# DDoS Defense Mechanism by applying stamps

**S S Nagamuthu Krishnan**
(PhD Research Scholar, Bhartathiar University, Coimbatore – 641 146, Tamilnadu, INDIA)

**Dr. V. Saravanan**
(Professor & HOD, Department of Computer Application, Karunya University, Coimbatore – 641 114, Tamilnadu, INDIA,

**Abstract:**
In current trend, internet plays a vital role in our life and distributed computing structure grows dramatically in size, functionality and complexity and has become the integral part of our life. In distributed network computing there are lot of vulnerabilities such as Dos, DDos (Distributed Denial of service),virus, worms, etc. Distributed Denial of Service Attacks has recently emerged as one of the most newsworthy. Denial of service (DoS) attacks have continued to evolve and impact Internet Infrastructure. The control mechanisms for DDoS attack networks are changing to make greater use of Internet Relay Chat (IRC) technology. The impacts of DDos attacks are causing greater collateral damage, and widespread automated propagation itself has become a vehicle for causing denial of service. In our paper we propose a solution to prevent our network system resources from DDos attacks applying stamps.

***Keywords:***
*DDos, DefCOM, Stamping,PRNG, CPRNG*

## 1. Introduction:

Distributed denial of service (DDoS) attacks aim to disrupt the service of information systems by overwhelming the processing capacity of systems or by flooding the network bandwidth of the targeted business. Recently, these attacks have been used to deny service to commercial web sites that rely on a constant Internet presence for their business. The attacks differ from traditional DDoS attacks in the targeted nature and shear number of attacking hosts. Even hardened Internet companies such as the SCO group and Microsoft are not immune to attack, and historically high-profile retailers such as eBay have had their services disrupted.The threat from the latest attacks has become greater due to the political and financial agendas of those instigating them, particularly the involvement of international organized crime in protection extortion attempts.

This was a major event, covered in the major news media. They have done an excellent job in their coverage; as far as it has gone, their coverage has been accurate. The problem is, their coverage hasn't been sufficiently detailed to explain why we cannot track down the people committing these attacks, and why we can't defend against them. There's a good reason for these omissions: the attack is subtle, and understanding how it works well enough to understand why we can't cope today, and what will have to change before we can, requires a more detailed explanation of how the Internet is constructed than the mass media are prepared to deliver to their audiences. There is no simple solution to mitigate the risk of these attacks, but there are strategies that can help minimize the impact of a large-scale attack. In our SSRDM (Secure System Resource Defensive mechanism) we provide way to protect our system resources.

## 2. Distributed denial of service:

DoS / DDoS attacks are a virulent, relatively new type of Internet attacks, and have caused some biggest web sites on the world. Let us move to a discussion on Dos

### 2.1 Inside Denial of service:

Denial of service is accomplished technologically. The primary goal of an attack is to deny the victim(s) access to a particular resource. It is an explicit attempt by attackers to prevent legitimate users of a computer-related service from using that service. But, as any information and network security issue, combating denial of service is primarily an exercise in risk management. To mitigate the risk, we need to make business decisions as well as technical decisions. Managing the risks posed by denial of service requires a multi-pronged approach:

- Design the business for survivability. Have business continuity provisions in place.

Manuscript received August 5, 2009
Manuscript revised August 20, 2009

- Design the network for survivability. Take steps that help to ensure that critical services continue in spite of attacks or failures. (Keep in mind that increased complexity means increased costs and decreased reliability.)
- Be a good netizen (net citizen). The potential to be attacked depends on the security of other sites and vice versa. The threat to network is directly proportional to the extent that other Internet users, including home users, adhere to good practices. Conversely, the threat that your network represents to others is irectly proportional to the extent that your organization adheres to good practices.Denial of service may be indistinguishable from a heavy (but otherwise legitimate) load on your network. For example the victim might be flooded with legitimate connections to his web site as a result of a major news event such as the disaster that occurred on tember 11, 2001. Users might have difficultly connecting to the web site simply because so many people are trying to connect at one time and not because it is the target of a denial-of-service attack. It is important to establish criteria by which it can be declared that the site is “under attack” and invoke emergency procedures. Mitigation strategies for attacks and heavy legitimate traffic may be similar.

