An Acute Analysis And Advancement on SOS For Mitigating Intelligent DoS Attack

Basundhara Dey
Department of Computer Science
University Of Central Florida
Orlando, Florida
Dey.basundhara@knights.ucf.edu

***Abstract*— In recent years, Internet Service (IS) is resonating in different industrial fields, e.g. banking, power stations, mission critical applications, defensive system etc., wherever one sector needs to distantly control over another sector. With increasing reliance of each other, sudden absence or termination of connection directly hits on our regular life. Here Denial of Services attack (DoS), driven by one or more multiple hosts in a way more harmonized manner has proven as a rapidly viable threat in today's internet. Secure Overlay Services (SOS) acts as a premise to protect the time critical network disruption caused by Dos attack.**

Although the architecture is promising in countering simple congestion based attacks, it is still dubious that if the architecture is really volatile to the intelligent Distributed Denial of Service Attack (DDoS) attack which aim to enact SOS to launch more vulnerability. So our intent in this paper to gauge the prospect of successful DDoS attack against a SOS protected network. This includes peer review of different intelligent attacks possible on SOS architecture and through that understanding more detail attacker's strategy. It also encompass few schemes for enhancing SOS against the intelligent DDoS attack.

Keywords—DDoS, SOS, Network, intelligent attacker, Active network Technology, Fosel, Simulation

I. INTRODUCTION

Over the decades, Distributed Denial of service attack prolongs to unfold as most system menace. For many communication reliable systems over the internet, prevention to disrupt communication from malicious users inside and outside of the system is the utmost priority. Recent level of composure to DDoS attacks in Internet service pliancy is far from explicit. Moreover, most of the explications towards indicating, defining and then blocking the vicious packets are not superficial for time critical and emergency applications.

Secure Overlay Service (SOS) architecture is the first covenant that acts as a basis of all overlay based framework with a set of system deployed peers serve as compromising transmitters from clients to server during critical situations and provide attack defensive features to the overall network. It gives higher extent of secure path availability during random DDoS attacks. The design rationale is to ensure that in the presence of DDoS attacks, the target is not overloaded; the probability of all available paths between clients and the target being compromised is very small; and the attack traffic is dropped [1].

The SOS design uses 3 layers of overlay nodes between the source and the target in order that it solely receives the legitimate traffic even without system recovery under on-going attacks. The layers are SOAP (secure Overlay Access Point), Beacons, and Secret Servlets. SOAP receives traffic to do verification on it. An appropriate Beacon, chosen by the hash function, accepts the traffic from a SOAP through chord routing, destined for a particular target. Secret Servlets are the only entry point to the target

through a well filtered region. Only bacons know the identity of the Secret Servlets for the target.

Considering the proactive architecture, the system ensures, 1) that the server and the middleware communication flow is concealed from any intruder, 2) existence of alternative route for better reliability, and 3) prevent unauthorized users by access control. The main objective of SOS is to ensure that during high intensive communication traffic using random congestion-based DDoS attacks, provides high degree secure path availability.

While the system provide good performance in the above scenario, by critical analysis the following catechisms are naturally arise:

- System can be out braked by intelligent attackers. This means that the attacker can bombard a huge amount of congestion-based DDoS attacks with a prior knowledge of system peers. Breaking into a node and revealing its close by nodes in the communication string, is known as break-in attacks. Coupling break-in attack with congestion-attack, attacker can exacerbate damage. Under intense break-in attacks, attacker can exploit the list of disclosed nodes to forward subsequent congestion attack and thus gradually can disclose the server and revoke the complete system. So what is the impact of this combined attack on SOS?
- The architecture compose of three key design features: number of layers, number of neighbors per node and the node distribution per layer [1]. So how this layering, mapping degree and node distribution [2] effect the system conduct. Moreover, what is the impact of this architectural design on intelligent DDoS attack?

This paper's objective is to observe the impact of the above issues. To do so, this paper includes 1) Generalization of the SOS architecture to a flexible module and more secure to probable attacks. 2) Define DDoS attack modules and introduce some real time Intelligent DDoS attack models which gives severe threat to the architecture. 3) Discuss two probable module to enhance the generalized SOS architecture and results achieved by using those improvement techniques.

II. THE GENERALIZED SOS ARCHITECTURE

This sector will discuss about generalization of SoS of architecture.

