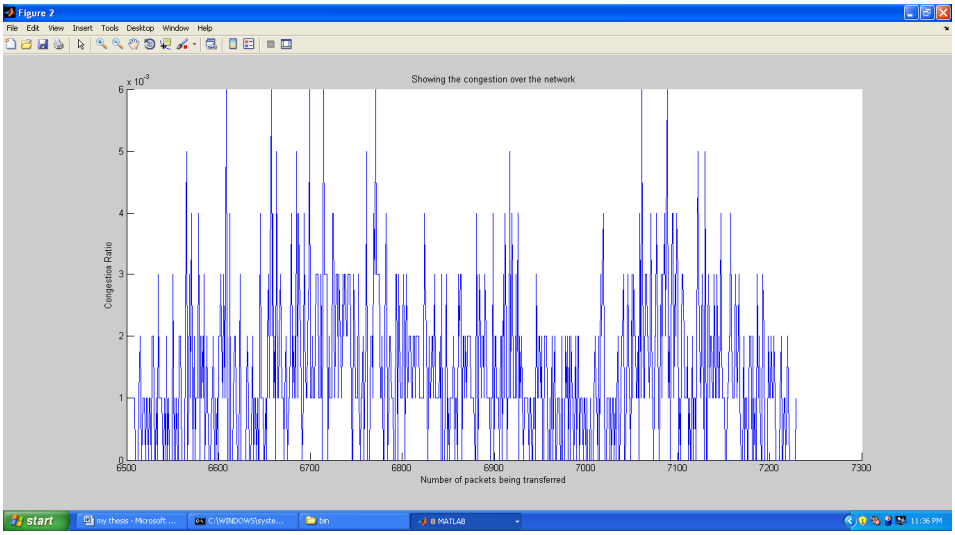



Figure 6 Congestion occur over the network.

It represents the congestion occur when ever the packets being transferred is sown in fig 6. As we can see as the no. of packet increased in the network when ever the congestion increased**.**

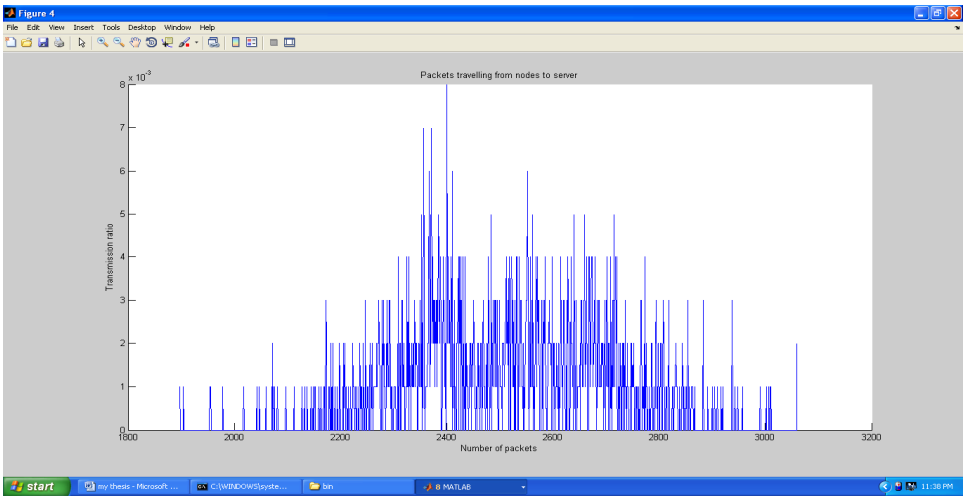



Figure 7 Transmission ratios of the packets over the network**.**

The packets are traveling from nodes to server. It describes total number of packets transferred to server and finds the transmission ratio of packets over the network.