## 3. Realeted work:

The Defensive Cooperative Overlay Mesh DefCOM)[1] is an example design of a distributed framework for DDoS defense. DefCOM consists of heterogeneous defense nodes organized into a peer-to-peer network, communicating to achieve a dynamic cooperative defense. Defense nodes are organized in a peer-to-peer network whose topology construction allows approximation of the underlying routing topology. During the attack they discover the victim-rooted franc tree, thus identifying upstream-downstream relationships between peers. They then devise the appropriate rate limits to restrain the attack traffic, and place them as close to source networks as possible. At the same time, classifier nodes differentiate legitimate from attack streams. All nodes in the framework give preferential service to legitimate traffic.

### 3.1 Traffic tree discovery

When a DDoS attack occurs, the alert generator node closest to the victim detects it and propagates the alert message to all nodes in the peer network. They cooperate to trace out the topology of the victim-rooted traffic tree by deploying secure tragic stamping. Tracing of the tree structure enables each node to assign upstream or downstream classification to its peers, thus defining its policy and message types to be sent to these peers. Secure packet stamping actually serves four purposes: [1] discovery of the victim-rooted traffic tree topology, [2] differentiation of traffic types, [3] protection of legitimate traffic and [4] transparent operation through legacy touters. Each active defense node picks a stamp and communicates it securely to its neighbors. The node places this stamp in the header of packets it forwards to the victim. It also observes packets it receives from its neighbors, looking for their stamps. A node becomes a parent of a neighbor if it observes its neighbor's stamped traffic. A parent sends an explicit message to its children to inform them of their child status. To protect the packet stamping mechanism from misuse, every pair of neighboring nodes uses stamps unique to them, and changes the packet stamps on a frequent basis, using encryption for privacy and authentication to establish a secured communication channel for this exchange.For instance, for IPv4, IP Traceback [3] suggested overloading the IP identifier field in the IP header, pointing out that less than 0.25% of IP packets are fragmented. The eventual adoption of IPv6 will offer better options for packet stamping. A malicious outsider falsely reporting a DDoS attack will be a serious problem. If the false report is believed and DefCOM deploys distributed responses that rate limit traffic inbound to the supposed victim, potential damage can be done to legitimate traffic. This attack would effectively use DefCOM to degrade the victim's service (it couldn't quite *deny* service, but it could reduce it). It is planned to investigate scalable methods to allow potential victims to delegate alert-generation responsibility and to enable DefCOM nodes to authenticate alert signals. DefCOM nodes will only recognize those alarms that are signed by the victim or its delegated alert generators. A scalable authentication through a public key infrastructure (PKI) will probably be necessary to verify the alarms, but the PKI infrastructure itself must be protected. That problem is likely to be manageable, because DefCOM's defenses can be activated to protect PKI servers, and also because the PKI service would not be a general public service; it is limited to the set of previously authenticated DefCOM nodes, so approaches like [4] are likely to be effective. Alert-generator nodes might become compromised and issue false alarms. We also plan to investigate ways to allow victims to revoke alert generator responsibility from compromised nodes. Broadcast encryption [5] is a promising approach that has scalable revocation properties compared to traditional PKI.

## 4. SSRDM (secure system resource defence mechanisum):

In DefCOM, If the false report is believed that legitimate packet may consider as attacker packet, and Def-COM deploys distributed responses that rate limit traffic inbound to the supposed victim, potential damage can be done to legitimate traffic. This attack would effectively use DefCOM to degrade the victim's service. In DefCOM they have used stamping technique for acknowledgement; and the problem with this architecture is where to place the stamps in packet format. In our SSRDM architecture we provide the solution for the above mentioned problem by using the packet header free space.The distributed environment is one in which there are so many possibilities of attacks to happen. Here, we are considering two possibilities of attacks in distributing environment.