A. The original SOS Architecture

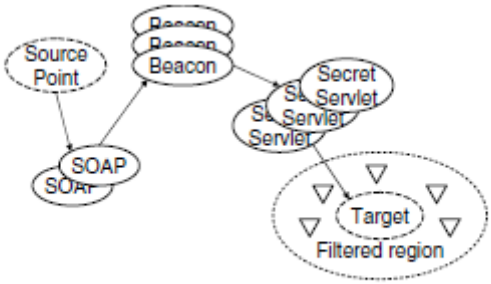

Figure 1. The original SOS architecture.

The above shown Figure 1[1] is the original SOS architecture. Here the communication flows between source and target through three intermediate layers. Source contact the SOAP (Secure overlay Access Point), SOAP transfer data to Beacon, Beacon knows the identity of Secret Servlet and pass the data to it and finally Secret Servlet forward the data packet to legitimate Target, following through some Filtered Region. This Filtered region surrounds the target as a firewall. Like the Beacon, only Secret servlets are aware of the filter identities. This forwarding system use Chording for more obscurity. The performance metric is the probability that a client can communicate successfully with the target by finding a path to it [1]. During random congestion-based DDoS attacks, attacked nodes become nonfunctional and thus compromise path availability, even in the presence of filtering.

B. The Generalized SOS Architecture

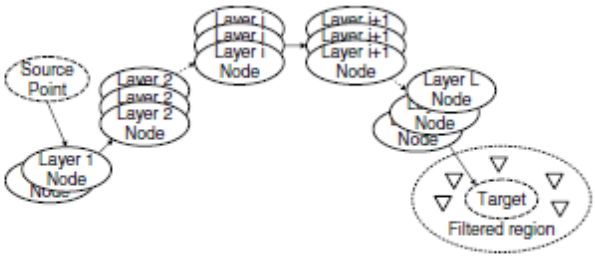

Figure 2. The generalized SOS architecture.

To improve the loopholes in above SOS architecture, here I introduce generalized SOS architecture, which is an extended form of the original one and consists a number of multiple layers of peers as shown in the Figure 2[1].

- Layering [2]: the more number of layers present, the more secure control over the data packets flow through nodes. The layering is denoted by L here. In a presence of numerous layers, target can be easily hidden from external intruders.
- Connectivity [2]: In a certain Layer, say i, each node forwards packets to the nodes to next Layer, which is i+1.Connectivity measures by the mapping degree of neighbors of each node, resides in the second forward layer. The bigger the mapping degree, higher the path availability.
- Node distribution [2]: The count of nodes present in each layer is referred. Though, for load balancing, uniform distribution of nodes across all layers is preferred. Technically, if more number of nodes are present in the layers near to Target, it will increase security in the whole network due to more ambiguity.

The advantages over normal SOS architecture are: A) Each node in a certain layer have knowledge of its neighbor nodes only in its acquaintance layer. B) Architecture is resilience as node and layer number can be designed keeping an eye on other factors, e.g. performance setback, insured delivery for special hosts/ targets.

III. DDoS Attack models

Over the decade, through numerous research on DDoS attack, analysts recognized different types of attacks on SOS and they categorized them as follow.

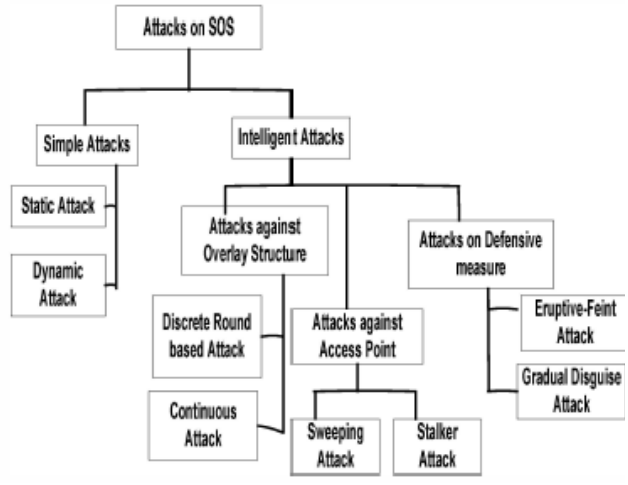

Figure 3. Classification of attacks on SOS [5]

A. Simple Attacks

Though we are not concern about Simple attacks here, for added knowledge I would like to briefly discuss about it. In Simple attack, with the prior knowledge of participating nodes in the Network, attacker congest them randomly with traffic, without being aware of nodes' role play. Now this can be classified into two categories:

