ISSN No:-2456-2165

ESOBSTEB SIP- DDoS Defense Tool: An Aggressive Defense Framework for Detecting and Countering Flood based SIP-App (D)DoS Attacks on the Internet

[1]Madaki, S. D
[1]Computer Science Department, FCE(T) Asaba, Delta State, Nigeria

[2]Odachi Gabriel C
[4]Ezekwe Chinwe G
[2,4]Department of Computing sciences, Admiralty University of Nigeria, Ibusa, Delta State, Nigeria

[3]Joshua Joshua Tom
[3]Department of Cyber Security, Elizade University, Ilara Mokin, Nigeria.

Abstract:- ESOBSTEB SIP- DDoS defense tool is an internet attack based defense tool that has four components, the acronym "ESOBSTEB" came from the four components which are: enhanced SIP proxy server and an enhanced application layer stateless firewall, outer attack blocking (OB) component, service traceback architecture (STBA) and entropy based (EB) component. The increasing usage of SIP servers for multimedia transmissions has resulted in a high and frequent experience of Distributed Denial of Service (DDoS) attacks. The drive to curb the menace caused by Distributed denial of service (DDoS) attack which are threats resulting in huge damages on legitimate Internet usage and civil security in the last decade has been the objective of most network security researchers from academia, industry and also governmental organizations. This research study intend to fix this gap by first identifying and detecting the Flood based SIP-App (D)DoS attacks and create a defense mechanisms against them using the four components. The enhanced SIP proxy server updates the firewall with the IP addresses of legitimate users and alerts the firewall when a legitimate user IP address expires and should be removed from the list. The second component of the framework that will be deployed at the edge router compares and examines the IP source of the incoming request according to its blacklist database table and blocks or forwards it to the next part of the framework. The third part of the framework validates whether the incoming request is launched by a human (real web browser) or by an automated tool (bots) and it traces back the incoming request in order to find out the true IP attacking source. The forth part of the framework detects anomalies in SIP network traffic and to differentiate whether it is high rate DDoS (HR-DDoS) attacks or flash crowd (FC) attacks. In case EB classifies that the incoming SIP network traffic is high rate SIP DoS/DDoS (HR-DDoS) attacks, it blocks it immediately. Whereas if EB classifies that the incoming SIP network traffic is flash crowd (FC) attacks, it decreases the maximum connection's timeout value and decreases the maximum allowed request per this timeout, until these two values reach zero. Once the values of the timeout and the maximum allowed requests reach zero, EB component disables KeepAlive feature of SIP connection. The framework will be simulated with practical experiments of AntiDDoS_Shield system on NS2 simulation environment.

***Keywords*:-** *ESOBSTEB SIP- DDoS Defense Tool, Enhanced SIP Proxy Server, Outer Attack Blocking (OB) Component, Service Traceback Architecture (STBA) and Entropy based (EB) Component*

I. INTRODUCTION

The popularity and sensitive information transactions being processed on the internet have attracted the good, the bad and the ugly. However, the complexity and diversity of the attacks conducted on the internet have grown considerably. Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attacks are two of the most harmful threats to network functionality. These malicious attacks have caused tremendous loss by impairing the functionalities of the networks. With increase in dependency on web technologies, a commensurate increase has been noted in destructive attempts to disrupt the essential web technologies, hence leading to service failures. The increasing usage of SIP servers for multimedia transmissions has resulted in a high and frequent experience of Distributed Denial of Service (DDoS) attacks, with the ability to overwhelm a web server, thereby slowing it down and potentially taking it down completely. Some researchers also cite the need for a framework that will assist in the selection of the right training data set for analyzing the different type of attack irregularities expected in a DDoS attack (Chen et al, 2009; Modi et al, 2013).

