Optimizing DDOS Attacks Using LCIA

Supriya Sawwashere¹, Sanjeev Shrivastava², Ashutosh Lanjewar³, D.S.Bhilare⁴

¹,³Guru Nanak Institute of Engineering and Technology, Nagpur, India
²⁴DAVV, Indore, India

Abstract

Security is the most important parameter for ideal network. Various attacks are of great challenge and proved as obstacles for constructing the ideal network. Distributed Denial of Service (DDoS) is one of threats which damage the network applications and affect the bandwidth consumption. There are many Legitimate Traffic detecting mitigation algorithms exists to overcome the network attacks. This project mainly concentrates on implementing the Legitimate Chance Inspection Algorithm (LCIA) for Optimizing DDOS Attacks. In LCIA the number of packets being malicious under the Legitimate packets are removed for improving the network performance. There are two challenges in order to overcome the DDoS, firstly there is need to identify the machine from which malicious flow is generated and secondly minimizing the attack of those malicious attack on legitimate traffic flow. In LCIA, basically a mathematical equation and is implemented to find the number of malicious packets in the network.

Keywords: DDOS, Security, Quality of service, Attacks

1. INTRODUCTION

Network Security is the most important parameter for ideal network. It consists of the provisions and policies adopted by a network administrator to prevent and monitor illegal access, mistreat, alteration or denial of a computer network and network-accessible resources. It involves the access authorization to data in the network, which is monitored by the network administrator. It covers a variety of computer networks, such as public and private, used everywhere conducting transactions and communications among businesses, government agencies and individuals. It is involved in industries, organizations, and other types of institutions. Internet is growing in day to day applications. Generally to protect the information, hiding it from the unauthorized access and unauthorized changes make that information available only to the authorized users. Internet is a complex network due to changes in network traffic load, traffic assimilation, mixing of congestion control actions, on/off flows. Due to these reasons, the statistics of arriving traffic changes dynamically. The available link bandwidth varies in accordance with the statistics of the input traffic. Various attacks are of great challenge and proved as obstacles for constructing the ideal network. Distributed Denial of Service attack is one of the most widely spread problems in internet application is Distributed Denial of Service (DDoS) attacks. It is one of the foremost damaging threats faced by most of the web applications. Under the DDoS attacks, attackers affected the normal users to achieve the bandwidth-consumption attacks. This attack includes IP spoofing, smurf and fraggle attacks and resource starvation attacks include SYN floods. To minimize the effect of an ongoing attack, mitigation process is used. The basic problem with this strategy is to distinguish between legitimate and illegitimate client packets. Attackers are making their attacks impossible to determine whether a packet belongs to legitimate client or an attacker. It is a large-scale, coordinated attack on the availability of services of a victim system or may be through many negotiated computers on the Internet. The frequency of DDoS attacks that target to the internet is continuously increasing to slow down a victim server. In DDoS, the attack is initiated from a large number of attackers. The motives and targets of DDoS attacks can greatly vary. The DDoS attack is that they involve concerted efforts to saturate the victim machine (often a web-server) with a large volume of traffic, which causes the server unable to respond to authenticated user requests. The most common way of executing a DDoS involves the use of a system of corrupted/infected nodes, which is called as botnet.

2. TYPES OF DDOS ATTACKS:

A denial-of-service attack is defined as an explicit attempt made by attackers to avoid authenticated users in the network. Generally DoS attacks can be formed as crash services and flood services. A DoS attack can be implemented in various ways. The five basic types of attack are a) computational resources consumption, such as bandwidth, disk space, or processor time, etc b) Distraction of configuration information, such as routing information c) Distraction of information at a particular instance, such as unwanted resetting of TCP sessions. d) Distraction of physical network components. e) Obstructing the message medium between the intended users and the victim so that they will not be able to communicate adequately.

