A Proactive Approach towards DDoS Management in Shortest Path Bridging

Mensah Sitti
Anna University,
Department of Computer Science and Engineering
Chennai, India

Gideon Naah
University of Electronic Science and Technology of China
Dept. of Electronic Engineering
Chengdu, China

Daniel Owusu-Donkor
Anna University
Dept. of Electronic and Communication Engineering
Chennai, India

ABSTRACT
Changes in technology have affected a large number of sections in the domain of Ethernet. Cloud computing has provided a new dimension for virtual networks (VLAN) as well. These changes have help shaped the paradigm of computer networks on the whole and continues to be the back bone of linking various datacenters. With the introduction of shortest path bridging (approved by IEEE as 802.1aq) computer networks will experience a more refined way of getting things done in a very excellent way. Distributed Denial of Service (DDoS) on the other hand has affected computer systems and networks to a large degree, although solutions have been provided to contain the situation. Attackers typically exploit well-known vulnerabilities, many of which have readily available fixes. Complicating matters are the intrusion tools that are widely available. Intruders have automated the processes for discovering vulnerable sites, compromising them, installing daemons, and concealing the intrusion. Even security-conscious sites can suffer a denial of service because attackers can control other, more vulnerable computer systems and use them against the more secure site. The use of shortest path bridging to manage DDoS attack is not only to help contain the situation but to also provide a way out and render the attacker helpless. This paper suggests ways that can be used by a victim computer to counter a DDoS attack from a possible attacker or an unintentional attack. It helps to safeguard the user against unwarranted service which might command a computer to do without necessarily being aware. The simulation was conducted on a Linux operating system using ns3 and result obtained gives a promising future to pursue further work on the use of IEEE 802.1aq Shortest Path Bridging in managing Distributed Denial of service (DDoS).

Keywords
Shortest Path Bridging; DDoS Attack; Security-Conscious; VLAN; Ethernet; Intruders; STP

1. INTRODUCTION
The need to get dependable and proficient source of information in today's global village is becoming imperatively inevitable. Especially at a time when organizations want to get reasonable gain over other firms in business. Days of the traditional way of doing business and filing different forms of documents in file cabinets are gradually becoming a thing of the past. All these way have been converted in electronic sources where users can easily replicate thousands of copies and distribute to all stakeholders. More importantly, with the emergence of cloud and online working documents, students, worker and associates can seamlessly see what other colleagues are doing on a particular document at a time, irrespective of the distance involved. Simple switched Ethernet networks, while a great improvement over repeater-based Ethernet, suffer from single points of failure, attacks that trick switches or hosts into sending data to a machine even if it is not intended for it, scalability and security issues with regard to broadcast radiation and multicast traffic, and bandwidth choke points where a lot of traffic is forced down a single link [1]. Advanced networking features in switches and routers combat these issues through means including spanning-tree protocol to maintain the active links of the network as a tree while allowing physical loops for redundancy, port security and protection features such as MAC lock down and broadcast radiation filtering, virtual LANs to keep different classes of users separate while using the same physical infrastructure, multilayer switching to route between different classes and link aggregation to add bandwidth to overloaded links and to provide some measure of redundancy[1].

IEEE 802.1aq Shortest Path Bridging (SPB) includes the use of the link-state routing protocol IS-IS to allow larger networks with shortest path routes between devices. [1]. It is intended to simplify the creation and configuration of networks, while enabling multipath routing. [2]. IEEE 802.1aq is the replacement for the older Spanning Tree Protocols (IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP) which permitted only a single path toward the root bridge and blocked any redundant paths which could result in a layer 2 loop. IEEE 802.1aq allows all paths to be active with multiple equal cost paths, provides much larger layer 2 topologies (up to 16 million compared to the 4096 VLANs limit) [3], faster convergence times, and improves the use of the mesh topologies through increased bandwidth and redundancy between all devices by allowing traffic to load share across all paths of a mesh network [4].

Denial-of-service (DoS) attacks have been launched against Internet sites for years. They are a significant problem because they can shut an organization off from the Internet and because there is no comprehensive solutionfor protecting your site or recovering from a 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, an administrator needs to make business decisions as well as technical decisions. Managing the risks posed by denials of service requires a multi-pronged approach such as:

- Design business for survivability. Have business continuity provisions in place[5].

- Design the network for survivability. Take steps that help to ensure that critical services continue in spite of attacks or failures[5].
- Be a good netizen (net citizen). User potential to be attacked depends on the security of other sites and vice versa.

