A HELLINGER DISTANCE BASED ALGORITHM TO DETECT DISTRIBUTED DENIAL OF SERVICE ATTACKS ON VOICE OVER INTERNET PROTOCOL ENVIRONMENTS

NARAYANAN SAMBATH

UNIVERSITI SAINS MALAYSIA

2017

A HELLINGER DISTANCE BASED ALGORITHM TO DETECT DISTRIBUTED DENIAL OF SERVICE ATTACKS ON VOICE OVER INTERNET PROTOCOL ENVIRONMENTS

by

NARAYANAN SAMBATH

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science

August 2017

DEDICATION

This thesis is dedicated to my parents. My father, S. Narayanan did not only raise and nurture me but also taxed himself dearly over the years for my education and intellectual development. My mother, N. Selvi has been a source of motivation and strength during moments of despair and discouragement. My sincere heartful gratitude to my brothers, N.Dhanabalan and N.Hariprasanth for their endless love and support during this study period. I would like to appreciate my sister in law, D.Roobini for her encouragement during my study period. I would like to thank uncle Gunasaygaran for his help when I had frustration. I would like to convey my appreciation to my friends, Gowtham (Bond) and Dheenadhayalan for their support to initiate this study. A special thanks and appreciation to my friend, G.Revathy for her special caring and recommendation, who changed my profession to pursue this study successfully. I finally dedicate this thesis to my little princess D.Dheekshika. Word cannot truly express how much I owe you all.

ACKNOWLEDGEMENT

I am deeply indebted to my supervisor, Dr. Selvakumar Manickam from National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), whose guidance and help, stimulating suggestions and encouragement helped me in the research for writing of this thesis. I thank my co-supervisor Dr. Shankar Karuppayah for his support to complete my research work. I'm glad to thank Dr. Parminder Singh Bawa from NAv6, USM, for his motivation and support to pursue my research. I am very thankful to Dr. Leau Yu Beng, from Universiti Malaysia Sabah (UMS) for his valuable comments and suggestions along with his help and support for this thesis.

I would like to convey my appreciation to all the academic staffs, the administration, support staffs and colleagues in NAv6, USM for their dedication and persistent support. As does my funding body, the USM Fellowship, USM for awarding me a scholarship to pursuit this study. I am extremely grateful to my family for being patient and supporting me during my research.

Thank you.