A DoS attack may implement malware functions in the systems intended to: a) Maximize the processor's usage, preventing any work from occurring. b) Trigger errors in the microcode of the machine c) Trigger errors in the sequencing of instructions, so that it should be possible to force the computer into an unstable state or lock-up d) Exploit errors in the operating system, to cause resource starvation and thrashing e) Crash the operating system. The rest of this paper is
ordered as the related works in Section 3, working of LCIA in Section 4 and the proposed work in Section 5. Section 6 provides the detail of simulation results and its discussion. Section 7 provides conclusion and future work whereas section 8 represents References.

3. RELATED WORK
Legitimate Chance Inspection Algorithm (LCIA) [5] is a new mitigation technique based on hop count inspection across legitimate identification. Stephen M. Specht et.al. [1] had proposed taxonomies of DDoS attacks, tools, and countermeasures to assist span the DDoS trouble, also to facilitate more comprehensive solutions. Simpson S. Lindsay et.al. [2] had proposed a plan to mitigate bandwidth-starvation DDoS attacks. D. Garg [3] had analyzed the attacks based on the severity, position of attacker and real time of attack. Yu. Chen et.al [4] had proposed that it is essential to minimize the illegitimate traffic at the time of filtering DDoS attack flows. DDoS defense systems may coincidentally reject a sure portion, of legitimate users’ access by mistaking them as attackers. A. Challita et.al. [6] had proposed the packet funneling system to moderate the effect of the attacker on the victim. In this approach, the congested traffic is funneled before sending to the destination. It continuously searches spoofed IP addresses and handles the DDoS attacks without blocking any legal packets. Debra L. Cook et.al. [7] had presented an architecture called as WebSoS, which allows legitimate users to access a web server in the presence of a DOS attack. They utilized various cryptographic mechanisms for authentication, packet filtering, overlay networks, and consistent hashing for providing service to authorized users trying to contact a web server under attack. G. Jin et.al. [8] had presented a simple and effective method called as hop-count-based filtering scheme, which detects and removes spoofed IP packets to make system Resources more secure. HCF can eliminate about 90% of spoofed traffic even though an attacker is aware of HCF. It can be easily implemented in the Linux kernel. R. Mahajan et.al. [9] had proposed a system for local and cooperative mechanisms. It resolves the attacks in the network for aggregate-based congestion control. This system is useful in controlling DDoS attacks and Flash crowds. J. Ioannidis et.al. [10] had proposed a mechanism that treats DDoS attacks as the problem of congestion control, and actions by identifying and intentionally dropping traffic aggregates responsible for such congestion. Jelena Mirković et.al. [11] had proposed the D-WARD that offers an effective defense against distributed denial-of-service attacks. By applying that defense at the point where DDoS traffic enters the network, D-WARD is able to spread the deployment cost among many systems and remove the useless load of DDoS traffic from the Internet as a whole. In a few seconds, D-WARD can detect many common forms of DDoS attacks, and can dramatically reduce their effect almost immediately. More sophisticated attacks, such as those that slowly increase their sending rates, take longer to detect, but D-WARD controls them almost as soon as they have sufficient volume to affect the victim. At the same time, legitimate flows from the source network proceed unharmed. A. Yaar et.al. [12] had proposed an approach to defend against DDoS attacks called as Pi. It is related with marking paths from the elements of IP trace back systems, which can be used to filter each incoming packet. A. Yaar et.al. [13] had presented a new method to mark and filter the packet in the Pi defense scheme, called a StackPi. It is a stack based method that permits a DDoS sufferer to select the optimal threshold value for the Pi filter. Also they proposed a system in which IP data of each packet, making it far less likely that an attacker will successfully bypass the filter. Yu Chen et.al. [14] had introduced a scheme to identify malicious flow and cutoff called MAFIC. They used adaptive packet dropping and probing algorithm. Malicious attacks are exactly identified by observing the reply to packet loss from the flow source and all those packets are dropped before reaching the victim.