The threat to a user network is directly proportional to the extent that other Internet users, including home users, adhere to good practices. Conversely, the threat that a user network represents to others is directly proportional to the extent that user's organization adheres to good practices [5].

Denial of service may be indistinguishable from a heavy (but otherwise legitimate) load on your network. For example, a user might be flooded with legitimate connections to a web site as a result of a major news event such as the disaster that occurred on September 11, 2001. Users might have difficultly connecting to a web site simply because so many people are trying to connect at one time and not because the user is the target of a denial-of-service attack. It is important to establish criteria by which a user will declare a site "under attack" and invoke emergency procedures. Mitigation strategies for attacks and heavy, legitimate traffic may be similar [6].

The rest of this paper is organized into five (5) sections with the current section been the introduction, introducing SPB and DDoS. It also provides a short summary of Ethernet and a little background. Section 2 describes the related work from other researchers and their work in this field. Section 3 presents the proposed model and it operation. Section 4 describes the experimental simulation and results analysis. The last but not the least, section 5, discusses the conclusion of our work and future work to possibly stop DDoS Attack.

2. RELATED WORK

The report concerns the multi-homing of networks, seamlessly switching between available connectivity, network code packets, load balancing across available paths for such multi homed networks/ provider network and a way of preventing a denial of service. These areas are each, individually, rather long-standing topics. However, this project is attempting to combine them into a single service. Multi-homing has typically been used for redundancy; thus, if a specific path fails, traffic can be switched over to any existing backup paths. The redundancy approach has a long operational history. Protocols such as virtual router redundancy protocol (VRRP) [2] can be used to provide near-immediate switchovers in case of equipment or link failures when all of the network elements are managed by a single entity.

Most prior research on multi-path algorithms, such as that by Leung and Li [7], assumes that the information available to algorithms on network conditions is always accurate. However, connections with continuously changing characteristics, such as mobile networks, are constantly increasing in popularity, and thus the information is becoming harder to attain. Our work is also related to seamless mobility [8], where multiple approaches exist for conducting vertical mobility between different access technologies and networks. Most of the existing work is limited to utilizing single path – multiple paths may be concurrently used for short periods to facilitate handovers, but most of the time only a single path is used. Notable extensions include, for example, multi-hop multipath heterogeneous connectivity (MMHC) work [9], which attempts to provide seamless multi-path routing on a per-application basis. Studies have been previously conducted on the RAIIC concept using Mobile IP as a signaling protocol via simulation [10] and real-world implementation [11]. Thus far, the signaling has proven quite promising from an end-user perspective. For interactive applications such as web browsing, performing a handover to the alternate physical connection is practically transparent. In real-time applications, such as VoIP, the effect is noticeable but tolerable. The pause is in the sub-second range, and it is been assumed that outages do not occur frequently enough that repetitive, short outages would become an annoyance. As such, it has been concluded that signaling can be conducted with satisfactory performance.

To cope with DDoS attacks intrusion, many researchers have proposed novel methods for attack detection and identification. G. No in [12] proposed a fast entropy computation method with adaptive threshold updater by moving average window in early phase of the attack.

Y. Shi in [13] proposed a linear variation method of inertia weight to greatly improve the optimizing ability and convergence speed of algorithm. P. Yu in [14] proposed a novel improved Renyi entropy method to detect attacks with sensitive entropy value changing. When DDoS attacks occur, it will lead to network flows surging over the servers in a short period, entropy values simultaneously increase rapidly. Based on the advantages of above literature methods, we design an integrated and novel approach for DDoS attack management in IEEE 802.1aq-Shortest Path Bridging.

