A NOVEL SIP BASED DISTRIBUTED REFLECTION DENIAL-OF-SERVICE ATTACK AND AN EFFECTIVE DEFENSE MECHANISM

M. Selva Ganapathi[1], A. Ramasubramaniyam[2]

[1]Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.
Email : selvakrish820@gmail.com

[2]Associate Professor, Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.
Email: ramasubramanian.csa@avit.ac.in

Abstract

We are launching a SIP based attack Named as SR-DRDoS attack, which is slightly exploited Known SIP facilities using IP-spoofing Techniques, reflection-based attack logic and DDoS Attack Logic. Also, we make a SIP Mr. DoS / DDoS attack simulator based on SIP, Use this to activate our SR-DRDoS attack. Our Attack has been shown to dramatically increase CPU SIP server load 4. 0% to 100% only A few minutes after the attack began. our first Creates orderly traffic in intelligent attack SIP network using reflection methods, ie Blacklist and ignore IPs, pocket numbers or numbers Session / Transaction based rate limit and Automatic Message Formation Identification System Art security living in the state of the periphery Firewalls, intrusion detection / prevention etc. Systems and anomaly detection systems. Without this, We propose a new security mechanism Our proposed DRDoS effectively mitigates the attack. Our security system has been shown to be successful Reduce CPU load of attacked SIP server Reduced from 41% to 14% within 3 minutes started.

.

Keywords: SIP, SIP Security,DoS, DDoS, DRDoS, Distributed Reflection Denial of Service Attack, Reflection Attack , Session Initiation Protocol

1. INTRODUCTION

Voice over IP (VoIP) protocol has become one Important component of modern corporate Communication and many enterprises fully Rely on it for their voice and video Communications. However, VoIP brings Due to opportunities as well as its security risks Current Weaknesses in Internet Protocol (IP) And their possible exploitation by hackers. Session initiation protocol (SIP) is widely used VoIP signaling protocol for signaling and Control of multimedia communication sessions. The most common applications of SIP are Internet Telephony and video calls over IP networks. Sip Defines the messages that control the installation, Call termination and other basic elements Occurs between endpoints. Fraud survey Communication Fraud Control Report Association (CFCA) shows that approx. Global Telecom Revenue for 2017 $ 2: 30 Trillion And the estimated global loss is 29: 2 billion dollars, Same year. Damage due to network misuse, Device or configuration vulnerabilities reported $ 1: 29 billion.

2. RELATED WORK

IM Tas, B Ugurdogan, S Baktir [1] Voice-over-IP (VoIP) and its underlying session initiation protocol (SIP) technology have become popular in recent years. VoIP/SIP technologies are widely used in unified communications systems and next generation networks, and there is no doubt that they will play an increasingly important role in the future of communication technologies. However, unlike Transmission Control Protocol (TCP)-based applications, User Datagram Protocol (UDP)-based VoIP/SIP applications are not as mature and have some security vulnerabilities.

T Bessis, VK Gurbani, A Rana [2] As Session Initiative Protocol (SIP) deployment accelerates, simultaneous There is a need to secure the SIP infrastructure. One way to do this is through a SIP firewall, which is Loosely defined as a device that prevents invasion through SIP. Using this definition, A firewall is indistinguishable from a session boundary controller (SBC), which is also used by a SIP service. provider to secure your network. SIP firewalls and SBCs are often deployed by a SIP service Provider within the periphery of the network to place an order on SIP traffic...

CFCA Fraud Loss Survey [3] This article is about embedded SIP communication servers with easy integration into computer networks based on open source solutions and its effective defense against the most current attack - denial of service. The article contains a brief introduction to Bright Embedded Solutions for IP Telephony - BESIP and describes the most common types of DoS attacks, applied to SIP elements of VoIP infrastructure, including the consequences of defensive mechanisms that have been designed has gone.

T Mahjabin, Y Xiao, G Sun [4] Distributed denial of service is one of the most prominent and important attacks in today's cyber world. With a simple yet extremely powerful attack mechanism, it poses a great threat to today's internet community. In this article, we present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a systematic analysis of these types of attacks, including motivation and development, analysis of various attacks so far, security techniques and mitigation techniques, and potential limitations and challenges of existing research. Finally, some important research directions are outlined that need more attention in the near future to ensure a successful defense against distributed denial of service attacks.

