International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

Effects of DoS Attacks on the e- voting System and Feasible Measures to prevent them

Darshan Lal Meena
Ph.D. Research Scholar, Dept of Computer Science, Research centre: MITS, Gwalior
MP Bhoj Open University, Bhopal, Madhya Pradesh, India – 462016

Abstract:

An Electronic voting (E-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information .With the rapid growth in computer networks and internet, internet voting system can be a viable alternative for conducting an election and such a voting system must provide the same level of security as ordinary paper based elections. This paper discusses the various security threats for an online internet voting system and describes the most common threat in the communication medium, i.e. Denial of Service Attacks and its effects on the online voting system and describing few measures taken to prevent these attacks. However this paper does not propose a new online voting system. The paper also aims to provide a comparative overview of different authors based on the feasible security measures taken to prevent the denial of service attacks.

Keyword: ***e-voting ,SERVE, Attack, DoS, DDoS, Voting System***

1. INTRODUCTION

Voting is a fundamental right - The heart of democracy is voting. The heart of voting is TRUST that each vote is recorded and counted with accuracy and impartiality. The purpose of an election is not to name the winner, but it is to convince the losers that they lost said by (Dr. Dan Wallach, Computer security expert, Rice University).

An Electronic voting (E-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. The research on E-voting is a very important topic for the progress of democracy. If a secure and convenient E-voting system is provided, it will be used more frequently to collect people's opinion through cyberspace. Internet Voting System is defined as a voting system, where we can cast our vote over Internet and send the vote to the concern election authority or officer safely. Internet voting is intended as a service to the electorate, so that the voters might have more convenience to cast their vote. They can vote from anywhere in the world by any computer connected to the Internet. The implementation of this internet voting system requires various technical solutions to ensure accurate voter authentication, secrecy of the ballot and security. As a voting method, any voting system (internet voting system or electronic voting system) needs confidence, without security there is no Confidence. When designing any security architecture of any internet voting system, they should consider the insecurity of the communication medium. There are many Security threats that are concerned with the internet for many commercial transactions like online payments, but still the advantages outweigh disadvantages for various business activities. And still there are been many research going on whether internet voting is safety or not, particularly in large organization like any government elections in any country, most of the research organizations are still uncertain whether a secure internet voting system is suitable for a large organization or not, because if something goes wrong in the internet voting system, then it would affect the decision of the entire country. And as the internet is open to the world, there are chances of various kinds of threats. In this paper I would introduce different kinds of threats to an internet voting system and as we know that the most common and important threat in internet is **denial of service attack**, so We would explain what denial of service attack is, types of attacks in denial of service and then explain how SERVE [1] or any internet voting system is effected by that and what are the feasible solutions or methods to avoid the attacks. [1, 2]

2. THE E-VOTING DESCRIPTION

Electronic elections gain more and more public interest. Some countries offer their citizens to participate in elections using electronic channels. E-voting is generally any type of voting that involves Electronic means [3]. The letter E is associated with anything that involves web based or computers these days. However, the terminology of E-voting is nascent, and a crucial distinction lies between the various different ways in which voters can vote. E-voting is similar to classic “paper-form” voting. In classical “paper-form” voting voters entering the Polling station have to be identified. If identification is Passed, they are able to vote. The whole scenario of classical voting can be seen in Figure 2.1. There are two recognized types of E-voting systems. The first one is based on visiting a polling station as illustrated in Figure 2.2. In this case voters are still identified by using identification cards. Voters do not fill voting cards as in the paper form but push buttons on various electronic devices. The second type of E-voting system is based on remote technology. Usually voters have the chance to vote by using computers at remote locations or at polling stations. They use computer and internet networks for voting. Voters can vote out with the normal interval for voting (usually office hours). They can also, vote from abroad. These constitute the most important advantages of the remote-based voting system.