4. LEGITIMATE CHANCE INSPECTION ALGORITHM
Legitimate Chance Inspection Algorithm (LCIA) is a new mitigation technique based on hop count inspection across legitimate identification. This scheme is extended from the hop count inspection. Legitimate chance inspection is analytical approaches based on the mathematical equation which will be used to find the number of packets being malicious under legitimate data packets. This algorithm will be used to mitigate the malicious packets which are coming along the legitimate data and improve the efficiency of the network performance. LCIA identifies the legitimate packets from the malicious attack packets. The flow table will be maintained for malicious and suspicious packets. After filtering malicious and suspicious packets from the flow table, it can effectively identify the legitimate clients. The first step in Legitimate Chance Inspection for Identifying Legitimate Clients under DDoS Attacks is attack and victim system identification. The first challenge in solving the DDoS attack problem is to determine if there is any DDoS victim being attacked by the traffic passing through the router. When a victim is in under attack, it needs to determine how much of traffic volume flow to the target victim should be classified as suspicious. After finding the suspicious attacks, it will be maintained in suspicious flow table. Second step is legitimate and attack traffic classification. Once the attack traffic is classified, defense actions should be automatically taken place to mitigate the impact of the attack. By discarding the attack packets using the flow tables, this not only prevents the bad packets from reaching the target victim but also automatically reduce the workload of routers that forward them and avoid.
Figure 1 shows the scheme of the Legitimate Chance inspection Algorithm. LCIA algorithm maintains the malicious flow table and suspicious flow table for maintaining malicious and suspicious attacks respectively. Incoming packets will be received and checked with the flow tables and legitimate clients are identified. The LCIA algorithm mitigates DDoS attacks by identifying the legitimate packets from the malicious attack packets. In this algorithm, time constraints values are generated for frequently refreshing the white list instead of a user. So, it effectively maintains white list of legitimate clients. In LCIA algorithm, all incoming traffic is maintained in the common IP table. Through this table packets will be generated and sent to the victim server. Packet information status can be known through the detection analysis. In malicious flow table (MFT), all continuous IP addresses will be monitored and stored into that table. Using traffic normalization rule, the unwanted packets from this table should be dropped immediately. Suspicious flow table (SFT) consists of all doubtful packets from the incoming traffic. Client puzzle algorithm will be used to remove all suspicious packets from the SFT. After filter malicious packets, routers find any suspicious packets that should be stored in a suspicious flow table. White list contained all illegitimate client IP addresses. It should be refreshed frequently with particular time intervals. Legitimate Chance Inspection Algorithm (LCIA) used to generate the time intervals for refreshing the white list. Instead of refreshing a user, this algorithm will refresh the entire white list frequently. So, the attacker cannot spoof the legitimate clients IP addresses. White list can effectively maintain the legitimate clients.

5. PROPOSED WORK
In network once an attack victim is discovered, it is important to carry out defense mechanisms to allow the victim host to be accessible for legitimate user. The LCIA algorithm presents a problem of how to differentiate attack traffic from the legitimate traffic efficiently and accurately to reduce the malicious attack damages. The algorithm is as follows

Step 1: Initialize incoming traffic count.
Step 2: For each incoming traffic, maintain common IP tables.
Step 3: Generate packets from the IP tables.
Step 4: For each value of packet count = 1 to n

Extract malicious flow table and suspicious flow table for each packet

- If (IP! = spoofed)
  - Then
    - ‘Allow the packet’
  - Else
    - ‘Discard the packet’

Step 5: compute probability for SFT packets

- If (IP == spoofed)
  - Then
    - ‘Discard the packets’
  - Else
    - ‘Allow the packets’

Step 6: repeat steps 4 & 5 until packet
6. SIMULATION RESULTS AND DISCUSSION

LCIA algorithm is implemented on NS-2 to evaluate the performance of the algorithm. The proposed work has multiple advantages. The efficient network mainly concerns with the reliable data transfer from source to destination with minimum cost, less packet loss and network load as well. The performance of Normal packet transfer and the transfer with LCIA algorithm protocols are compared based on the performance metrics. The following parameters are evaluated against number of transfers.