ISSN No:-2456-2165

II. RELATED LITERATURES

Over the years there have been several detection and mitigation techniques proposed by researchers to counter VoIP DDoS attack. Some of them are Wavelet approach (Li and Li, 2009), which mainly detects DoS attacks, they do not scan signatures, although this approach, it depends on statistical traffic pattern before detection. It provides less efficiency in attack detection and also influenced on wavelet basis functions. Entropy based approach detects DoS/DDoS attacks; they do not scan signatures, are more efficient but are slow (Tritilanunt et al., 2010). Another major problem in Entropy method is that the attacking method is modified by the attacker by knowing the detection strategy. Sketch and Hellinger distance approach both detects and prevent DoS/DDoS attacks, using this method, the attack traffic is scanned for signature. This method is less efficient, slow and cannot accurately detect attack (Tang et al., 2012). Sunshine framework both detects and prevents DoS/DDoS attacks. It scan signatures; detection time is moderate and more efficient (Tang et al., 2012; Hoffstadt, et al., 2014). Recurrence Quantification based approach mainly both detects DoS/DDoS attacks but does not scan signatures. The attack detection and mitigation time is slow with less accuracy. Furthermore, this method involves more complicated framework (Jeyanthi et al., 2014). Evidently, the shortfalls in the different approaches to counter SIP-App-DDoS attacks still enable the attacks to grow rapidly, harder to detect and cause severe problems in accessing a particular on-line service.

SIP (Session Initiation Protocol) is an application layer protocol which creates, modifies and terminates sessions in VoIP communications (see figure 1). VoIP is a new generation international calling system with video and multimedia file accessing along with the voice calling (Sambath et al. 2016). In a typical SIP session, the SIP handles the session with initiation, call parameters etc. next the RTP (real time transport protocol) encodes the voice signal into digital voice data and sends it over the network using TCP, UDP or some other protocol that runs on top of IP. Making calls to a regular telephone requires a special gateway that connects the VoIP traffic to the regular phone network.

In DDoS attack, the various layers of the OSI model come to play, but special emphasis is to be laid upon the seventh layer, the application layer. The seventh layer that facilitates programs such as web browsers, email services, and photo applications in sending network communications, is a main target for DDoS attack because it is the protocols that directly service users (e.g., HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH etc.) and support protocols that underpin various system functions (e.g., DNS, SNMP, BOOTP/DHCP, TLS/SSL, SIP, RTP, NTP etc.). The security threats have not left SIP servers and VoIP environment.

In recent times, there have been reported DDoS attacks on end-users of computer systems. DDoS attacks are usually performed by a group of network of computers together to flood the servers of end users with huge amount of illegitimate packets request which the server cannot handle hence leading to denial of service. In a typical DoS attack scenario there are usually three parties - the attacker, the zombie and the victim. The attacker is the computer that issues commands to order the zombie which is a compromised computer to start the DoS attack. The zombie then starts the DoS attack by sending tremendous packets to the victim which is the computer that provides services to the users.