➢ **Electronic Voting in India**: In Electronic voting in India has been done with electronic voting machines (EMV) partially in 1998, and totally since 2002.EVMs manufactured in 1989-90 were used on experimental basis for the first time in 16 Assembly Constituencies in the States of Madhya Pradesh (5), Rajasthan (5) and NCT of Delhi (6) at the General Elections to the respective Legislative Assemblies held in November, 1998**.** EMV's are made by two government owned defence equipment manufacturing units. The e-voting system is composed of two pieces of equipment, the voting unit used by the voter, and the control unit, manipulated by the electoral officer. The former has a blue button for each candidate, with capacity for 16 candidates, but since as many as four units can be chained, the number increases to 64 candidates. The latter has three buttons on the surface, one to release a single vote, another to see the total number of vote casts at a given point, and yet another to close the election process. India's Electronic Voting Machines (EVMs) have two main components (1) CONTROL UNIT, used by poll workers, which stores and accumulates votes, and (2) a BALLOT UNIT,(Fig:2.3) located in the election booth, which is used by voters. These units are connected by a 5 m cable, which has one end permanently fixed to the ballot unit. The system is powered by a battery pack inside the control unit. The ballot unit has 16 candidate buttons. If any are unused, they are covered with a plastic masking tab inside the unit. When there are more than 16 candidates, an additional ballot unit can be connected to a port on the underside of the first ballot unit. Up to four ballot units can be chained together in this way, for a maximum of 64 candidates. A four-position slide switch in the ballot unit selects its position in the chain. The Bharat Electronics Limited (BEL) and Electronics Corporation of India (ECIL) are the manufacturers of EVMs in India and the foreign companies in US and Japan supplying micro controllers, EVMs are powered by a 6 volt alkaline battery enabling the use of EVMs all through the country without interruption. A maximum of 3840 votes can be recorded, more than enough for a polling station since they usually have no more than 1400 voters assigned. It is impossible to vote more than once by pressing the button over and over. Once a particular button on the voting unit is pushed, the vote is registered for that particular candidate and the machine gets locked. Moreover, the machines cannot be pre-programmed to favour a party or a candidate, and the selection of EVMs for polling stations is randomized by computer selection.

The benefits of EMV's include saving on paper ballot printing, transportation, storage as well as on counting staff; fast voting counting with result in 2-3 hours as opposed to 30 to 40 hours with the ballot paper system; marking it easier for illiterate people to vote; preventing multiple votes by a single voter; 10 year lasting memory; and safety, sine EMV's use a 6 volt battery, there is no risk for the voter to get an electric shock.

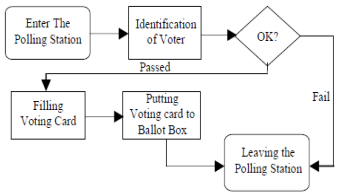


Fig:2.1The classical voting process[4]

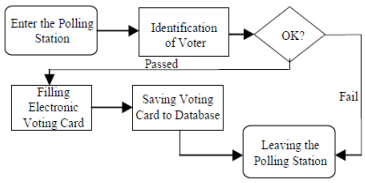


Fig 2.2 The in-site E-voting system[4]

Fig:2.3 EVM used in India for electronic Voting

2.1 Basic requirement for e-voting System: According to **[2]** the basic requirements for the internet voting system are following

2.1.1. Authorization and authentication

Authorization is like only eligible or legal person can vote. For most of the government elections they require a minimum age of 18 years old to cast their vote. It can be done by the trusted authority and this process can be done before the elections. Authentication is the process where the validation of the vote is checked at the time of casting the vote.

2..1.2Mobility

This is one of the important factors in internet voting system; voter should be able to cast his vote from any where in the world, as long they have the required resources with them like internet, PC, etc. For this process authorization, authentication and some security features need to be implemented.

2.1.2 Flexibility "Voters should be able to use different types of devices like desktop, laptop, mobile phones and different networks like Ethernet, wireless and dial-up connections". [2]

2.1.4 Count ability

This process is again dependent on authentication and authorization. If these processes are implemented then Countability accepts, and this is nothing but to see that only the valid votes are counted.