3. EXISTING SYSTEM

Since our intelligent attack method creates legitimate traffic over SIP networks using reflection methods, it can be used to blacklist IP-based, packet counting or session/transaction based rate limiting systems and bypass existing automated message generation detection systems. can be done for. proves to be done. State-of-the-art security perimeters such as firewalls, intrusion detection / prevention systems and anomaly detection systems. Against an SR-DRDoS attack, we propose an effective defense mechanism that periodically collects a window of network traffic and calculates dynamic threshold values to trigger rule-based filtering actions.

Disadvantages

- Power management and equipment scheduling problem is solved by observation, learning and optimization (OLA) algorithm which adds more intelligence to EMS. The proposed mechanism significantly reduces cost and PAR, but UC is compromised.
- The proposed scheme did not consider the convenience of the user in problem formulation.
- Rapid growth in home electronic equipment significantly increases the demand for electricity in the residential sector.

4. PROPOSED WORK

While DRDoS attacks have been investigated theoretically in the literature, they have not been implemented on a real SIP network to see their negative effects on the operation of the network. Furthermore, there are several attack simulators publicly and commercially available, whereas we are not aware of any simulators focusing on replicating multiple attack scenarios to help service providers and/or home users to test their networks for vulnerabilities. With this work, we propose a novel SIP based DRDoS attack, named as SIP Request Based DRDoS (SR-DRDoS), and show its efficacy in a real VoIP network environment using our novel attack simulator tool. Furthermore, we propose a novel defense mechanism that effectively mitigates the proposed DRDoS attack.

Advantages

- In this attack, the attacker uses broadcast networks and has the advantage of having the ability to use a zombie without infiltrating or manipulating the system.
- We propose a new SIP-based DRDoS attack called SR-DRDoS, which uses attack vectors obtained by fusing vulnerabilities in some lesser-known SIP features with IP spoofing techniques, image-based attack logic, and DDoS attack logic. it is.
- Our DRDoS attack simulator bypasses attack detection and prevention systems using features such as IP spoofing, generation of SIP request / reflection messages, and generation of random SIP messages.

5. ARCHITECTURE

The Structural design of the proposed system is shown in the figure-1:

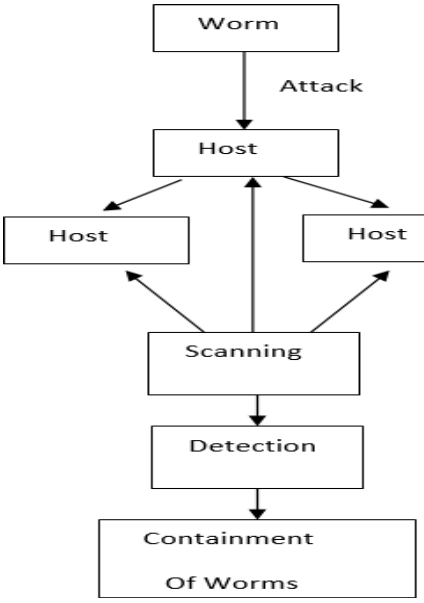


Fig 1 : Denial-of-Service attack Architecture

6. MODULE DESCRIPTION

6.1 Distributed reflection denial of service Attacks:

Reflection-based attack logic is used in DRDoS attacks. In a DRDoS attack, the attacker aims to force Reflector to send packets to the victim. To do this, the attacker impersonates the target victim and sends forged requests to millions of computers, causing the target victim to be inundated with responses from those computers. In a DRDoS attack, the effect of a packet sent by an attacker is reflected in multiple detractors, making it more effective than normal DoS / DDoS attacks. The greater the number of reflectors, the greater the effect of the attack. For example, when a packet sends more than 250 reflectors, it consumes 250 times more resources than a DDoS attack. A DRDoS attack is much more intense than other types of DoS attacks and can easily destroy a server.

6.2 Dos and ddos attack against sip

Certain mechanisms in the SIP protocol structure potentially facilitate exploitation using DoS/DDoS attacks. DoS attacks are blocking-of-service attacks that can be used to consume excessive amounts of resources such as bandwidth, physical disk space, and CPU time. This can result in corruption of configuration information, overloading with service requests (which the server cannot handle) or even failure of physical components in the network. The total number of requests sent from a single IP address within a certain pre-determined time frame can be intercepted, or session/transaction based rate-limiting security can be employed to protect SIP systems against DoS attacks. could.