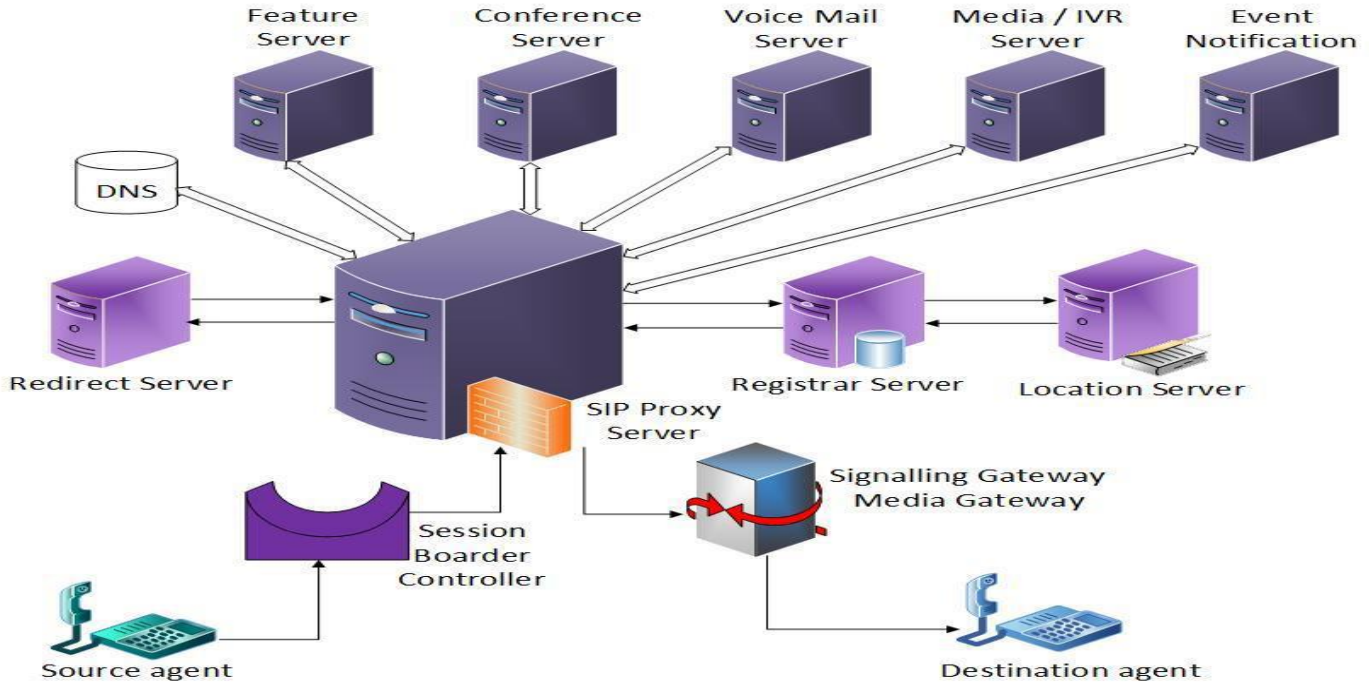

Fig 1 SIP Architecture for VoIP
(Source: Sambath et al. 2016)

Radware (2014) in 2011 claimed that application layer attacks are prevalent, for 46 % of cyber attacks were at the network while 56% were targeted at applications. Within the application layer attack, SIP was 2%, SMTP (9%), HTTPS (13%), HTTP (21%) and DNS (9%). In 2012, Prolex's annual report mentioned a 42.97 % growth in layer seven DdoS attacks. Later, quarterly reports by Prolex show a definite tendency of increasing popularity, particularly of SIP DDoS attacks in the period from April 2012 to June 2013.

III. PROBLEM DEFINITION

- The quest to counter SIP-App-DDos attack continues to look discouraging despite the enormous researches that have been undertaken, for there is no standardized frame work that will act as a yardstick for the design of an efficient SIP-App-Dos attack within acknowledged environmental factors.
- Some researchers use Intrusion Detection Approach that already gives a wrong description of the nature of SIP-App-DDos attacks, for this approach, does not enable all malformed messages to be discarded before they reach the destination. Some others use SNORT which cannot detect new anomalies.
- Using Entropy Detection Schemes has enabled attackers to identify the detection strategies.
- The volume-based techniques can only detect high volume traffic which can be from legitimate users, neglecting short-term DoS attacks. But huge volumetric traffic delivered by legitimate users to the server is undistinguished from higher traffic of bogus messages delivered by the attackers.
- Approaches using anomaly-based scheme provides only a small number of detection rules, such as detecting orphan RTP flow and verifying IP source address. To enhance the anomaly approach, there is need to have a framework that formulate rules for stateful detection on SIP.
- There is no specific framework that guide researchers into building systems within SNORT domain that uses the source SIP addresses to profile traffic thus detecting the flooding attacks and identifying the offending SIP messages efficiently.
- It is evident that existing techniques are insufficient in curbing SIP-App-DDos attacks. Presently, there exists no framework with the corpus parameters or metrics for defining the comprehensive nature of SIP-App-DDos attacks that will enhance detection.