2.1.5 Anonymity

"There should be no link between a particular vote and the person who cast the vote. In mandatory voting systems, the fact that the voter has cast a vote should also be recorded". [2]

2.2 Architecture of electronic voting System: The figure(2.3) describes the system architecture of electronic voting system[3]We will start* by describing the parties which in the figure 2.3 are represented by differently coloured squares and fig(2.4) describes Schematic of Precinct/polling place Elements

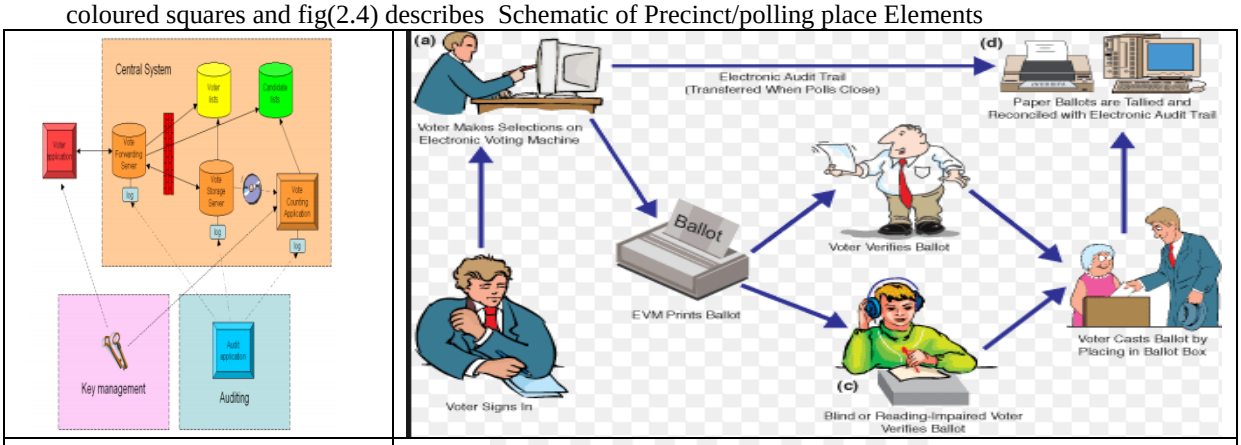


Fig:2.3Electronic Voting System Architecture

Fig.2.4 Schematic of Precinct/Polling Place Element.
(a)Electronic Voting station(b) Electronic Voting Station with Reading-impaired interface(Not shown) (c) Ballot verification Station (d) Ballot Reconciliation Station

***Voter**'s-voter with his/her PC. Create an encrypted and digital vote and send it to the central system.
***Central System**: system component that is under the responsibility of the National Election Committee. Receives and process the vote until the composite result of e-voting is output.
***Key management**:-Generate and manage the key pair(s) of the system. The public key(keys) are integrated into Voter's application, private key(s) are delivered to Vote counting application.
***Auditing**-Solve dispute and complaints, using logged information from the Central system

There are three component of the central system:

- **Vote Forwarding server(VFS)**:-authenticate the voter with the means of ID-card, display the candidate of voter's constituency to the voter and receive the encrypted and digitally signed e-vote. The e-vote is immediately sent to the vote storage server and the confirmation received from there is then forwarded to the voter. Ends it work after the close of advance polls.
- **Vote Storage Server (VSS)-**receive e-vote from the VFS and store them. After the close of advance polls remove double votes, cancels the vote by intangible voters and receive and process e-vote cancellation. Finally it separates inner envelops from outer envelops and readies them for the Vote Counting Application.
- **Vote Counting Application(VCA)-**offline components to which crypted votes are transmitted with the digital signature removed. The Vote counting server use the private key of the system, tabulate the votes and outputs the result of e-voting

E-Voting Threats: According to SERVE [1] the four main threats in internet voting system: [1]

E-voting systems threats exist in many different forms; they can compromise an E-voting system in various ways. Different threats can compromise the various areas of security leading to untrustworthy systems According to report review and critique of computer and communication security issues in the SERVE voting system **(Secure Electronic Registration and Voting Experiment)**[1] the four main threats in internet voting system: [1]

2.3.1 Viruses or Malicious Software

There is a threat of introducing any malicious software onto the internet voting server before or on the Election Day by any communication link or email and also if huge number of PCs (personal computers) connected to the internet voting server, then any PC which is infected with virus, there might be more number of chances to spread the viruses to the voting server. The insecurity of the browser setup or operating system at the user end may easily lead to install the malicious software and which may change the confidentiality and integrity of the vote or even the vote may be changed without the knowledge of the voter before it is transmitted to the voting server. [1]