Narayanan Sambath

TABLE OF CONTENTS

Acknowledgement ii

Table of Contents iii

List of Figures viii

List of Tables xi

List of Abbreviations xii

Abstrak xiv

Abstract xvi

CHAPTER 1: INTRODUCTION 1

1.1 Introduction 1

1.2 Security Issues faced by VoIP 4

1.2.1 Malformed Message Attack 4

1.2.2 Spoofing Attack 5

1.2.3 Eavesdropping Attack 6

1.2.4 Man in the Middle (MITM) Attack 7

1.2.5 Spam over Internet Telephony (SPIT) Attack 7

1.2.6 Call Hijacking Attack 8

1.2.7 Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack 9

1.3 Problem Statement 10

1.4 Thesis Aims and Objectives 11

1.5 Research Steps 11

1.6 Research Scope and Limitation 14

1.7 Research Contribution 14

1.8 Thesis Organization 15

CHAPTER 2: BACKGROUND AND RELATED WORK 17

2.1 Introduction to VoIP Architecture 17

2.1.1 Importance of VoIP 18

2.1.2 VoIP Protocols 19

2.2 SIP Architecture 21

2.2.1 SIP Messages 23

2.3 Denial of Service Attack 24

2.3.1 VoIP Signalling DoS Attack 25

2.3.2 VoIP Media DoS Attack 25

2.3.3 Physical DoS Attack 25

2.4 Distributed Denial of Service Attack 26

2.4.1 Invite Flooding DDoS Attack 27

2.4.2 Bye Flooding DDoS Attack 27

2.4.3 Spoofing Attack 27

2.5 Related Research 28

2.5.1 Entropy 33

2.5.2 Wavelet 34

2.5.3 Sketch and Hellinger Distance (SHD) 35

2.5.4 Sunshine 36

2.5.5 Recurrence Quantification Approach (RQA) 37

2.6 Discussion of Related Research 39

2.7 Summary 41

CHAPTER 3: PROPOSED HELLINGER DISTANCE BASED ALGORITHM IN VOIP ENVIRONMENT 42

3.1 Overview.....42

3.2 The General Structure of Proposed Algorithm.....42

3.3 Key Requirements of the Proposed Algorithm.....44

3.4 Overview of the Proposed Algorithm.....44

3.4.1 Data Preparation Phase.....46

3.4.1(a) Blacklist Checker.....46

3.4.1(b) Queue Steps.....47

3.4.2 Feature Extraction Phase.....47

3.4.2(a) Pike Screen Module.....48

3.4.2(b) Feature Processor.....49

3.4.3 Anomaly Detection Phase.....49

3.4.3(a) Anomaly Analyser.....50

3.4.3(b) Anomaly Detector.....52

3.4.4 DDoS Mitigation Phase.....53

3.4.4(a) Decision Engine.....53

3.4.4(b) Blacklisting Mechanism.....54

3.5 Scenarios in the Proposed Algorithm.....54

3.5.1 Scenario 1: Least Number of Pikes.....54

3.5.2 Scenario 2: Flash Crowd or DDoS Attack.....55

3.6 Chapter Summary.....57

CHAPTER 4: IMPLEMENTATION OF THE PROPOSED VDDM 58

4.1 Introduction.....58

4.2 Overview of Testbed Setup 58
4.2.1 Managed Switch 60
4.2.2 User Agent Entity 61
4.2.3 Attacker 62
4.2.4 Traffic Generator 63
4.2.5 SIP Server Entity 63
4.2.6 Mechanism Entity 64
4.3 Tools and Technologies 65
4.3.1 Inviteflood 66
4.3.2 SIPp 66
4.3.3 Collectl 67
4.3.4 Pyshark, Tshark 67
4.3.5 Python Script 68
4.4 Implementation Architecture 68
4.4.1 Data Preparation Phase 70
4.4.2 Feature Extraction Phase 71
4.4.3 Anomaly Detection Phase 72
4.4.4 DDoS Mitigation Phase 74
4.5 Summary 75

CHAPTER 5: EXPERIMENTS AND RESULTS 77

5.1 Introduction 77
5.2 Experiment Design 77
5.2.1 User Traffic Dataset 77
5.2.2 Experimental Setup 79

5.2.3 Evaluation Metrics 79
5.3 Evaluation Results 80
5.3.1 Dynamic SIP Traffic 81
5.3.1(a) Low Intensity Attack 81
5.3.1(b) High Intensity Attack 86
5.3.2 Constant SIP Traffic 89
5.3.2(a) Low Intensity Attack 89
5.3.2(b) Medium Intensity Attack 93
5.3.2(c) High Intensity Attack 96
5.4 Comparative Evaluation 99
5.4.1 Dynamic SIP Traffic 100
5.4.2 Constant SIP Traffic 101
5.5 Summary 103

CHAPTER 6: CONCLUSION AND FUTURE WORK 105
6.1 Overview 105
6.2 Summary of Research and Findings 105
6.3 Future Work 107

REFERENCES 108
LIST OF PUBLICATIONS

LIST OF FIGURES

Page

Figure 1.1	Growth of VoIP Subscribers	3
Figure 1.2	Malformed Message Attack	5
Figure 1.3	Spoofing Attack	5
Figure 1.4	Eavesdropping Attack	6
Figure 1.5	Man in the Middle Attack	7
Figure 1.6	SPIT Attack	8
Figure 1.7	Call Hijacking Attack	9
Figure 1.8	VoIP Security Threats	10
Figure 1.9	Research Methodology	13
Figure 2.1	VoIP Architecture	17
Figure 2.2	SIP Architecture	22
Figure 2.3	SIP Messages	23
Figure 2.4	DoS Attack Scenario	24
Figure 2.5	DDoS Attack Scenario	26
Figure 3.1	Design Architecture of VDDM Algorithm	43
Figure 3.2	The Proposed VDDM Algorithm Phases	45
Figure 3.3	Data Preparation Phase	46
Figure 3.4	Feature Extraction Phase	48
Figure 3.5	Anomaly Detection Phase	50
Figure 3.6	DDoS Mitigation Phase	53
Figure 3.7	Scenario of Least Number of Pikes	55
Figure 3.8	Scenario of Flash Crowd or DDoS Attack	56
Figure 4.1	Design of testbed topology	59