.

6.3 Session initiation protocal

The Voice Over IP (VoIP) protocol has become an important component of modern corporate communications and many companies rely entirely on it for their voice and video communications. However, VoIP offers opportunities along with its security risks due to vulnerabilities in the Internet Protocol (IP) and its possible exploitation by hackers. Session Initiation Protocol (SIP) is a widely used VoIP signaling protocol for signaling and controlling multimedia communication sessions. The most common applications for SIP are Internet telephony and video calls over IP networks. SIP defines the messages that govern the setup, termination, and other basic elements of calls that take place between endpoints. The Communication Fraud Control Association (CFCA) fraud survey report shows that the estimated global telecommunications revenue for 2017 is $ 2: 30 trillion and the estimated global loss is $ 29: 2 billion for the same year . Losses due to network abuse, device or configuration weaknesses are reported to be $ 1: 29 billion.

6.4 Distribution denial of service:

A DoS attack is performed by a single computer, while a Distributed Denial of Service (DDoS) attack is performed by multiple computers. In this attack, the large amount of network traffic generated overwhelms the server and prevents legitimate users from accessing its services. Unlike Transmission Control Protocol (TCP) based applications, User Datagram Protocol (UDP) based applications are not as mature and have some vulnerabilities. In a distributed reflection denial of service (DRDoS) attack, the attacker spoofs the victim's IP address and, using UDP, sends an information request to a reflector known to respond to this type of request. The reflectors respond to a request for information and send their response (mirror) to the victim's IP address. A previous study exploits the vulnerabilities of the SIP relay mechanism by using IP address spoofing techniques. In this study, we exploit the reflection mechanism in SIP.