2.3.2 Hacking

If the links of the voting system is changed or hacked then the voter may face difficulty in casting his vote, which may change the Confidentiality and integrity of the vote. [1]

2.3. **3. Domain name service (DNS) attack**

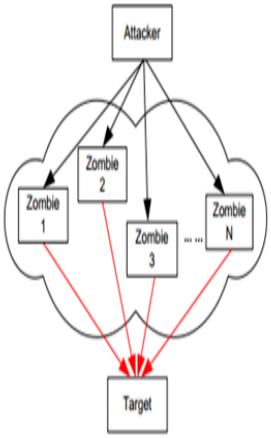
"Attacks against the Domain name service could route traffic to an attacker instead of to the legitimate vote service". [1]

2.3.4. Denial of service attacks (DOS)

This is a threat when the voter tries to cast his vote online and if the hacker overloads the election web server then that may lead to prevent the voter by not casting his vote. This type of attack is known as denial of service attack. According to the report of the SERVE [1] this is one of the serious attacks.

3. ABOUT DoS ATTACKS:

A "Denial-of-Service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: . Examples include: Attempts to "flood" a network, thereby preventing legitimate network traffic, Attempts to disrupt connections between two machines thereby preventing access to a Service, Attempts to prevent a particular individual from accessing a service, Attempts to disrupt service to a specific system or person.



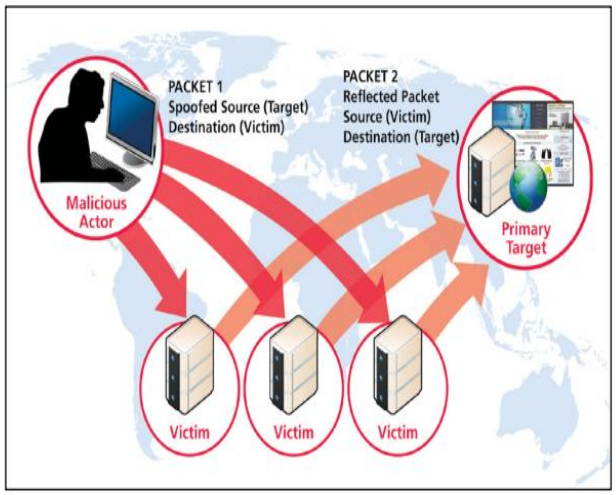


Fig-3.1 DoS Attacks Fig :3.2 DDoS Attacks Fig-3.3 DRDoS Attacks

3.1.1 DoS Attacks: DoS attacks (refer to Figure 3.1), a large number of malicious packets are sent from a single machine, with the aim of exhausting the target's computational and networking resources, or crashing the target. The purpose of such attacks is to deprive legitimate users of access to the target's services**. .** In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server's bandwidth and resources[**6**]

DoS is a threat when the voter tries to cast his vote online and if the hacker overloads the election web server then that may lead to prevent the voter by not casting his vote. This type of attack is known as Denial of service attack. According to the report of the SERVE [1] this is one of the serious attacks.

It is a resource-depleting attack on a network or on the internet such that the network would no longer be able to serve legitimate users. If a user is under denial of service attack then his system may become unreachable due to the depletion of the resources of the system, thus the user could loose the control of his system. The denial of service attack can be directed at an operating system or at the network A proper planned denial of service attack is difficult to detect and may cause severe problem to the internet and as well as to the user. [**5**]

3.1.2 DDoS attack: A distributed denial of service attack (DDoS) (refer to fig 3.2) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. This is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted [**7]**

3.1.3 DR-DoS attacks : distributed reflector denial of service (DRDoS) **(refer to** Figure 3.3) Illustrates another type of bandwidth attack called a **distributed reflector denial of service** (DRDoS) attack, which aims to obscure the sources of attack traffic by using third parties (routers or web servers) to relay attack traffic to the victim. These innocent third parties are also called the reflectors. Any machine that replies to an incoming packet can become a potential reflector. In 2012 there was a significance increase in the use of a specific distributed denial of service (DDoS) methodology known as Distributed Reflection Denial of Service attacks (DR-DoS). DR-DoS attacks have been a persistent and effective type of DDoS attack for for more than 10 years. Denial of Service (DoS) attacks that are carried out have devastating consequences and in most cases the extremely affect the ability to provide availability to a system. Denial-of-service attacks could happen if the computers at a polling place all crashed simultaneously or if computers depending on internet connections to download ballots at the start of an election were denied service.