3. PROPOSED SYSTEM

3.1 Block Diagram

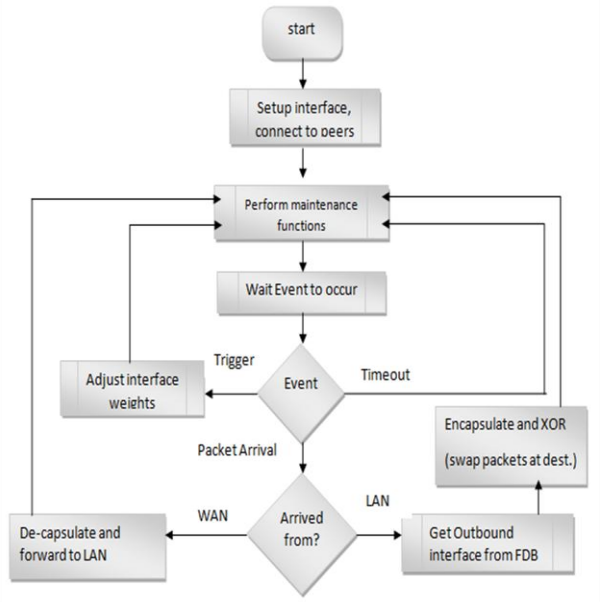

Fig1. Block Diagram

This algorithm is based on the work in [14]. The original idea was to divide the number of detected flows by the weight of the interface, aiming for maximum fairness while keeping each flow on a single path. This work has now been extended in an attempt to not treat all flows as being equal, since in some cases the flow might be limited due to throttling at the source, as well as for other reasons. The router maintains a weighted moving average of bandwidth utilization on each outbound interface and the number of flows traversing each interface. Information on each flow is maintained as well. The data structure containing the flow information is a 256-entry hash table, with each entry containing a linked list of flows. The hash is a modulo of all five attributes of an IP packet.

$$P = \left(\sum_{i=1}^{m} (Ai \bmod n)\right) \bmod n, \text{where P is the path index} \quad (1)$$

In addition to the identifying information, the number of bytes transmitted is stored for each flow. The algorithm splits the flows into categories. Flows that are considered ‘‘normal’’ attempt to utilize all available bandwidth in accordance with congestion-control mechanisms. Flows in the second category are called ‘‘underflows’’ – they transmit less data than what they are capable of transmitting. Typical examples of underflows are TCP packets consisting solely of acknowledgments.

If a flow is fluctuating rapidly, for example, due to being in the slow-start phase, it will be categorized as a normal flow as a precaution. The difference between normal flows and underflows is that normal flows yield bandwidth according to congestion control rules; underflows are already below their fair share, and, thus, they will not yield bandwidth.

When the router requests an interface for an outbound packet, a lookup is performed based on the tuple. If an entry is found, the entry will contain the appropriate interface to use. If no entry is found, one is created. The flow is initially allocated to the interface with the largest potential bandwidth meaning the interface where the flow would reach maximum throughput if it behaves like a normal flow.

$$Pbw_{iface} = \frac{\left(bw_{iface} - \sum_{i=1}^{nUnderFlows} flowbw_i\right)}{nNormalFlows} \quad (2)$$

3.2 Maintenance Function

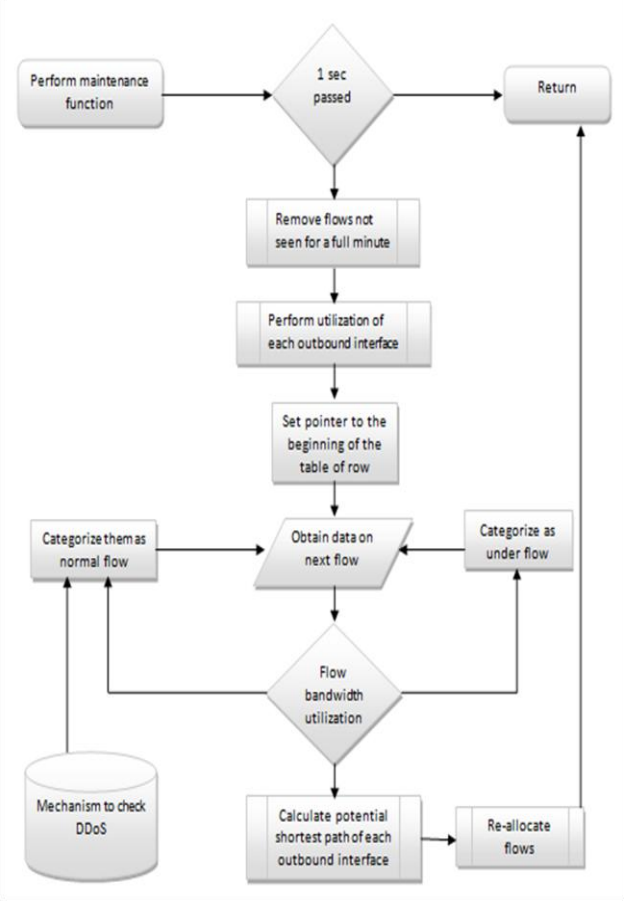

Fig 2. Maintenance Function

1. All flows are checked for whether they have activity. If not even a single packet has been seen for one full minute, the flow is removed from the table.