7. RESULTS

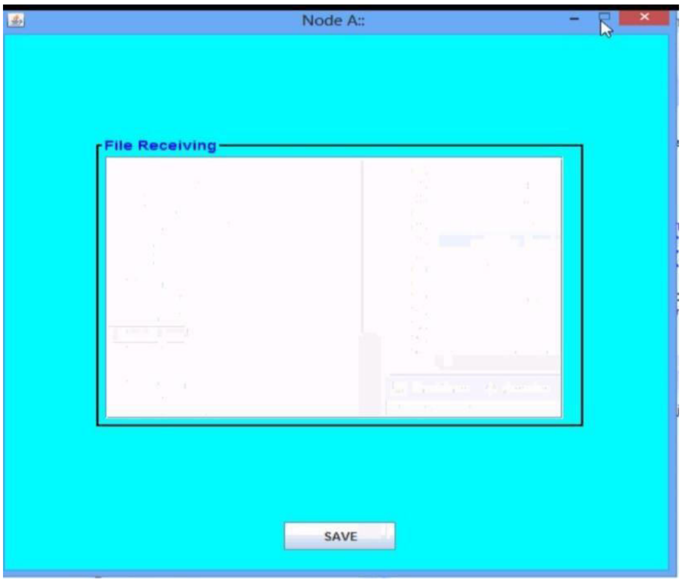


Fig 2: Node A

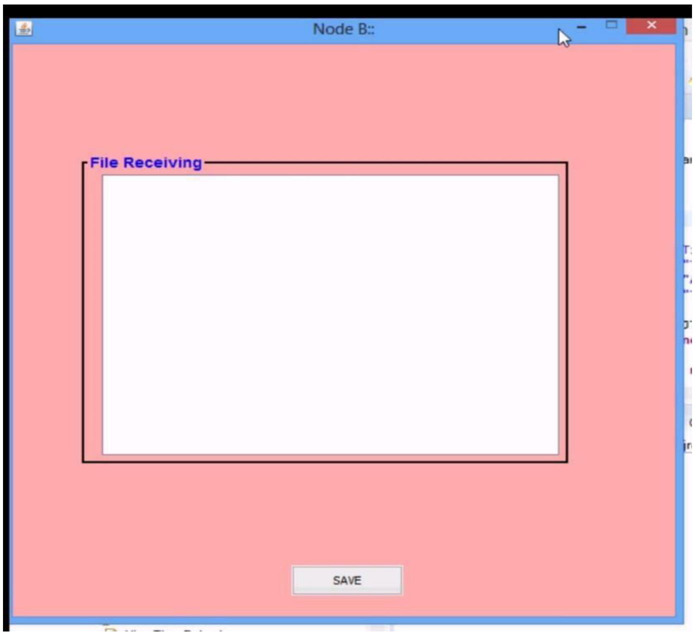
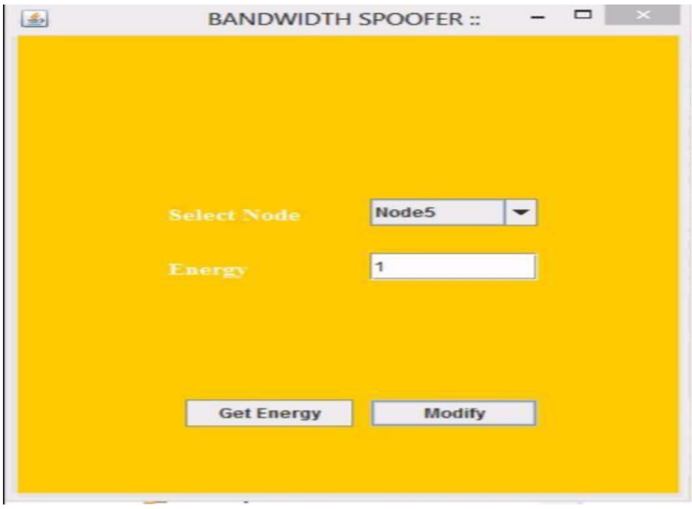


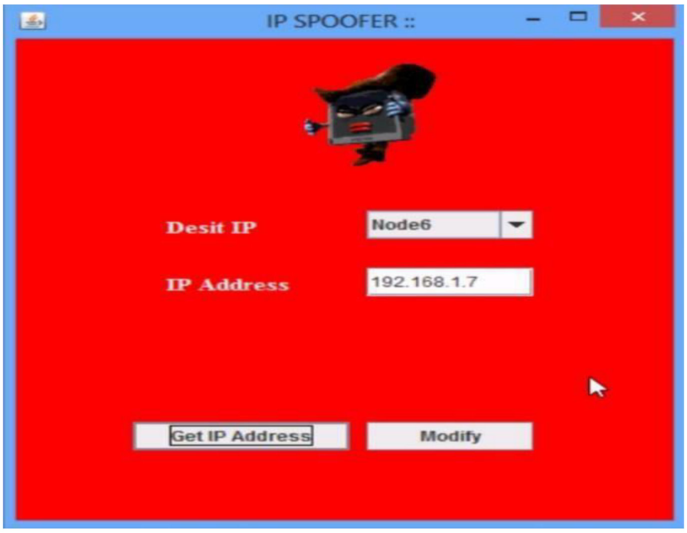
Fig 3 : Node B



Select Node: Node5

Energy: 1

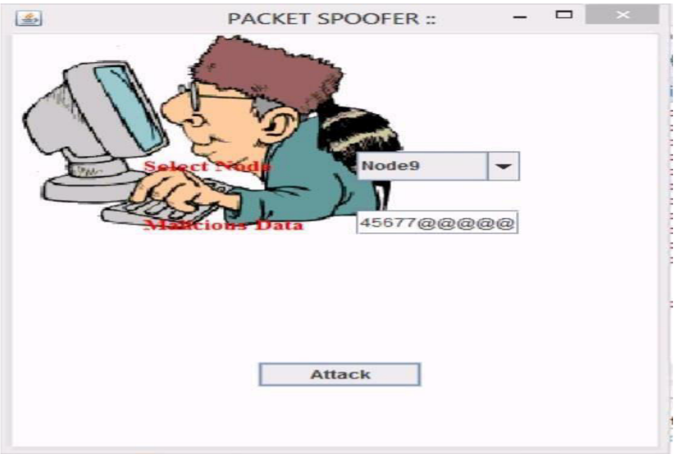
Fig 4 : BandWidth Spoofer –successfully Attacked node 5