"Distributed denial of service problems are expected to only become more severe and serious in the future. For instance, they could be used in cyber warfare to disable strategic business, government, public utility, and even military sites. They can also be used by cyber gangsters to blackmail companies that rely on internet connectivity for their revenues". [8]

3.1.4 Types of denial of service attacks: Denial of service attacks are basically divided into three different types [9]

i. Denial of service attack via bandwidth consumption:

In this type of attack basically all the available bandwidth is consumed and no bandwidth remains for legitimate user. Basically a network might be flooded by UDP or ICMP ECHO packets to try and consume all available bandwidth."A simple bandwidth consumption attack can exploit the throughput limits of servers or network equipment by focusing on high packet rates – sending large numbers of small packets. High packet rate attacks typically overwhelm network equipment before the traffic reaches the limit of available bandwidth". [9] "In practice, denial of service is often accomplished by high packet rates, nor by sheer traffic volume". [9]]

ii. Denial of service attack via protocol attack

These attacks are almost directly target the host machines and these are overcome by the patches in the operating system. Examples of protocol attacks.

- "SYN flood is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections". [9]
- In Smurf attack the attacker sends an ECHO request message directed to broadcast addresses. When the request is received by other systems in the network, all the systems in the network will reply to the ECHO message to the target system and as the number of request received from all the systems in the network are high and as it is difficult to manage by the amount of buffer allocated to the target system. [9]

iii. Denial of service attack via logical attack

"Logical attacks exploit vulnerabilities in network software, such as web server, or the underlying TCP/IP stack". [6] Examples of logical attacks are [9]**Teardrop, Land crafts,Ping of death.Naptha**

4. How Denial of Service Attack Affects on e- Voting System.

According to the SERVE [1] report, "denial of service attack are serious risk for SERVE" [1]. The author says that it can affect the internet voting system in two different ways of denial of service attacks, in the first attack an hacker may able to change the network connection of the targeted web server with junk data that clogs the network and prevents the user or voter by accessing the web server and casting his vote. [1] A real time example in our daily life for this kind of attack is an email address we get more than 100,s of junk mails which are not relevant to us, and we waste most of the space in the mail box, by this we miss the required or wanted mails as they bounced because the inbox is filled with the unnecessary junk mails. In the same way the hacker could overload the election web server with irrelevant data and prevent the electorate to cast his vote. "On the internet, denial of service attacks are often much more devastating, because internet denial of service attacks can be automated with a computer, and because suck attacks can often be mounted untraceably over the internet. [1]

In the second attack the hacker may put irrelevant resources with useless task on the election web server so that the server is busy; as if the server is busy it may unable to respond to the legitimate voters. This type of attack may mostly done on the last day of the election, as most of the electorate may plan to cast their vote on the last day, so if this kind of attack is done on the last day then most of the voters may fail to cast their vote.

5. Feasible Measures for Denial of Service Attacks:

According to Cyber vote [10] some of the security measures that can be taken to avoid the denial of service attack [10]

"As a measure of precaution, routers have to be upgraded with the implementation of secure routing protocols. One of the more common methods of blocking a "denial of service" attack is to set up a filter, or "sniffer," on a network before a stream of information reaches a site's web server. The filter can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed to block messages containing that patter, protecting the web server from having their lines tied up". [10]

According to [11] some of the security measures can be taken to avoid denial of service attack

- Filtering all the packets in the network which are entering and leaving the networks can prevent attacks from the neighbouring networks. "This measure requires installing ingress and egress packet filters on all routers". [11]
- Upgrade the host computers with the latest security patches and techniques, for example in case of the SYN flood attack. Increase the size of the connection queue, decrease the time-out waiting for the three-way handshake and employ vendor software patches to detect and circumvent the problem, these can be done to protect the host computers can take to guard themselves from the denial of service attack. [11]
- Disabling the IP broadcast, the host computers will not used as amplifiers in ICMP Flood and Smurf attacks. To prevent this attack all the neighbouring networks need to be disable IP broadcast. [11]
- Unused network services should be disabled to prevent tampering and attacks.[11]
- Monitoring the traffic patterns on the network can know when the system is under attack, and can protect itself by the attack. [10]