2. The bandwidth utilization of each interface, as well as number of flows traversing that interface, are calculated.

3. For each flow, the flow is assigned to a category as follows:

- If the flow’s bandwidth utilization during the last second is more than 70% of the average for all flows on the same interface, consider the flow a normal flow.
- If the flow’s bandwidth utilization for the final 3 s has a difference of greater than 10% from the previous 3 s, consider the flow fluctuating and categorize it as normal flow.
- Otherwise, categorize the flow as underflow – a stabilized flow with below average traffic utilization.

4. Based on the data, the potential bandwidth is calculated for each interface. The potential bandwidth is the bandwidth that a newly formed flow will get if it utilizes all of the available bandwidth and behaves according to the TCP’s congestion-control mechanisms. The potential bandwidth is calculated as the interface’s bandwidth reduced by the combined bandwidth of the underflows, divided by the number of normal flows, as in formula (2).

5. A check is conducted on whether or not any of the current flows should be re-allocated to a different interface to achieve better overall fairness. The interfaces with the minimum and maximum calculated potential bandwidths are checked as such:

(a) If the difference between the minimum and maximum potential bandwidth is less than 3%, no further checks need to be made – the situation is considered fair and the process is stopped. This threshold prevents flows flapping between several paths.

(b) If a moving a single normal flow from the interface with the minimum potential bandwidth to the one with the maximum potential bandwidth results in the roles simply being swapped, or if there are no flows to move, the process is stopped.

(c) If moving the flow causes the potential bandwidths to be more equal, but does not cause a position swap, a random normal flow is moved.

(d) Repeat the process until one of the conditions to stop further processing is fulfilled.

3.3 Computing Routes

To compute paths, we use two n by n matrices. The matrix distance[n][n] contains the distances between nodes in the simulation. For example, if distance[i][j] is 10, the weight of the path from i to j is equal to 10. Another matrix predecessor[n][n] contains the predecessor to node j on a shortest path from i to j. In other words, predecessor is the intermediate node. A predecessor matrix value is a 64-bit Bridge Identifier which is the concatenation of the bridge priority and the bridge system id. A bridge system id is numerical form of a MAC address of a node. The algorithm is provided below:

1: Initialize distance[n][n]

2: Initialize predecessor[n][n]

3: for k = 0 to n do

```
4:  for i = 0 to n do
5:   for j = 0 to n do
6:    if distance[i][j] > distance[i][k]+distance[k][j] then
7:       distance[i][j] = distance[i][k] + distance[k][j]
8:    else if distance[i][j]=distance[i][k]+distance[k][j] then
9:       Path1 = BuildPath from i to j
10:      Path2 = BuildPath from i to j passing through k
11:      if Path2 has higher priority then
12:       predecessor[i][j] = predecessor[k][j]
13:      end if
14:   else
15:      Do nothing
16:    end if
17:   end for
18: end for
```

Lines number 9 and 10 both create path from i to j. A Path is a list of 64-bit Bridge Identifiers. The difference between lines 9 and 10 is that line 10 creates the path passing through k. Line number 10 joins two paths, one is from i to k and another one is from k to j. If path i to k is on a shortest path and path k to j is, then path, i to j, is also on a shortest path. Computing a shortest path has optimal substructure. Thus, we guarantee that path i to j passing through k also on a shortest path. Line 11 compares two paths using ECT-Algorithm. There are 16 different ECT-Algorithm. The least significant 1 byte of an ECT-Algorithm is used to XOR on each path

Shortest Path Bridging (SPB) has the tie-breaking mechanism to prioritize the equal cost path. Each node advertises the costs of the attached links. These costs are presented in SPB Link Metric sub-TLV. The sum of the link costs on the path is equal to the cost of the path. If equal cost paths exist between two end points, the path with smaller hop counts has the priority. If there are more than two paths with the same link cost and hop counts, the default tie-breaking mechanism picks up the path traversing the intermediate node with the lower Bridge Identifier. Mesh network such as a data center may have multiple paths with the same link cost and the hope counts. This SPB tie-breaking mechanism guarantees diversity.

Line 11 compares two equal cost paths. A path with lower hop counts has the higher priority. Since a path is a list of bridge identifiers, the number of elements in the list is equal to the hop counts including the source and the destination. Thus, the smaller size of the list, the path, has the higher priority. If two paths have the same hop counts then, ECT-Algorithm value is XORed with the paths. The path with the smaller result has the higher priority.