IV. RESEARCH OBJECTIVES

- The framework will comprise of four subsequent component parts for Preventing, detecting and countering SIP DoS/DDoS Flooding attacks.
- The first component of the framework would consist of a security enhanced SIP proxy server and an enhanced application layer stateless firewall to maintain both the firewall and the SIP server the addresses of known (legitimate) users in order to give them priority handling.
- The second part of the framework will be an outer attack blocking (OB) component, which would be deployed at the edge router, since it is the most nearest point to the IP attacking source. It will first compare and examine the IP source of the incoming request according to its blacklist database table and blocks or forwards it to the next part of the framework.
- The third part of the framework is service traceback oriented architecture (STBOA) component that would be designed to validate whether the incoming request is launched by a human (real web browser) or by an automated tool (bots).
- The forth part of the framework shall be entropy based (EB) component, which would be employed to detect anomalies in SIP network traffic and to differentiate whether it is high rate DDoS (HR-DDoS) attacks or flash crowd (FC) attacks.
- The framework would be evaluated using simulation of practical experiments of AntiDDoS_Shield system, which would be developed based on the Framework, and the analysis of corresponding experimental results. The simulation environment will be constructed by using virtualization technology to include all of the needed vectors and players.
- The Quagga and iproute2 routing suites software would be employed on the edge router at the entrance of the network. The main objective of these two tools is to permit or deny network traffic routing to inside and outside of the network.

V. THE PROPOSED DEFENSE FRAMEWORK FOR COUNTERING FLOOD BASED SIP-APP (D)DOS ATTACK

The defense framework for Countering Flood based SIP-App (D)DoS Attack will be traffic volume limit based defense framework. We will explain the framework more with operational architecture, the traffic volume architecture and the conceptual architecture.

➢ *Operational Architecture of Framework for Countering Flood based SIP-App (D)DoS Attack*

As shown in figure 2 has two active domains which are the core networks and the edge networks. A core network usually consists of high-speed core routers, this is the backbone of network which is in charge of transferring traffics among multiple edge networks (this architecture has four edge networks). The edge network is the second domain which connects the core network through edge routers. Figure 1 shows that our Flood based SIP-App (D)DoS defense system is deployed in each edge router of the protected network. Whenever distributed denial of service (DDoS) attack traffic is being transmitted across the edge network towards the victims, the defense system in the victim-end edge network can easily detect the attack because attack traffic creates a larger set of anomalies at the victim end than at the source ends but it is impossible for the defense system to react to the attacks in the victim-end edge

ISSN No:-2456-2165

network when the attacks are heavy. From the traffic volume architecture (figure 2) and the conceptual architecture of the framework (figure 3), we proposed a second line of action with a defense system in the source-end edge networks to react to the attacks. In our framework, the detection of and response to DDoS attacks happen at the source end edge routers. The source end edge router has enough resources with relatively low traffic. The traffic volume based DDoS detection techniques detect DDoS attacks in the victim-end edge network by recognizing anomalous changes of average traffic volumes at the victims' edge routers. The two architectures show more of the activities of the defense framework.