6. Conclusions

In this paper we discussed about the internet voting system and its security threats, concentrating more on a particular threat namely, denial of service attacks on the Internet. The other variants of these kinds of attacks and few possible

counter measures that can be implemented in order to reduce the denial of service attacks. In accordance with the arguments presented in the report [8] it can be derived that there is no realistic prevention technique to avoid denial of service attacks. There exist few precautionary measures which reduces the possibility of such attacks. According to the authors of [11] they argue that there is no complete solution in preventing the denial of service attacks, only few measures can be taken to avoid and defend to these attacks. From the above articles and arguments produced by the authors of these articles I conclude that there are no complete defensive techniques existing for the resisting denial of service attacks. But only they are some precautionary measures which can be taken to avoid and defend the denial of service attacks. Hence I conclude that without the complete prevention of these attacks it's not a good idea to implement online internet voting system for any organization like any country's government Elections, as the total outcome of the election depends on the securing functions of the online voting system

ACKNOWLEDGMENTS

Author like to thanks to my Ph.D Research guide Dr. R.S.Jadon and Pre-Ph.D Course work Director Dr. Praveen Jain for his deep efforts and support towards the development of this research paper. Also, Author would like to thanks MITS, Gwalior and resource persons of Pre-Ph.D Course conducted by MP Bhoj open University for providing such a valuable dataset for research in the field of. *Effects of DoS Attacks on the internet voting system and* Feasible *measures to prevent them*

REFERENCES

[1] A Security Analysis of the Secure Electronic Registration and VotingExperiment (SERVE)D. Jefferson, A. Rubin, B. Simons, D. Wagner.

[2] Internet voting: concerns and solutions Chuan-Kun Wu; Sankaranarayana, R.;Cyber Worlds, 2002. Proceedings. First International Symposium on, 6-8 Nov.2002 Pages: 261 – 266

[3] IPI, "Report of the National Workshop on Internet Voting: Issues and Research Agenda," *Technical Report*, Internet Policy Institute, Washington, 2003

[4] Gibson S., "Distribute Denial of Service Attack," available at: http://www.grc.com/dos/drdos.htm, last visited 2011

[5] Protecting the Internet from distributed denial-of-service attacks: a proposalCrocker, S.D.; Proceedings of the IEEE, Volume: 92, Issue: 9, Sept. 2004 Pages: 1375 – 1381

[6] Charalampos Patrikakis, Michalis Masikos and Olga Zouraraki, "The Internet Protocol- Vol 7, Number 4

[7] Jelena Mirkovic,Sven Dietrich,David Dittrich,Peter Reiher, "Internet Denial of Service:Attack and Defencse

[8] Results of the Distributed-Systems Intruder Tools WorkshopCERT Coordination Center and otherhttp://www.cert.org/reports/dsit_workshop.pdf , Nov 1999

[9] **Managing the Threat of Denial-of-Service Attacks v10.0** Allen House holder, Art Manion, Linda pesante, George M. Weaver, CERT/CC CERT Coordination Centre in collaboration with Rob Thomas October 2001 www.cert.org/archive/pdf/Managing_DoS.pdf

[10] **CyberVote consortium. D6V1, Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting, January 28, 2002. Vol.1.** http://www.eucybervote.org/TUE-WP2-D6V1v1.0.pdf

[11] **Defeating distributed denial of service attacks,** *Xianju Geng; Whinston, A.B.;*IT Professional , Volume: 2 , Issue: 4 , July-Aug. 2000 Pages:36 - 42

AUTHOR PROFILE

Mr.Darshan Lal meena is working as PGT(Computer Science) in Kendriya Vidyalaya ,Sarni Under MHRD,Govt.of India and Presently pursuing Ph.D (Computer Science) from ,MP Bhoj Open University, Bhopal, Madhya Pradesh Under the supervision of Dr.R.S.Jadon Professor & Head ,Deptt.of Computer Application ,MITS Gwalior. Research Centre of Ph.D is MITS,Gwalior. Area of research is Network Security, DDoS Attacks in which author tried to find **Novel Solution for Distributed Denial of Service Attacks.**