Desit IP: Node6

IP Address: 192.168.1.7

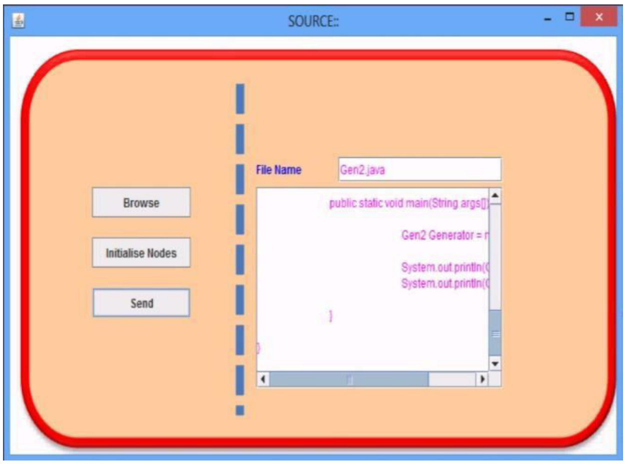
Fig 5:IP Spoofer.- Attacked node 6



Select Node: Node9

Malicious Data: 45677@@@@@

Fig 6 : Packet Spoofer – Attacked node 9



File Name: Gen2.java

```
                    public static void main(String args[])
                                  Gen2 Generator = n
                                  System.out.println((
                                  System.out.println((
                    }
}
```

Fig 7 : Source – browse the data then initiate Node B, data send to Node B

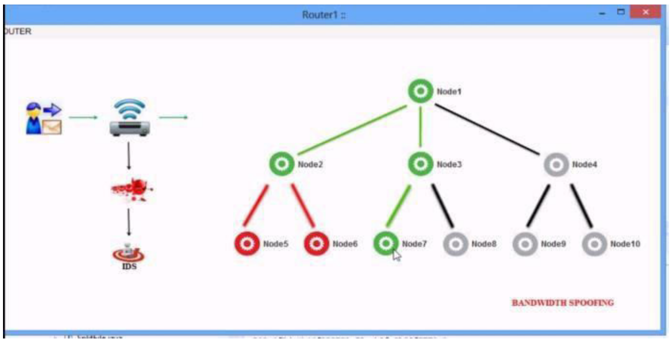
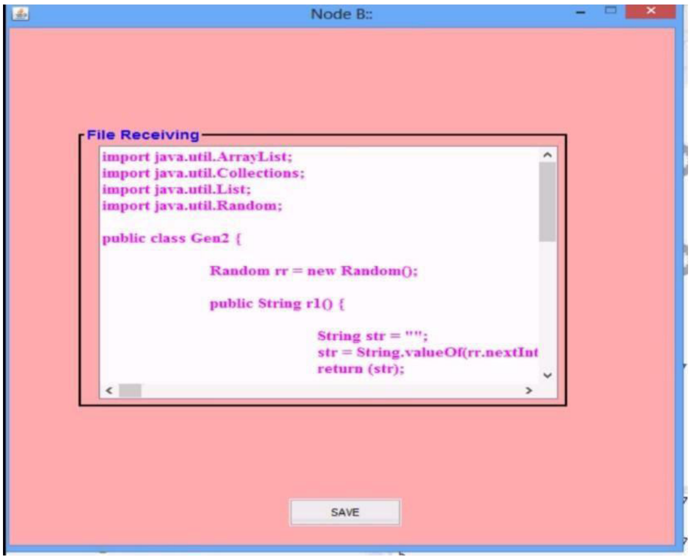
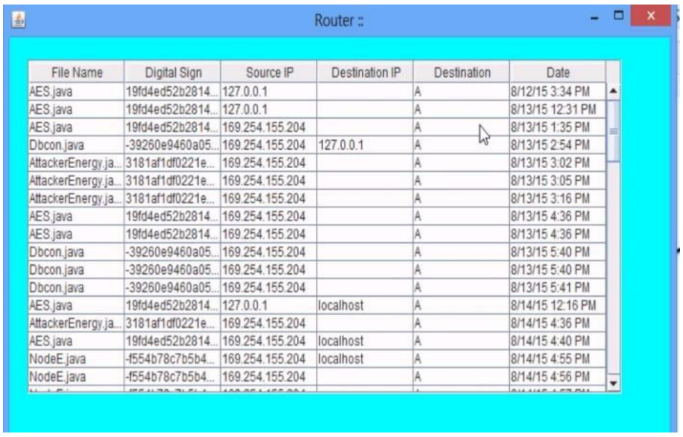