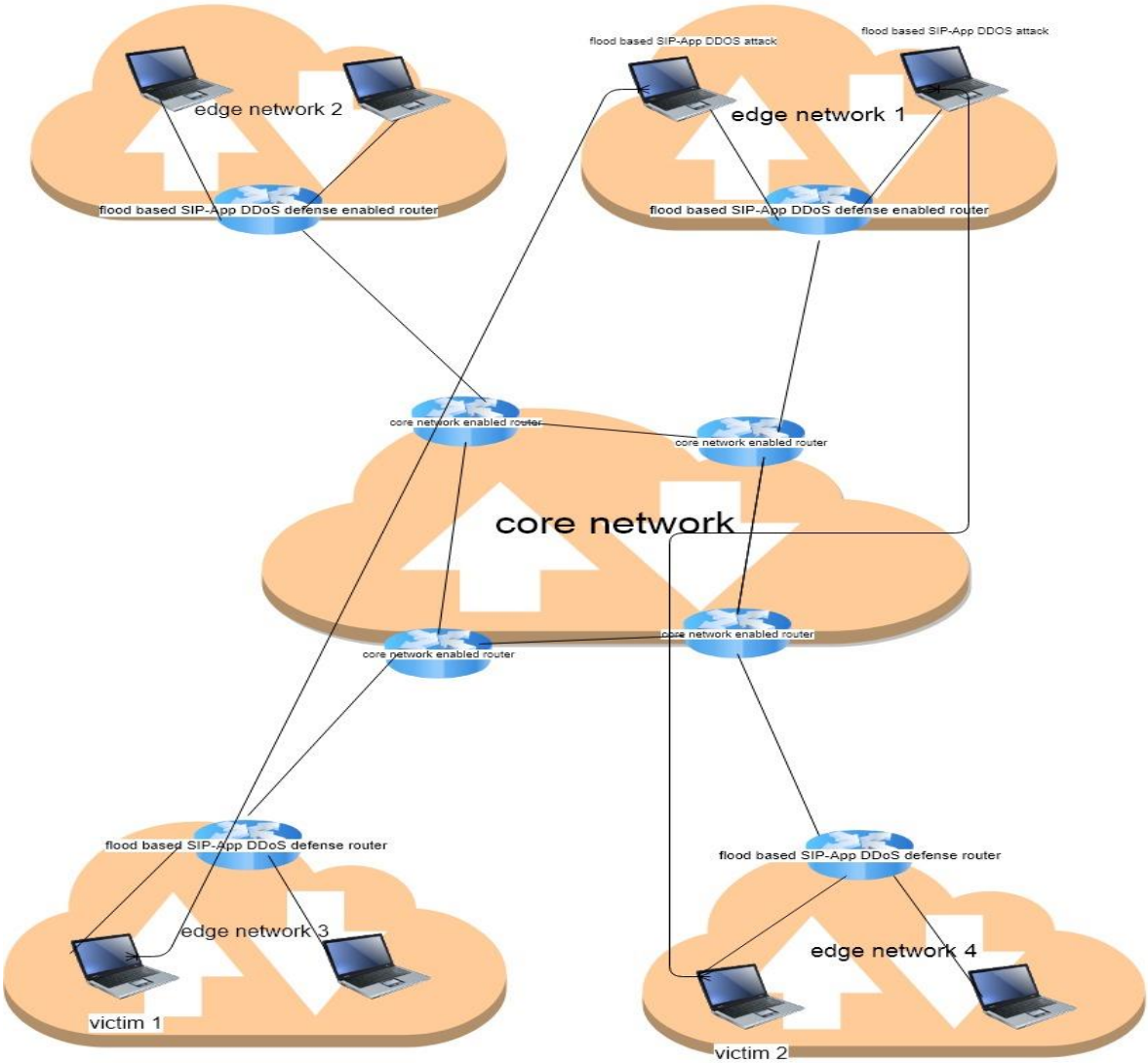

Fig 2 Operational Architecture of Framework for Countering Flood based SIP-App (D)DoS

- *Traffic Volume Architecture of Framework for Countering Flood based SIP-App (D)Dos*

As shown in figure 3 illustrates the overall operation of defending in the event of a Flood based SIP-App DDoS attack. It has the victim end and source end part of the defense. It also has four activities at the victim end which are; action of detecting flood based attack, the action of observing the aggressive network, the action of observing stable network and the action of detecting the end of flood based attacks. There are alert messages between a victim end and a source end include three types: Request messages, Update messages, and Cancel messages. These messages are used in different phases of defeating a Flood based SIP-App DDoS attack. At the beginning of an attack, a request message from a victim end will provide a suggested rate of traffic limit value to a source end (it has four network actions which are: the action for setting up the traffic rate limit, the action for decreasing the traffic rate limit, the action for increasing the traffic rate limit and the action for canceling the traffic rate limit). When the volume of attack traffic increases aggressively, an update message will be sent to the source end again to decrease the traffic rate limit value. Based this message, the source-end defense system will decrease the traffic rate limit value exponentially. After the traffic rate at the victim end has returned to normal for a while, an update message will be sent to the source end asking it to increase the rate limit value linearly. Finally, if the defense system has not found any anomalous changes in the victim end since the update message was sent, a cancel message will be sent to the source end to remove the traffic rate limit at that point.