In the scenario of sharing the common memory in distributed environment has more number of legitimate users. So, there may be a chance for the intruders to attack the users who are utilizing the common shared resource. Obviously, the attacker knows that who are all using the resource.

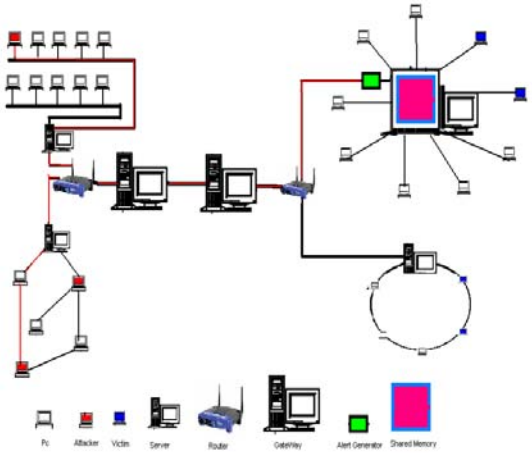


Fig-1 (Distributed Environment)

In the above specified SSRDM architecture there are three attackers (red Nodes), who are trying to attack the victim node simultaneously and attacker path is shown in red line. In distributed environment all the nodes use the shared memory which contain main server due to that all the attacker trying to access shared memory, if they accessed all legitimate user won't get proper service. There are two type of prevention mechanisms are One is preventive and another one is Reactive, where preventive is better than reactive because once the attack happen CPU utilization, buffer overloading and memory utilization become very low. We propose preventive algorithm to avoid DDos attack using stamps.

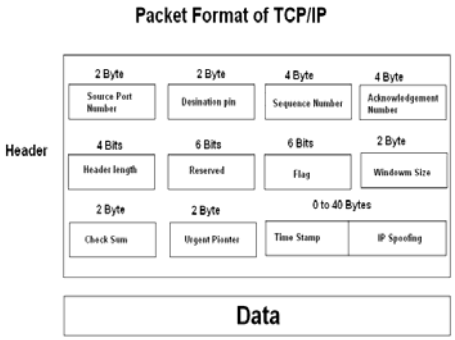



Fig 2 (Packet Format)

### 4.1 Damages and Costs:

There may be hidden costs associated with denial-of-service attacks. For example, the direct target of a DoS attack may not be the only victim. An attack against one site may affect network resources that serve multiple sites. Or resources that we share with other parties (upstream bandwidth) may be consumed by an attack on someone else—another customer of our Internet service provider is attacked, so our upstream connections and routers are not as available to our legitimate traffic. Thus, even when we are not the target of an attack, we might experience increased network latency and packet loss, or possibly a complete outage.

### 4.2 Inside Distributed Denial of service

The attacker installs DDoS software on certain machines, allowing them to control all these burgled machines to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims**.** The perpetrator starts by breaking into weakly-secured computers, using well-known defects in standard network service programs, and common weak configurations in operating systems. On each system, once they break in, they perform some additional steps. First, they install software to conceal the fact of the break-in, and to hide the traces of their subsequent activity. The attacker runs a single command, which sends command packets to all the captured machines, instructing them to launch a particular attack (from a menu of different varieties of flooding attacks) against a specific victim. When the attacker decides to stop the attack, they send another single command.