Fig 8: Router 1 – Finding the Secure way to Reach Node B



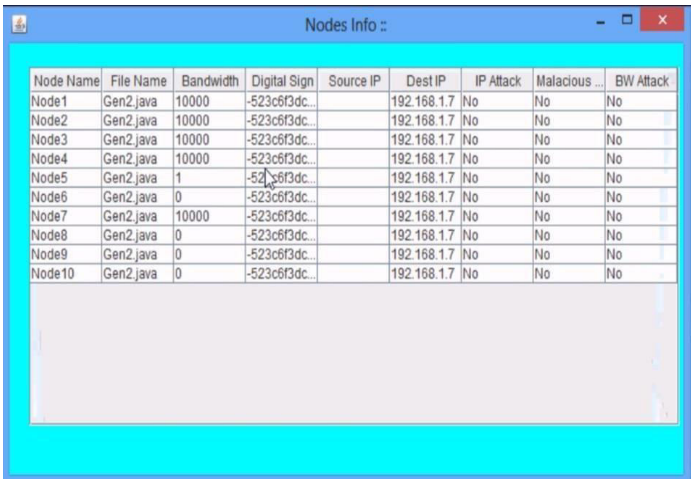
```
import java.util.ArrayList;
import java.util.Collections;
import java.util.List;
import java.util.Random;

public class Gen2 {

            Random rr = new Random();

            public String r1() {

                        String str = "";
                        str = String.valueOf(rr.nextInt
                        return (str);
```

Fig 9: Node B –Successfully Data received



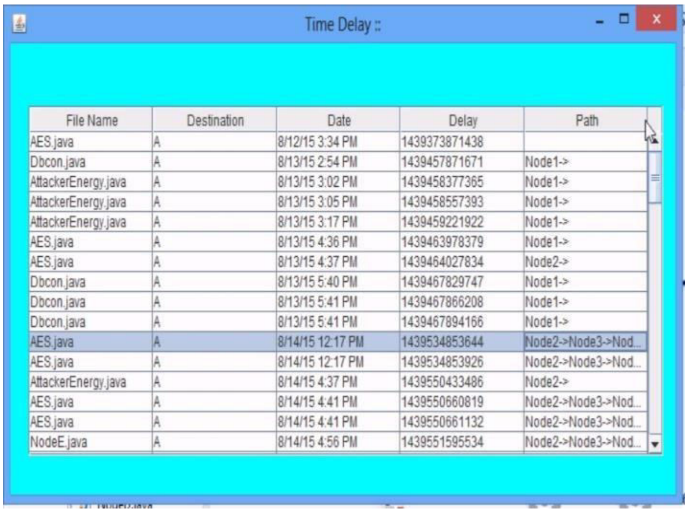
File Name	Digital Sign	Source IP	Destination IP	Destination	Date
AES.java	19fd4ed52b2814...	127.0.0.1		A	8/12/15 3:34 PM
AES.java	19fd4ed52b2814...	127.0.0.1		A	8/13/15 12:31 PM
AES.java	19fd4ed52b2814...	169.254.155.204		A	8/13/15 1:35 PM
Dbcon.java	-39260e9460a05...	169.254.155.204	127.0.0.1	A	8/13/15 2:54 PM
AttackerEnergy.ja...	3181af1df0221e...	169.254.155.204		A	8/13/15 3:02 PM
AttackerEnergy.ja...	3181af1df0221e...	169.254.155.204		A	8/13/15 3:05 PM
AttackerEnergy.ja...	3181af1df0221e...	169.254.155.204		A	8/13/15 3:16 PM
AES.java	19fd4ed52b2814...	169.254.155.204		A	8/13/15 4:36 PM
AES.java	19fd4ed52b2814...	169.254.155.204		A	8/13/15 4:36 PM
Dbcon.java	-39260e9460a05...	169.254.155.204		A	8/13/15 5:40 PM
Dbcon.java	-39260e9460a05...	169.254.155.204		A	8/13/15 5:40 PM
Dbcon.java	-39260e9460a05...	169.254.155.204		A	8/13/15 5:41 PM
AES.java	19fd4ed52b2814...	127.0.0.1	localhost	A	8/14/15 12:16 PM
AttackerEnergy.ja...	3181af1df0221e...	169.254.155.204		A	8/14/15 4:36 PM
AES.java	19fd4ed52b2814...	169.254.155.204	localhost	A	8/14/15 4:40 PM
NodeE.java	-f554b78c7b5b4...	169.254.155.204	localhost	A	8/14/15 4:55 PM
NodeE.java	-f554b78c7b5b4...	169.254.155.204		A	8/14/15 4:56 PM