- Static Attack [5]: When attacker targets for a fixed node set without considering the repairing action taken by the system. But when the node number is large, this attack fails due to the unavailability of plenty of attack resources.
- Dynamic Attack [5]: Like the static attack module, attacker targets a definite set of node initially. But while performing repair system during the attack, SOS either drop the attacked node or change data flow path through different nodes. To counter this recovery, attacker also alter its attack towards the new path. Henceforth, this random attack process can be classified into four different attack models, i.e.
  1. Centralized attack and Centralized repair[5]
  2. Distributed attack and Distributed repair[5]
  3. Centralized attack and Distributed repair[5]
  4. Distributed attack and Centralized repair[5]

B. Intelligent Attacks

It is already inferred that attacker can do extensive damage to the system with the prior knowledge of nodes in SOS architecture. Addition to this quality, an intelligent attacker also capable of breaking into next layer neighbors' node by gaining knowledge from already infected node. Intelligent attacks can further be categorized differently, depending on the way an attacker uses his knowledge to break into the security system.

- Attacks on Overlay Structure [5]: Two DDoS attack models are described below, considering the newly added features of generalized SOS architecture.

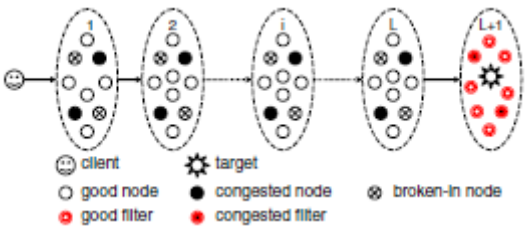

Figure 4. A snapshot of the generalized SOS architecture under the Intelligent DDoS attack [1]

- Break–in attacks: The attacker able to break into nodes successfully and easily disclose the next layer's neighbor nodes list. The break-in attack execution possibly happen because of any intrusion attacks, or by Trojan Horse or Active Worm attack, where some petty code can be hidden into a message sent by a virulent client. As soon as the victim will receive or open the message, the code will execute, node will be unfunctionl and neighbors' list will be disclosed. In worst scenario, the code itself will propagate it to the retrieved list.
- Congestion Attacks: The intruder can congest the victim node with known identities false traffic and thus the victim will discontinue to serve legitimate clients. Best examples of Congestion attacks are TCP SYN attack, TCP and UDP Flood attack, ICMP Echo attack and Smurf attack [2]. In result of this attacks, the targeted machine will be unable to connect to server any longer. Network link will be blocked and the connection and communication will be terminated.

This paper will mostly concentrate on theoretical analysis of the effect of Intelligent DDoS attacks on generalized SOS architecture. However, keeping an eye on these two attacks, the best policy an attacker can achieve is clubbing this two types. Breaking into nodes and get the neighbors' list and then congest all of them and terminate service. To do so, two different ways are there:

- Discrete Round based attack Model: For this attack model, attacker choose a limited number of nodes and perform the attack in a round by round way. In each round, attacker use only a part of his resources to do the break in attack. We can call this attack Discrete [2] because the attacker waits to start next round only after successful completion of first round. Followed by Congestion attacks, which are conducted in a single round.

By analyzing the system performance in this attack, this paper conclude on how the improved architecture fractures of SOS and attack ferocity can affect this policy's success probability.

1. The more the intensity of attack increase, system's successful network probability decrease.
2. As the number of layers increase, the number of node per layer decrease. So during attack, it is easy to compromise nodes per layer by congestion, so the attack will be successful.
3. If the mapping degree in a system for any certain node is one to all, then the system attack success probability is almost zero.
4. Incretion of Node distribution degree directly impact the intruder's success.

- Continuous attack model: Unlike the previous one, break in attack is followed by congestion attack here. The difference from the previous model is, the break in attack happens on few nodes and identities reveled, congestion follow on them. Attacker will not wait for all nodes to be done in once as previous.

This paper also analyze and conclude some points as before mentioned for the previous model.

1. This attack is less conscious to layering and mapping degree, as system recovery can replace infected nodes as soon as the attacker moves to the next layer.
2. Increase layering will inversely decrease the system security, unlike the Round based model.
3. If the intensity of attack is small, the network hijacking with lower mapping degree start to perform better, especially when the system recovery process is comparatively poor.

I would also like to mention that SOS architecture also has some recovery mechanism to protect against malicious attacks, i.e. Proactive Repair [5], Reactive Repair [5]. Howbeit, depending on attack and networks layout, recovery ability also varies. Depending on the attacker speed, sometime system fails to conduct recovery, which results into disruption of communication for a certain amount of period. In contrary, if the attack speed is slow, the recovery will get enough time to restore back the systems performance.