**Cost:** Number of nodes utilized, power consumed and packet loss.

**End to End delay:** Difference between the packet receiving and packet sending time.

**Packets drop:** when the data travel from source to destination there is possibility that packets may lost in transit due to network performance parameter.

**Network Load:** The total traffic (bits/sec) sent by the MAC to the network layer is accepted and queued for transmission.

The simulation of 40 nodes has been prepared using Network Simulator 2.34 of size 1000 m x 1000 m area. The performance parameters such as cost, end to end delay and Network Load are evaluated against number of transfers for both normal and LCIA protocols. The red colour curve represents the Normal traffic flow whereas the green colour curve represents the implemented LCIA protocol. The Simulation Parameters are given below.

### Table 1 – Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS2.34</td>
</tr>
<tr>
<td>Simulator Time</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>20, 40, 60</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>500 x 500</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Traffic</td>
<td>CBR (UDP)</td>
</tr>
<tr>
<td>Channel Capacity</td>
<td>1 M Bits/sec</td>
</tr>
<tr>
<td>MAC Layer Protocol</td>
<td>IEEE802.11</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>1.5 Meters</td>
</tr>
<tr>
<td>Maximal speed</td>
<td>100 m/s</td>
</tr>
</tbody>
</table>

Figure 2 shows the IP Table generated as an output, which represents the IP addresses of the nodes created in the simulation. The NS2 simulator creates total 40 nodes to simulate the packet transmission using LCIA algorithm.

![Figure 2: IP Table created in NS2](image-url)
Figure 3 shows the data transfer between source and destination node including the intermediate path. It also shows the throughput in terms of cost with the minimum distance and delay time.

In Figure 4 Data transfer is plotted against the cost. In the graph only three data transfers are considered. It is observed that cost required in a legitimate chance inspection algorithm is very less as compared with normal traffic flow. It shows that when the DDoS packets rate is increased, legitimate chance inspection scheme has better average throughput of normal packets than the other two schemes. So, the Legitimate Chance Inspection scheme can effectively reduce the traffic of malicious users.

Figure 5 shows that the Packet loss using LCIA algorithm (Green Color) is less than normal traffic flow (Red Color).
Figure 6 shows the reduction in the network load after implementing the LCIA algorithm. Red curve represents the normal traffic flow and the green curve represents the LCIA algorithm.

![Network Load Graph](image)

**Figure 6**: Network Load using normal traffic flow (Red Color) and using LCIA algorithm (Green Color).

Figure 7 shows the graph of delay for the packet transmission using LCIA algorithm (Green color) which is reduced as compared to the normal traffic flow (Red color).

![Transmission Delay Graph](image)

**Figure 7**: Transmission delay by using normal traffic flow (Red Color) and using LCIA algorithm (Green Color).

Figure 8 shows the network simulation of the data transfer from the source node to the destination node by refreshing the IP addresses of the nodes with the specific time interval.

![Network Simulation](image)

**Figure 8**: NAM file of Network Simulator (NS2)
7. CONCLUSION
Distributed Denial of Service (DDoS) attack is one of the foremost damaging threats faced by most of the web applications. In DDoS attacks, attackers affect the normal users to achieve the bandwidth-consumption attack. This attack includes IP spoofing, smurf and fraggle attacks and resource starvation attacks include SYN floods. To minimize the effect of an ongoing attack, mitigation process is used. The basic problem with network is to distinguish between legitimate and illegitimate client packets. In the Project i.e. Implementation of Legitimate Chance Inspection for Identifying Legitimate Clients under DDOS attacks removes the possibility of IP spoofing, smurf and fraggle attacks and resource starvation attacks include SYN floods. The result of LCIA help to achieve the network with maximum throughput, low cost, less delay, low packet loss and network load.

REFERENCES