Fig 10: Router Details



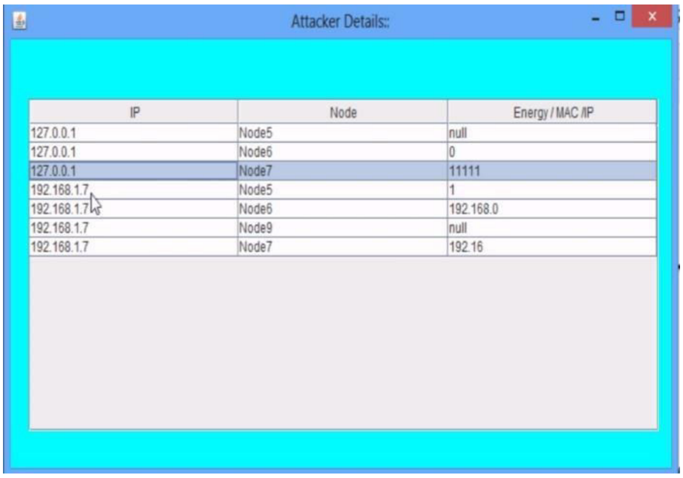
Node Name	File Name	Bandwidth	Digital Sign	Source IP	Dest IP	IP Attack	Malacious ...	BW Attack
Node1	Gen2.java	10000	-523c6f3dc...		192.168.1.7	No	No	No
Node2	Gen2.java	10000	-523c6f3dc...		192.168.1.7	No	No	No
Node3	Gen2.java	10000	-523c6f3dc...		192.168.1.7	No	No	No
Node4	Gen2.java	10000	-523c6f3dc...		192.168.1.7	No	No	No
Node5	Gen2.java	1	-523c6f3dc...		192.168.1.7	No	No	No
Node6	Gen2.java	0	-523c6f3dc...		192.168.1.7	No	No	No
Node7	Gen2.java	10000	-523c6f3dc...		192.168.1.7	No	No	No
Node8	Gen2.java	0	-523c6f3dc...		192.168.1.7	No	No	No
Node9	Gen2.java	0	-523c6f3dc...		192.168.1.7	No	No	No
Node10	Gen2.java	0	-523c6f3dc...		192.168.1.7	No	No	No

Fig 11: Nodes Info



File Name	Destination	Date	Delay	Path
AES.java	A	8/12/15 3:34 PM	1439373871438	
Dbcon.java	A	8/13/15 2:54 PM	1439457871671	Node1->
AttackerEnergy.java	A	8/13/15 3:02 PM	1439458377365	Node1->
AttackerEnergy.java	A	8/13/15 3:05 PM	1439458557393	Node1->
AttackerEnergy.java	A	8/13/15 3:17 PM	1439459221922	Node1->
AES.java	A	8/13/15 4:36 PM	1439463978379	Node1->
AES.java	A	8/13/15 4:37 PM	1439464027834	Node2->
Dbcon.java	A	8/13/15 5:40 PM	1439467829747	Node1->
Dbcon.java	A	8/13/15 5:41 PM	1439467866208	Node1->
Dbcon.java	A	8/13/15 5:41 PM	1439467894166	Node1->
AES.java	A	8/14/15 12:17 PM	1439534853644	Node2->Node3->Nod...
AES.java	A	8/14/15 12:17 PM	1439534853926	Node2->Node3->Nod...
AttackerEnergy.java	A	8/14/15 4:37 PM	1439550433486	Node2->
AES.java	A	8/14/15 4:41 PM	1439550660819	Node2->Node3->Nod...
AES.java	A	8/14/15 4:41 PM	1439550661132	Node2->Node3->Nod...
NodeE.java	A	8/14/15 4:56 PM	1439551595534	Node2->Node3->Nod...