IV. Intelligent DDoS Attack

Considering all the background knowledge on different types of intelligent attacks, now it's time to introduce the two most significant real time example of Intelligent DDoS attack.

A. Eruptive-Feint Attack

The attacker comes to know one of the crucial SOS architecture characteristic: if any infected node found in the network, the SOS architecture will simply drop the node. Using this recovery feature, attacker first send a bulk chunk of malicious packet to the nodes in a very crisp time span. Once sent, the traffic will return to normal phase. Because after sending at a time, attacker will stop and wait for the attacked nodes to be dropped. From the traffic recordings, we can find the undulated changes of attack packets for the several turns of this kind attack [3]. In the result, attacker is successful to drop too many number of nodes from the system, though the nodes didn't receive any continuous attack.

B. Gradual-Disguise Attack

The attacker use Gradual-changed vicious traffic to make the good nodes unaware of the growing malicious attack. Many of the nodes have the self-learning feature. The nodes compare their existing parameters with the latest received value in current period, then decide accordingly if they need to stay as it is or adapt them to new value. In this attack model, the intruder make the gradual change too hard to identify and adapt. The system would be overflowed with huge traffic and thus make it difficult for the nodes to change as per required; only normal changes will be done. Gradually, with long enough time, the malicious influx will have a good percentile of success over the natural traffic.

C. Attack and Defense in SOS

Sometime, attacker start his attack and follow the same steps in order to detect the target's location. It starts with choosing a pile of IP, preferably same geographical acquaintance nodes and send them malicious packets rigorously. During the course, analyze the response of legitimate traffic [3]. If from the response, the target can't be identified, simply change the group of nodes and start the process over.

V. Active Network Technology

Almost all detection system build some normal model, on basis of which they compare the system deviation. Keeping this in mind, the paper propose and defense technique using active network technology. To restrict the Eruptive-Feint Attack and Gradual-Disguise Attack, the paper describes a Partaking-based Self-reform Algorithm [3]. But before going into that detail, we must know some basic definitions.

A. Clustering

After collection all the information of the packets, one have to deal with a bulk of simple cluttered values. To abstract them into some specific group, we need to use clustering. It is a most important tool in data Mining process. Clustering problem is about partitioning a given data set into clusters such that the data points in a cluster are more similar to each other than points in different Clusters [3].

B. Proximity Measure

It a vector scale measurement that qualify the similarity of two data points. We need to make sure in most of the cases that in the time of computation, all the chosen features are contributed equally. Moreover, no any feature should dominate the other.

C. Malicious Clustter List

This type of clusters will be accounted mostly for this defense system. They have some particularity: A) the instance number in normal situation is small for this cluster, B) discontinuous appearance of instance, C) comparative to total traffic increment, cluster increment is higher.

D. Architecture

While under attack, the general SOS architecture can't send more information. To beaten this

shortcoming, we use the overlays to build a channel to let the IDs can shard their detection information [3]. This way it propose a new detection algorithm against the stated intelligent attacks. To do so, this algorithm introduced the active network component, named as Bulletin Board; which tends to store the available access types and routing information.

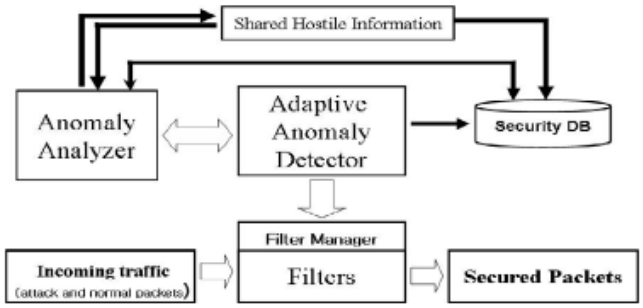

Figure 5. Detection Mechanism [3]

It was set within the same level because the Execution atmosphere within the Active spec, as a result of it's operate is self-ruled from the opposite active network part whose operate is predicated on the Execution atmosphere. Currently we wish to create full use of it to boost the protection.

1. Shared Hostile list is used to keep the shared data
2. Whenever a node find a DDoS attack, the list will be updated
3. Before drop itself, it pass on the information to the neighbor node to protect them.