ISSN No:-2456-2165

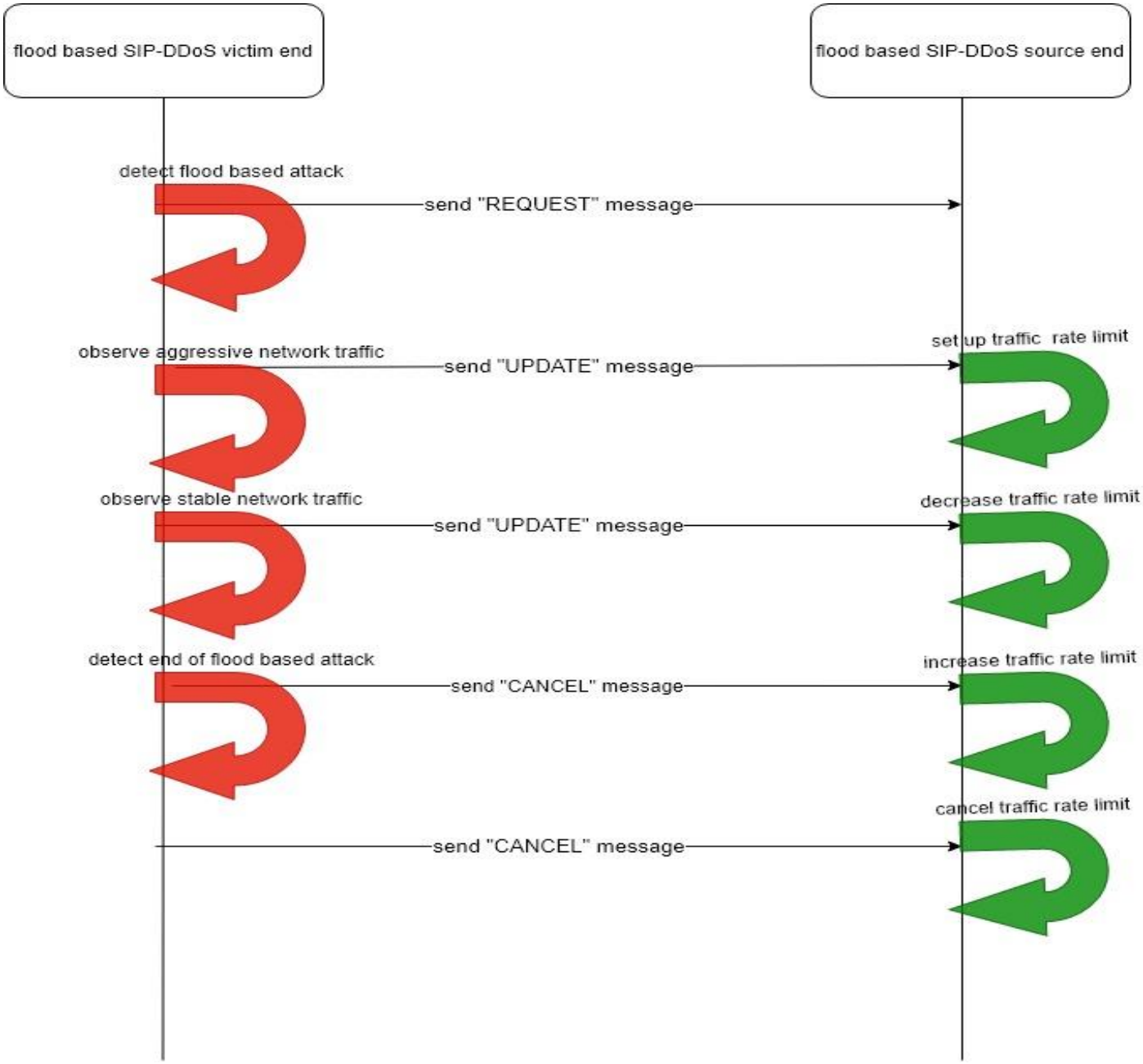

Fig 3 Traffic Volume Architecture of Framework for Countering Flood based SIP-App (D)DoS

➢ *Conceptual Architecture of Framework for Countering Flood based SIP-App (D)DoS*

Is shown in figure 4. This architecture has four components in the two active ends, which are:

- *The SIP proxy server and the stateless firewall,*
- *The outer attack blocking components,*
- *Service trace back Architecture and*
- *Entropy based component*

These four components of the defense system are found in the victim end defense system and source end defense system. The entropy based (EB) component of the flamework would be employed to detect anomalies in SIP network traffic and to differentiate whether it is high rate DDoS attacks or flash crowd (FC) attacks. After analyzing the information from a victim edge router (Router 2), the detection component will report the ongoing DDoS attack to the service trace back component.