4.2.1 Types of attack

DDoS attacks can take several approaches. Five common techniques are used to implement DDoS attacks [2]. Smurf Attacks send an ICMP Echo Request to the victim's network address with the victim's address as the source address. This causes all the computers on the network to reply with ICMP Echo Reply messages to the victim, thus overloading it. TCP SYN Attacks repeatedly send connection requests to the victim's server using an unreachable network address as the source IP address. The victim then replies to the invalid user with an ACK and SYN according to the three way handshake mechanism of TCP and awaits an ACK from the unreachable host. This results in several pending connections that drain the server's memory resources. UDP, TCP and ICMP Attacks flood the victim with packets continuously and at a high rate, requesting replies and thus causing congestion in the network. All of the above attacks use IP spoofing to conceal the identity of the attacker or direct traffic to a certain destination. In order to classify and evaluate the different defense mechanisms studied, it is important to first dissect the various attack methods. As can be observed from the mentioned DDoS attacks, they are mainly distinguished according to which system vulnerability they exploit: attacks taking advantage of some of the protocols' particularities such as Smurf and TCP SYN attacks are called protocol attacks, and those targeting the victim directly such as UDP, TCP and ICMP attacks are called brute force attacks. This classification is useful to distinguish on which attack types the defense methods are most effective.How do we know if an attack is happening? Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack: unusually slow network performance,unavailability of a particular web site ,inability to access any web site ,Dramatic increase in the amount of spam you receive in your account.How do we avoid being part of the problem? Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other omputers:Install and maintain anti-virus software ,Install a firewall, and configure it to restrict traffic coming into and leaving your computer.Follow good security practices for istributing your email address (see Reducing Spam for more information). Applying email filters may help you manage unwanted traffic.

## 5. Proposed Method-stamping mechanism

Data will be transferred in a peer to peer manner. Between two systems they transfer acknowledgement using stamps. So we need to place the stamps in packet, and so we propose a new packet format to place stamps. In ordinary TCP/IP, the packet size is 20 byte with optional 40 bytes and nearly 10 bytes are free in TCP/IP header. In that we use 2 bits for stamping.0Stamping uses random number generation method to produce numbers within certain domain values that will differ from network to network. To generate the random number we used A cryptographically secure pseudo random number generator (CSPRNG). It is a pseudo-random number generator (PRNG) with properties that make it suitable for use in cryptography.

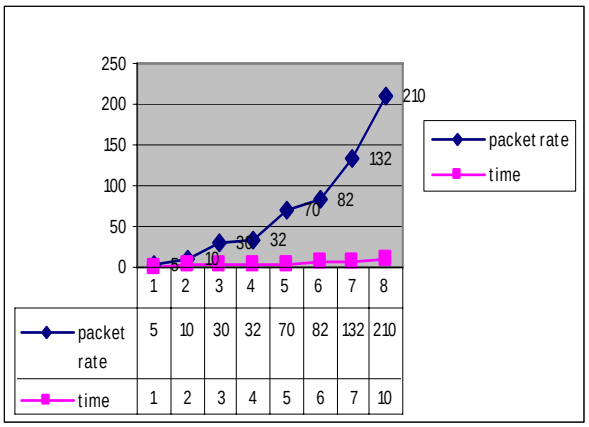
### 5.1 Cryptographically secure pseudo-randam number generator

The requirements of an ordinary PRNG are also satisfied by a cryptographically secure PRNG, but the reverse is not true. CSPRNG requirements fall into two groups: first, that they pass statistical randomness tests; and secondly, that they hold up well under serious attack, even when part of their initial or running state becomes available to an attacker.

- Every CSPRNG should satisfy the "next-bit test". The next-bit test is as follows: Given the first $k$ bits of a random sequence, there is no polynomial-time algorithm that can predict the ($k$+1)th bit with probability of success better than 50%.
- Every CSPRNG should withstand 'state compromise extensions'. In the event that part or all of its state has been revealed (or guessed correctly), it should be impossible to reconstruct the stream of random numbers prior to the revelation. Additionally, if there is an entropy input while running, it should be infeasible to use knowledge of the input's state to predict future conditions of the CSPRNG state.