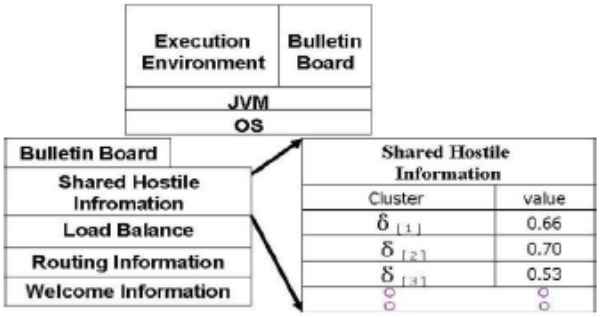

Figure 6. Bulletin Board [3]

Now the information that is shared between the dropped node and the good neighbor contains following: A) clustering criterion (lamda), B) Load balancing Info, C) Updated version of quittance nodes list.

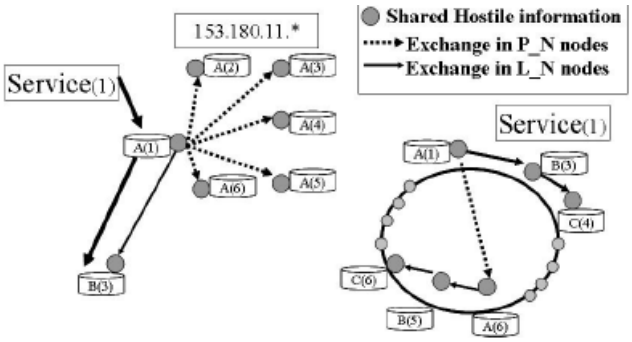

Figure 5. Broadcast of Bulletin Board [3]

As mentioned earlier, nodes are being choose in same geographical location. But the security information is not only limited to that, also transfers to local neighbors too as shown in Figure 5 [3].

VI. FOSEL ARCHITECTURE

Fosel is a proactive architecture that helps to guard destinations router with a well-filter to protect all the application sites from DoS attack. It can be executed if only the applications site already have given each other prior permission. Figure 8 presents a high level overview of this architecture.

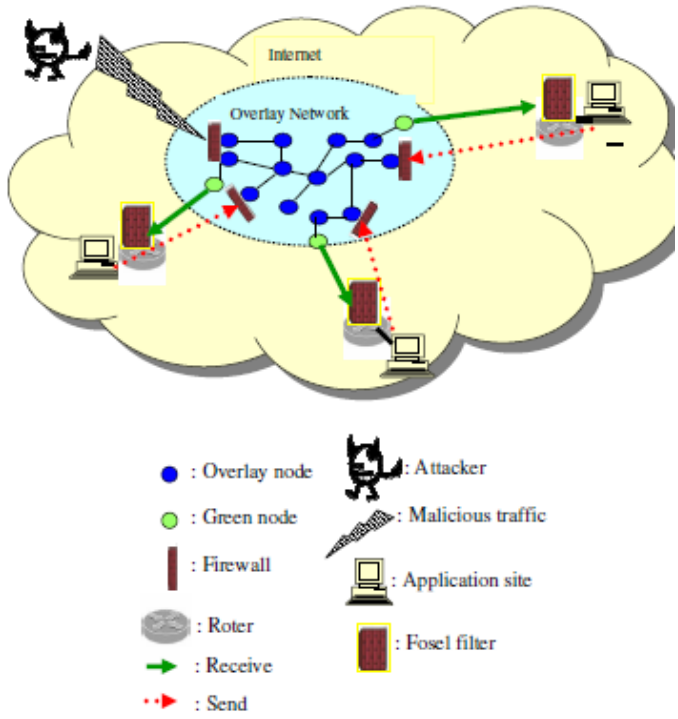

Figure 8. Fosel Architecture [4]

Before proceed to any further, we must know green node is a secret node of that overlay network.

Suppose A is a receiver site. The architecture works as follow in case of DoS attack against application site A:

1. A sends a data packet to its Green node, including the message that it is attacked by DoS.
2. A sender (application site) transmits its data to any random overlay node.
3. Using some authentication technique, that node verifies the message. If it is from an honest sender, it will be accepted, else dropped.
4. The node forward the data to the green node (secret node) of A.
5. The green nodes deliver C copies of message to the application site through Fosel Filter, which drops any malicious packet with P probability with any processing and process the rest [4].
6. By checking the source address of the remaining message, Fosel will get know if it's authentic (from green node) or not. I so accepted, else dropped.