3.4 Populating forwarding Database

Congruency between uncast and multicast, and symmetry between backward and forward paths makes populating a filtering database simple. We used the algorithm below to populate the node on a path. This algorithm takes a path, a SPB service identifier, and I-SID, as input:

```
1: n = total number of nodes in path
2: for i = 0 to n − 1 do
3:      for j = i + 1 to n do
4:      ForwardPath = Build Path from node[i] to [j]
5:           Install Unicast Entry for ForwardPath
6:           Install Multicast Entry for ForwardPath
7:      BackwardPath = Build Path from node[j] to [i]
8:           Install Unicast Entry for BackwardPath
9:           Install Multicast Entry for BackwardPath
10:     end for
11: end for
```

4. EXPERIMENTAL SIMULATION AND RESULTS

The simulation used a number of scenarios to generate the results that must be expected at the end of the experiment. To help better understand the packets being transferred from one node to another node, TCP and UDP were used to test if the model with work with both wired and wireless networks. The shortest path bridging does segments the network as mention earlier and makes it possible to be able to eliminate nodes that have choke bandwidth and are like to cause problems in the network to require administrative assistance.

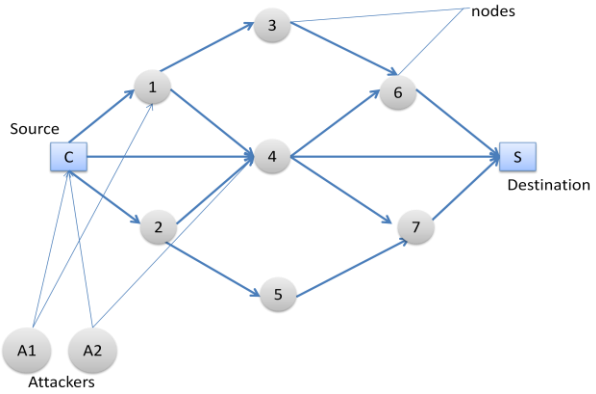

Fig 3. Experimental Topology

4.1 Results and Analysis

Fig 4 shows illegitimate users populating the congestion window of the server with legitimate users trying to equally gain access to the server. In such an instance it is consider DDoS attack as the legitimate users are denied access to the server or they need to compete with other illegitimate users to access the server.

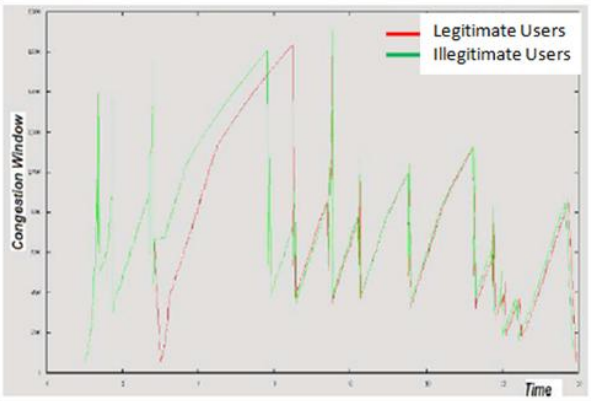

Fig 4. DDoS traffic flow

Fig 5 represents the congestion window plotted against time graph showing the managed attack of DDoS on a network using SPB. The upsurge from the very beginning shows a possible attack from illegitimate users in the inside of the network or from outside the network. Once it is detected of a possible attack the SPB mechanism investigate packets and distribute packets to the various I-SID or VID. Packets that do not have any tag of either the two will be discarded and the network is brought under control again.

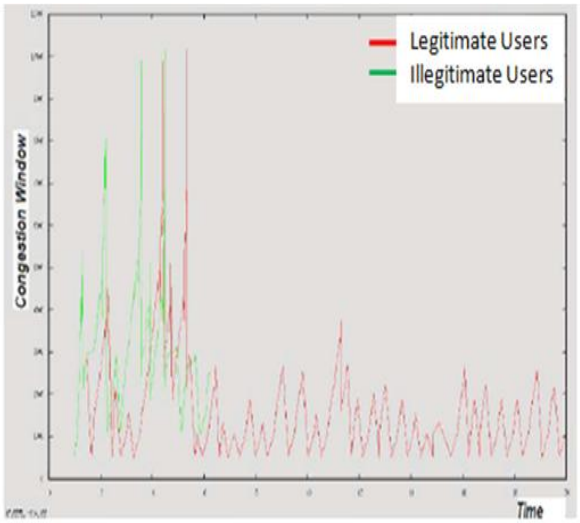

Fig 5. Improved Traffic flow with SPB

Fig 6 Shows the resources that are used when the network is under DDoS attack and when is under SPB management. The network is made to use more resources when under DDoS attack. The network is completely locked by activities of zombies which make the network seem very busy but is in effect servicing illegitimate users. When SPB is applied on the network the number of resource used are reduce whiles serving legitimate users on the network.