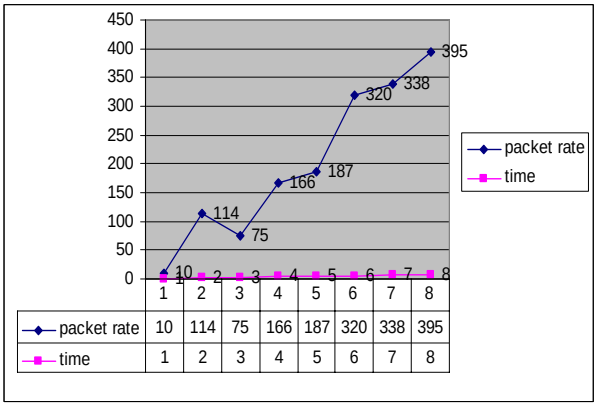
There are varieties of algorithmic models available in "cryptographically secure random number generator" in which we used simple hardware random number generator. It generates the random number and applies cryptography technique in random key which is placed into the stamps for acknowledgement; thatt will be sent from one node to another if the nodes are in different networks. Router takes the detection process using random number domain values. Even though the intruder pass the data between the nodes he can't access the shared memory because we implemented the packet

format checking and stamp checking in alert generator, and if any malicious packet is found it will simply discard that packet and also generate the alert signal to other active nodes. It takes the traffic tree discovery operation to find out attacker system. It completely eliminates the IP spoofing attack and other packet format attack.




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| packet rate | 5 | 10 | 30 | 32 | 70 | 82 | 132 | 210 |
| time | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 10 |

Fig: 3 (Proposed method)




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| packet rate | 10 | 114 | 75 | 166 | 187 | 320 | 338 | 395 |
| time | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Fig:4 (Existing methods)

Performance graph shows the rate limiting difference between the proposed method and existing one..

## 6 Result anaysis:

- SSRDM eliminates the packet spoofing up to 97% ,
- It optimally use bandwidth of network which automatically reduce rate limiting,
- It eases the process of finding the traffic tree
- It increases the overall network performance

## 7 Conclusion:

The DDoS field contains a multitude of attack and defense mechanisms, which obscures a global view of the DDoS problem. This paper is a first attempt to cut through the obscurity and structure the knowledge in this field. In our proposed method, it eliminates the distributed IP spoofing and packet format problems. It is an attempt to apply the cryptography concept to secure the data transfer and also improve the over all performance of the network.

## 8 Further work:

The proposed solution works for a distributed environment towards mitigating DDos attacks. It introduces the concept of time stamps as a part of the packet format which in turn enables added on authentication for incoming packets.

In future the method can be enhanced by adding more security in data transfer applying the cryptography principle for stamps.

### 9 Acknowledgements:

***Mr. M. Srinivasan, Faculty member,*** Thiagarajar School of Management, Madurai-625005.
**S.Rajeshwaran.** Thiagarajar school of management Madurai-625005
**R.Sundaranarayanan.** Thiagarajar school of management Madurai-625005
**R.Surendiran.** Thiagarajar school of management Madurai-625005

## 10 References:

[1] Jelena Mirkovic, Max Robinson, Peter Reiher, Alliance Formation for DoS Defense.
[2] Noureldien, N. “Protecting web servers from DoS/DDoS flooding attacks: a technical overview.”
[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson.Practical network support for IP traceback.
[4] A. D. Keromytis, V. Misra, and D. Rubeustein. SOS:Secure overlay services.
[5]J. Lotspiech, S. Nusser, and F. Pestoni. Broadcast encryption's bright future.
[6] A. Garg and A. L. N. Reddy. Mitigation of DoS attacks through QoS regulation.
[7] T. M. Gil and M. Poletto. MULTOPS: a data-structure for bandwidth attack detection.
[8] J. Ioannidis and S. M. BeUovin. Pushback: Router-based defense against DDoS attacks.
[9] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks.
[1O] A. D. Keromytis, V. Misra, and D. Rubeustein. SOS:Secure overlay services.