VII. TECHNICAL OVERVIEW

Most of the research used simulator to analysis and evaluate the generalized SOS architecture, The Active network architecture, Fosel architecture. A brief summary I will present in this paper on the technical part of those:

1. A general analytical approach is used to evaluate SOS under discrete round-based attacks. Under high mathematical evaluation, [1] paper also introduce an algorithm of the successive attack strategy. To summarize the numerical part, larger value of layering and smaller vale of mapping degrees make the system break-in attack prone, while the reverse is always true for the congestion based attack.
2. For the Active network technology [3], the use OPNET modeler to simulate. The system performance has been evaluated by the terms of number of filtered attack packet. As an end result, the paper's contribution in technical term – A) clustering based detection algorithm, B) Introduce use of Bulletin Board. By simulation they get the performance result of their system quite higher than the normal SOS.
3. For Fosel, they simulate the system in two part: A) attacking the applications site, B) attacking the overlay network. Through simulation the result is showing that applying Fosel filter, system is performing between 10% and 50% faster than SOS architecture. The other best and significant part of this architecture is, to make sure delivery of legitimate packets, multiple copies of data is sent through network.

VIII. DISCUSSION

After all the study I made throughout the paper, I understand that simple SOS module is not enough for DoS attack protection. I observe that many schemes like system design features, different attack strategies, intrusion intensity, gaining knowledge beforehand about the secret securities in the system and recovery procedures and speed of recovery – all of them equally impact the SOS system performance while defending against Intelligent DDoS attack. By studying the new generalized module of SOS, I think –

A) Design features of the architecture should be more resilient. If a SOS architecture already defined, the layers and the mapping can't be change run time whereas the defected nodes can be replaced by new nodes. Why note design such a frame that can alter its layer or generate new layers runtime?

B) Path availability or mapping is constant if the layering increased and as a result number of nodes present in layers decrease. Introducing randomness in not just enough. To fool the attacker, I think we can introduce "Fake Image" routing concept through the network. Like, a same data packet with fake image can be transmitted over the network. This way we can confuse the intruder and meanwhile system recovery get more time to defuse the attack.

C) Observing the SOS architecture, Filtering region only locates near the Target. I think we can keep some more filtering option throughout the route. Just using secret servlet, Green node is not enough.

D) While talking about node disruption and dropping due to infection in the node, the intruder can easily get neighbors list from the node. I feel there should be some technique by which examining the dropped node, we can detect the attack pattern. So the way attacker gets to know secret nodes,

neighbor nodes and all hidden information of the system, we can follow the same and use it to identify the attacker introduction. Active network Topology has introduced clustering here. I feel this can help to do it.

E) The biggest issue that has not been taken care of is the timely delivery of the packet. Moreover, I feel Dynamic repair should be introduced in generalized SOS architecture.

IX. Conclusion

This paper gives an overview on an improved SOS architecture, how the loopholes of SOS architecture are easily vulnerable to Intelligent DDoS attack and some possible developed architecture to prevent them. In the technical part, the paper also give a brief summary of the technical preceding in the referenced papers. In the discussion, I introduces some of my opinion on how to improve the SOS architecture and some possible solution to that. Thus the future work should be concentrated on developing more robust architecture with the strategies and questions in mind.

Acknowledgment

I am sincerely thankful to Professor Mostafa Bassiouni for his able guidance and encouragement in understanding the base of this selected topic and successful timely completion.

References

[1] D. Xuan, S.Chellappan, X.Wang and S.Wang, "Analyzing the secure overlay services architecture under intelligent DDoS attacks," Disributed Computing Systems, 2004. Proceedings. 24th International Conference on.

[2] X.Wang, S.Chellappan, P.Boyer, and D. Xuan, member, IEEE, "On the effectiveness of secure overlay forwarding systems under intelligent distributed DoS attacks" Department of Computer Science and engineering, The Ohio state University, published online 25May 2006.

[3] C.In, C.S.Homg and J.Wei, and K.Okamura,"An enhanced SOS architecture for DDoS attack defense using active network technology", 2005IEEE.

[4] H.Beitollahi, G.Deconinck, K.U.Leuven, "FOSel: filtering by helping an overlay security layer to mitigate DoS attack".2008 IEEE Computer Society.

[5] R.kaur, A.lal Sangal, K. Kumar."Secure overlay services(SOS): a critical analysis".2012 IEEE.

[6] Blackert, W.J.; Gregg, etc, "Distributed denial of service defense attack tradeoff analysis".DARPA Information Survivability Conference and Exposition, 2003.

[7] C. Seon Hong, P. Yong park, W.Jiang, "DDoS attack defense architecture using statistical mechanism on active network environment"., Applied Cryptography and Network Security, June 2004.