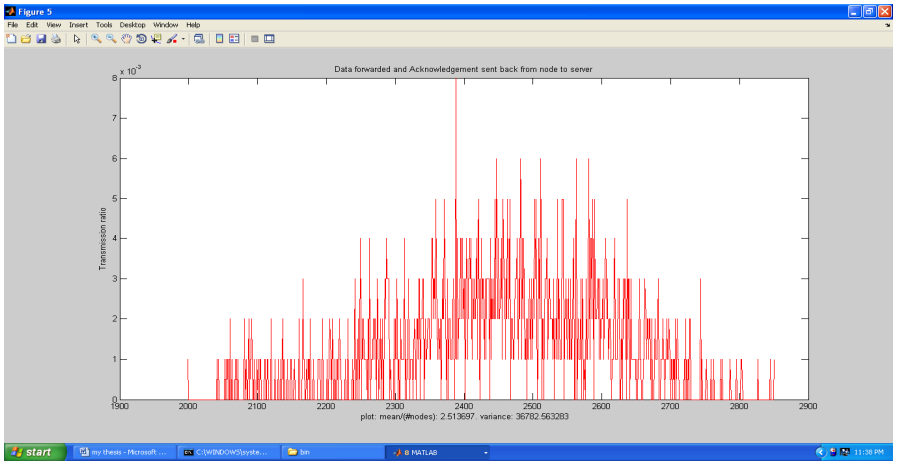



Figure 8 simulates the mean and variance of the transmission ratio.

It shows a distance graph from the mean packets transmitted over the network and represents the mean and variance of the transmission ratio.

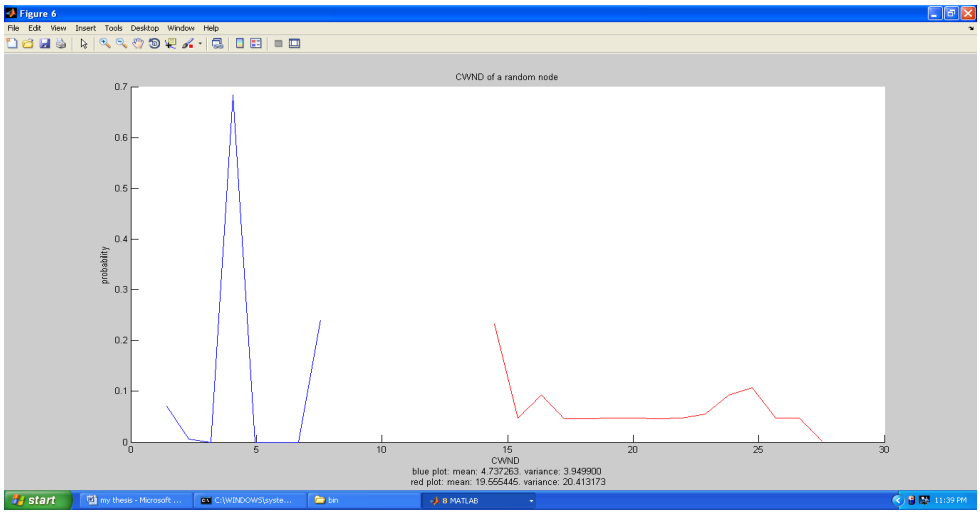



Figure 9 Probability of the congestion occurrence

It represents the probability of the congestion occurrence is shown in fig 9. The congestion will occur respective to the number of packets being transferred over the network. And also describe the congestion of random nodes.

## 6 Conclusions

In this paper we discussed DDOS attack and proposed a technique which is use to detect the attack. We proposed an algorithm which uses detection system to detect the attack. This work introduces an approach based on immune networks to analyze the network traffic, which focuses on the intrusion detection process for DOS flooding attacks. The idea behind the proposed approach is to dynamically cluster the network traffic and monitor activity of the clusters to look for dominating features of the traffic. Such approach allows in the first place togather information about incoming, or proceeding attack, to take the most efficient counter measures against the threat.

The results of the ongoing research presented in this paper show different interesting properties of the proposed approach, like recognition of repetitiveness of the traffic, temporary memorization of passing events and response to the current network context. These features combined with low resource consumption during experiments are encouraging future research in this field.

## 7 References

[1] Shanthi, N. et al. (2009) "Study of Different Attacks on Multicast Mobile ADHOC Network," Journal of Theoretical and Applied Information Technology, VOl.10 No.1, December 2009.

[2] Sargolzaey et al. (2009) **"**A Review and Comparison of Reliable Unicast Routing Protocols For Mobile Ad Hoc Networks," JCSNS International Journal of Computer Science and Network Security, VOL.9 No.1.