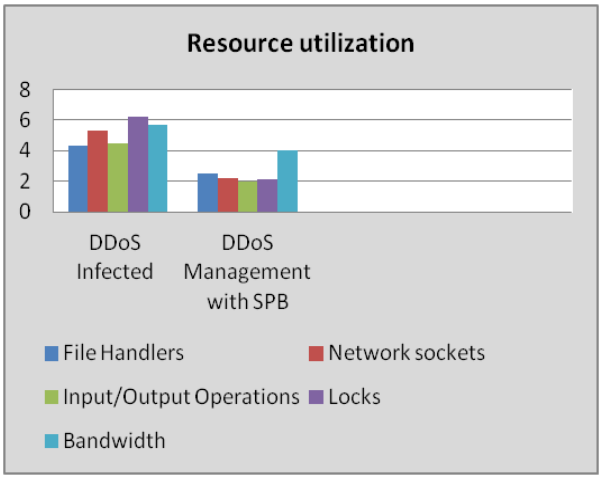

Fig 6. Resource Utilization

5. CONCLUSION AND FUTURE WORK

Shortest Path bridging as has been studied has provided a significant level of connectivity among data centers and virtualized environment. It features makes it easily adaptable with already existing features of Ethernet. The spanning tree protocol although has helped Ethernet and switched networks has not been that efficient and effective as it should be with denial of service attack.

However through the introduction of SPBusing its VID and MAC-in-MAC on a network and will careful monitoring through the experiment carried out we can say Denial of service attacks can be reduce by a significant margin and help systems communicating with each other have a good flow of packets and good access to webpages and systems connect to such domains. Flows that are deemed to have lasted their time are re-examined and discarded if necessary and/or otherwise queued to resend. Illegitimate users are gradually identified and their packets or frames are not allow to continually flood the network to allow legitimate users the bandwidth and have easily flow of packets on the network.

The promising features of SPB makes it a reckoning factor in preventing Distributed Denial of Service (DDoS) attack as it tends to only work with known or identified systems or users. Since SPB also preserves the features of Ethernet and its OAM, it will be very interesting to continue to study how it can be implemented on devices being currently manufactured. This will help to reduce attack, not only the software level but the hardware level as well to bring sanity to many networks in future.

6. REFERENCES

[1] http://en.wikipedia.org/wiki/Ethernet.

[2] Zhen, L. and Changjin, S., 2011"An improved shortest path bridging protocol for Ethernet backbone network", International Conference on Information Networking (ICOIN).

[3] http://standards.ieee.org/news/2012/802.1aq.html.

[4] Ashwood-Smith,P. 2011. Shortest Path Bridging IEEE 802.1aq Overview.

[5] https://resources.sei.cmu.edu/asset_files/WhitePaper/2001_019_001_52488.pdf

[6] Saman, T. Z., Joshi, J., Tipper D., 2013."A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks" 15 (4). IEEE Communications Surveys & Tutorials.

[7] Breyer, R. and Riley,S. 1999.Switched, Fast, and Gigabit Ethernet. Macmillan,

[8] Metcalfe, R. and Boggs, D. 1976. "Ethernet: Distributed Packet Switching for Local Computer Networks", Communications of the ACM 19(7).

[9] IEEE Standard, 2004. 802.1D IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE.

[10] Allan,D., Nigel. B., 2012. "802.1aq Shortest Path Bridging Design and Evolution," IEEE Press.

[11] Allan,D., Nigel. B., 2012"Why the SPB Control Plane Looks as it does," in 802.1aq Shortest Path Bridging: Design and Evolution the Architect's Perspective, New York, IEEE Press.

[12] No, G., Ra,I.,2011. Adaptive DDoS Detector Design Using Fast Entropy Computation Method in 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (ICIMISUC).

[13] Shi, Y., Eberhart,R. 1999. Empirical study of Particle swarm optimization in proc. of IEEE International Conference on Evolutionary Computation (ICEC).

[14] Yu, P., Li,Y. 2012. Adaptive DDoS detection approach based on improved Renyi entropy, Journal of Computational Information Systems.