ISSN No:-2456-2165

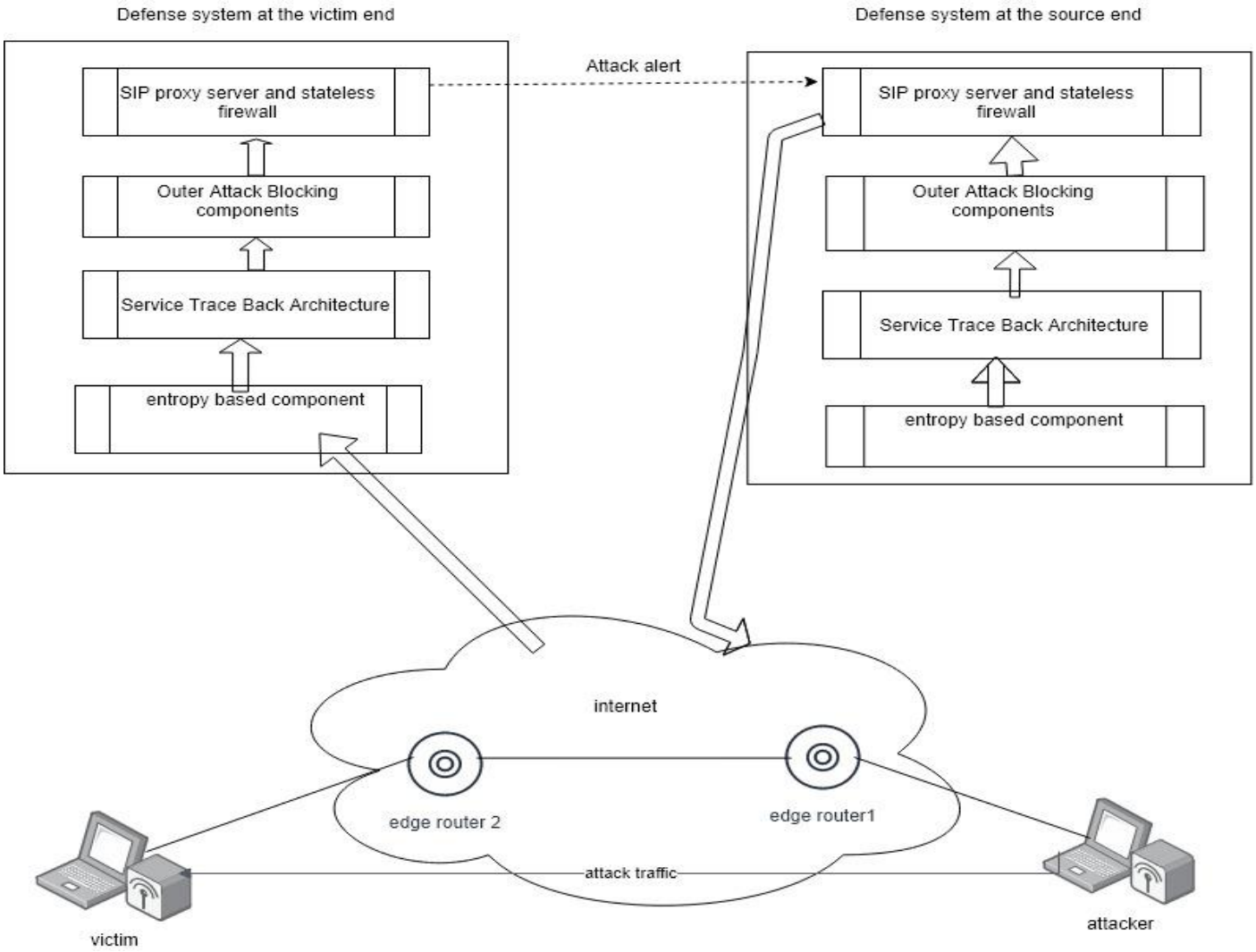

Fig 4 Conceptual Architecture of Framework for Countering Flood based SIP-App (D)DoS