Fig 12: Time Delay



IP	Node	Energy / MAC /IP
127.0.0.1	Node5	null
127.0.0.1	Node6	0
127.0.0.1	Node7	11111
192.168.1.7	Node5	1
192.168.1.7	Node6	192.168.0
192.168.1.7	Node9	null
192.168.1.7	Node7	192.16

Fig 13: Attackers details

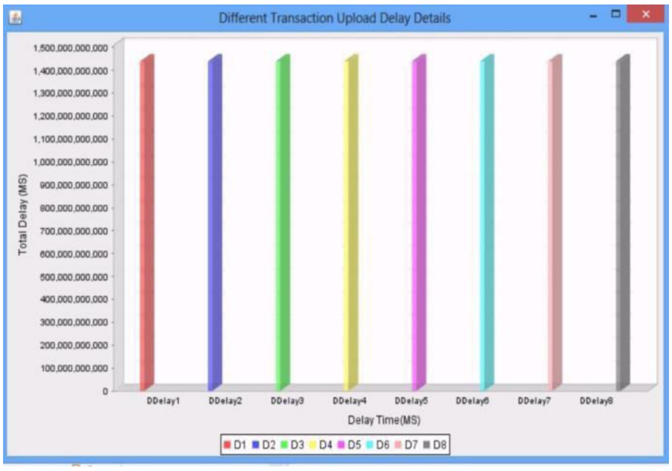


Fig 14: Different Transaction Upload Delay Details

8. CONCLUSION

We introduced a new DRDoS attack, named SRDRDoS attack, which exploits reflection based vulnerabilities in UDP based SIP signalling. Furthermore, we have developed a new attack tool called Mr.SIP, and used it to realize our SR-DRDoS attack in a simulated version of an enterprise-grade SIP network. Our attack implementation was shown to dramatically increase the CPU load of a SIP server from %0 to %100 within just 4 minutes after the start of the attack. Our SIP-based DRDoS attack implementation was proven to bypass existing network defense mechanisms in SIP networks, such as firewalls, intrusion detection/prevention systems, black-lists, IP address based rate-limiting and packet-count based rate-limiting - Limiting. In addition, we have proposed a new defense mechanism that effectively mitigates the proposed DRDoS attack and is proven to be more effective than the existing defense mechanism.

REFERENCES

[1] I. M. Tas, B. Ugurdogan, and S. Baktir, “ Novel session initiation protocolbased distributed denial-of- service attacks and effective defense strategies,” Computers & Security, vol. 63, pp. 29–44, 2016.

[2] T. Bessis, V. K. Gurbani, and A. Rana, “ Session initiation protocol firewall for the IP multimedia subsystem core,” Bell Labs Technical Journal, vol. 15, no. 4, pp. 169–187, 2011.

[3] CFCA Fraud Loss Survey, Communications Fraud Control Association, 2017. [Online]. Available: https://www.cfca.org/fraud-loss-survey

[4] D. Sisalem, J. Kuthan, and S. Ehlert, “Denial of Service Attacks and SIP Infrastructure: attack scenarios and prevention mechanisms,” IEEE Network, vol. 20, no. 5, pp. 26–31, 2006.

[5] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, “Booters – An analysis of DDoSas- a-service attacks,” in Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, Canada, May. 11- 15, 2015, pp. 243–251.

[6] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, “A survey of distributed denial-of-service attack, prevention, and mitigation techniques,” International Journal of Distributed Sensor Networks, vol. 13, no. 12, 2017.

[7] J. Stanek and L. Kencl, “SIPp-DD: SIP DDoS Flood-Attack Simulation Tool,” in Proc. 20th International Conference on Computer Communications and Networks (ICCCN), Maui, Hawaii, 31 July-4 August, 2011, pp. 1– 7.

[8] M. Poongothai and M. Sathyakala, “Simulation and analysis of DDoS attacks,” in Proc. International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET), Tiruchirappalli, India, December 13-14, 2012, pp. 78–85.