[3] Sklyarenko et al. (2009) "AODV Routing Protocol," European Journal of Scientific research, VOL.5 No.3

[4] Sengottaiyan et al. (2009) "Modified Routing Algorithm for Reducing Congestion in Wireless Sensor Networks," European Journal of Scientific Research, Vol.35 No 4 Department of Computer Science and Engineering, Nandha.

[5] Sarla Kumari et al. (2010) "Adhoc Network Routing Protocol," International Journal of Technology and Applied Science. VOL .4 No 3

[6] V.Vasanthi1 et al. (2010) "A Perspective Analysis of routing protocols in wireless sensor network," International Journal on Computer Science and Engineering**,** VOL.2, No. 8, November 2010.

[7] Mohammed Aleem (2009) "MANET Article about advantages and disadvantages," http://www.saching.com/Article/MANET---Mobile-Adhoc-network, 9 November, 2009.

[8] C.Siva Ram Murthy et al. (2004) **"**Ad Hoc Wireless Networks, Architectures and Protocols," published by Prentice Hall, 2004. http://airccj.org/CSCP/vol1/cscp0104.

[9] Shoaib et al. (2010) "Analysis of Black Hole attack On MANET Using different MANET Routing Protocols," it accessed on 29 Jun, 2010. www.seamist.se/com/mscee.nsf/attachments/.../2698_Thesis_Report.pdf

[10] Perkins et al. (1999) "Ad-hoc On-Demand Distance Vector Routing," Personal Communication IEEE, Issue Date: Feb 2001, VOL.8 Issue 1.

[11] Luke Klein (1999) "A Quick Guide to AODV Routing," National Institute of standards and technology, US. It accessed on 18 March, 2010.

[12] Dhaval Gada et al. (2004) "A Distributed Security Scheme for Ad Hoc Networks," Mumbai University, India. Magazine Crossroads, VOL 11, Issue 1, September 2004.

[13] Shiv Mehra (2000) **"**Enhancing the performance of mobile adhoc network with Internet Gateways,**"** International Conference on Wireless network, 2004. http://www.informatik.uni-trier.de/~ley/db/conf/icwn/icwn200...

[14] Steffen Reidt (2009) "Efficient, Reliable and Secure Distributed Protocols for MANET," www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-26.pdf . I accessed on 28 January, 2010.

[15] Yinghua Guo (2008) "Defending MANET against flooding attacks by Detective," institute for telecommunication Research, University of South Australia. April2008.http://www.itr.unisa.edu.au/research/publications/thesis/yg.pdf

[16] Bhavana Gandhi et al. (2007) "An Integrated Framework for Proactive Mitigation, characterization and Traceback of DDOS Attacks," Publish in (IJCSNS) international Journal of Computer Science and Network Security, Vol. 7, No. 3, it accessed on 30 Mar, 2007.

[17]Bayya et al. (2008) "Security in Ad-hoc Networks," Computer Science Department, University of Kentucky, www.cs.uky.edu/~singhal/term-papers/Fourth-paper.doc

[18]Gurjinder Kaur et al. (2011)**"**Distributed Denial of Service Attacks in Mobile Adhoc Networks," www.waset.org/journals/waset/v73/v73-128.pdf

[19] Gupt et al. (2011) **"**Truth of DDOS Attacks in MANET," GJCST Vol. 10 issue 15:9-14

[20] Sanjay B Ankali et al(2011) **"**Detection Architecture of Application Layer DDoS Attack" Int. J. Advanced Networking and Applications Volume: 03.

[21] Aleksey A. Galtsev et al(2011)" Network attack detection at flow level"

**Author1**

Dr. Vikram Singh is presently working as Professor of CSE Department, in Chaudhary Devi Lal University, Sirsa (haryana). He published many papers in National/ International journals and conferences. He posses qualification of P.H.D. His research interests are in Network Security, Operating System,Visual Basic.

**Author2**

Ms. Vatika has completed her B.Tech degree in Information Technology from BRCM Engineering college Bahal, Maharshi Dayanand University, Rohtak, India in the year 2008, and She is pursuing M.tech in Computer Science and Engineering, Chaudhary Devi Lal University, Sirsa from June 2009.Currently Her research Interests are in Network Security.