The service trace back component implements the Fast Internet Trace back technique by grouping enough packets from the source edge router (Router 1), the trace back component will also get the IP address of Router 1. The recorded IP address of router 1 will be sent to the outer attack blocking (OB) component of the framework which has being deployed at the edge router 2, since it is the most nearest point to the IP attacking source. It will first compare and examine the IP source of the incoming request according to its blacklist database table. Then it blocks or forwards it to the next part of the framework (SIP proxy server) based on whether the incoming request's IP source is listed in blacklist database table at the edge router or not. In case this IP source of the incoming request is not listed on blacklist database table, it forwards it to the next part of the framework. Otherwise, if it is listed on the blacklist database table, OB component blocks it immediately, and host unreachable message will be sent to the caller. This layer provides a helpful service to the web server for all blocking processes. Finally, an alert message which carries attack information and traffic rate limits is sent to the source-end defense system. Based on this information, the service trace back control components at the source end set up the traffic rate limit for the traffic sent to victim in Router 2. To drop all attack packets, the entropy based components will be triggered in the source-end edge network after receiving an alert message from the defense system of the victim-end edge network to filter all malicious traffic. The Conceptual architecture of framework for Countering Flood based SIP-App (D)DoS demonstrated the detection and response to Flood based SIP-App (D)DoS and the interaction of the internet with the four components of the framework.

VI. CONCLUSION

This research work will provides insight towards the development of a An aggressive defense framework for detecting and Countering Flood based SIP-App (D)DoS attacks on the internet, a framework that identifies and determine the corpus parameters in a DDoS detection. algorithm will assist in enabling security researcher design preventive algorithms that are robust in nature in protecting systems and curbing attacks before occurrence. It provides a novel alternative protective framework to protect web applications from all sorts of SIP-App DDDoS attacks, such as high rate DDoS (HR-DDoS) and flash crowd (FC). In addition, it is quite able to validate and trace back the real attacking IP sources and block them at the edge router by the outer attack blocking components.

REFERENCES

[1]. Chen, R.-C., Cheng, K.-F., Chen, Y.-H., & Hsieh, C.-F. (2009). Using rough set and support vector machine for network intrusion detection system. First Asian conference on intelligent information and database systems, April 1–3. IEEE. doi:10.1109/ACIIDS.2009.59

[2]. Li M and Li M (2009). A new approach for detecting DDoS attacks based on wavelet analysis. 2nd IEEE International Congress on Image and Signal Processing (CISP '09): 1-5. https://doi.org /10.1109/CISP.2009.5300903

[3]. Hoffstadt D, Rathgeb E, Liebig M, Meister R, Rebahi Y and Thanh TQ (2014). A comprehensive framework for detecting and preventing VoIP fraud and misuse. The IEEE International Conference on Computing, Networking and Communications (ICNC): 807-813. https:// doi.org/10.1109/ICCNC.2014.6785441

[4]. Jeyanthi N, Thandeeswaran R and Vinithra J (2014). Rqa based approach to detect and prevent ddos attacks in voip networks. Cybernetics and Information Technologies, 14(1): 11-24.

[5]. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., and Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, *36*(1), 42–57.

[6]. Prolexic. (2013). *Quarterly Global DDoS Attack Report Q3 2013*. Hollywood: Prolexic.

[7]. Prolexic. (2014). *Quarterly Global DDoS Attack Report Q1 2014*. Hollywood: Prolexic.

[8]. Radware (2014). Defense Flow – SDN Based Network DDoS, Application DoS and APT Protection . Available at: http://www.radware.com/Solutions/SDN/

[9]. Sambath N., Selvakumar M. and Yu-Beng L. (2016). DDoS attacks in VoIP: a brief review of detection and mitigation techniques. International Journal of Advanced and Applied Sciences, 3(9) 2016, Pages: 90-96

[10]. Tang J, Cheng Y and Hao Y (2012, March). Detection and prevention of SIP flooding attacks in voice over IP networks. The 2012 IEEE Proceedings In *Narayanan et al/ International Journal of Advanced and Applied Sciences, 3(9) 2016, Pages: 90-96*

[11]. Tritilanunt S, Sivakorn S, Juengjincharoen C and Siripornpisan A (2010). Entropy-based input-output traffic mode detection scheme for DOS/DDOS attacks. The 2010 IEEE International Symposium on Communications and Information Technologies (ISCIT): 804-809. https://doi.org/ 10.1109/ISCIT.2010.5665097