Figure 4.2	Configuration of Mirror Ports in ProCurve Switch	60
Figure 4.3	Algorithm for Data Preparation Phase	71
Figure 4.4	The Extracted SIP Features	71
Figure 4.5	Summarized Data in Pike Screen Module	72
Figure 4.6	Data in Feature Processor Module	72
Figure 4.7	Data in Anomaly Analyser Module	73
Figure 4.8	Data in Anomaly Detector Module	73
Figure 4.9	Data in One Freezing and One Proceeding Action	74
Figure 4.10	Algorithm for DDoS Mitigation Phase	75
Figure 5.1	Invite Packets per Second with 60 Attack Packets	82
Figure 5.2	Calculation of Hellinger Distance with 60 Attack Packets	83
Figure 5.3	Accumulated Invite Packets per Second with 60 Attack Packets	84
Figure 5.4	Invite Packets per Second with 500 Attack Packets	87
Figure 5.5	Calculation of Hellinger Distance with 500 Attack Packets	87
Figure 5.6	Accumulated Invite Packets per Second with 500 Attack Packets	88
Figure 5.7	Invite Packets per Second with 10 Attack Packets	90
Figure 5.8	Calculation of Hellinger Distance with 10 Attack Packets	90
Figure 5.9	Accumulated Invite Packets per Second with 10 Attack Packets	91
Figure 5.10	Invite Packets per Second with 80 Attack Packets	93
Figure 5.11	Calculation of Hellinger Distance with 80 Attack Packets	94
Figure 5.12	Accumulated Invite Packets per Second with 80 Attack Packets	95
Figure 5.13	Invite Packets per Second with 1200 Attack Packets	97
Figure 5.14	Calculation of Hellinger Distance with 1200 Attack Packets	97
Figure 5.15	Accumulated Invite Packets per Second with 1200 Attack Packets	98
Figure 5.16	Comparison of Detection Rate with Attack Packets	100

Figure 5.17 Comparison of Detection Rate with Other Techniques 102

LIST OF TABLES

Page

Table 2.1	Types of DDoS Attack	28
Table 2.2	Comparison of Existing Techniques for DDoS Attack in VoIP	40
Table 4.1	Hardware and Software Specifications for User Agents	61
Table 4.2	Hardware and Software Specifications for Attacker	62
Table 4.3	Hardware and Software Specifications for Traffic Generator	63
Table 4.4	Hardware and Software Specifications for SIP Server	64
Table 4.5	Hardware and Software Specifications for Mechanism Entity	65
Table 5.1	Packet Generation Statistics	101
Table 5.2	Comparison of Computation Time	101

LIST OF ABBREVIATIONS

ACK	Acknowledgement
ATA	Analog Telephone Adapter
ARPANET	Advanced Research Projects Agency Network
CDR	Call Data Record
CIA	Confidentiality, Integrity and Availability
CWT	Continuous Wavelet Transform
CPU	Central Processing Unit
DARPA	Defence Advanced Research Projects Agency
DNS	Domain Name System
DDoS	Distributed Denial of Service
sDoS	Denial of Service
DTMF	Dual Tone Multi Frequency
DWT	Discrete Wavelet Transform
EWMA	Exponentially Weighted Moving Average
HD	Hellinger Distance
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
MITM	Man in the Middle
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory

RQA	Recurrence Quantification Approach
SBC	Session Border Controller
SCS	Sensor Central Services
SDN	Software Defined Network
SHD	Sketch ad Hellinger Distance
SIP	Session Initiation Protocol
SPIT	Spam over Internet Telephony
TCP	Transmission Control Protocol
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URL	Universal Resource Locator
VoIP	Voice over Internet Protocol
WISR	Worldwide Infrastructure Security Report

ALGORITMA BERDASARKAN PENJARAKAN HELLINGER UNTUK MENGESAN SERANGAN PENAFIAN PERKHIDMATAN TERAGIH KE ATAS PERSEKITARAN PERKHIDMATAN PANGGILAN SUARA MELALUI PROTOKOL INTERNET

ABSTRAK

Komunikasi suara melalui Internet kini telah mengalami pertumbuhan yang pesat pada peringkat rumah dan perniagaan sejajar dengan perkembangan Suara melalui Protokol Internet (VoIP). Pertumbuhan pesat bilangan pelanggan VoIP adalah disebabkan oleh fleksibiliti VoIP, kualiti perkhidmatan yang lebih baik dan kos perkhidmatan yang rendah. Pertumbuhan ini menyebabkan ramai pengguna berpindah daripada Rangkaian Telefon Bersuis Awam (PSTN). Protokol Permulaan Sesi (SIP) merupakan protokol yang digunakan dalam VoIP, bertanggungjawab dalam mewujudkan sesi antara pemanggil dan penerima untuk komunikasi dwiarah menggunakan mesej SIP. VoIP, sepertimana perkhidmatan Internet yang lain, juga mengalami pelbagai isu-isu keselamatan dan kelemahan disebabkan pengenalan protokol-protokol baru di dalam infrastruktur rangkaian data tradisional yang sedia ada. Serangan Penafian Perkhidmatan Teragih (DDoS) adalah lebih mengancam berbanding dengan serangan-serangan lain. Tesis ini membincangkan serangan terhadap VoIP serta teknik pengesanan dan pertahanan terhadap serangan DDoS VoIP yang sedia ada. Ia juga mengemukakan suatu mekanisma untuk mengesan serangan DDoS dan mempertahankan perkhidmatan VoIP tanpa meletakkan beban tambahan ke atas pelayan SIP berdasarkan kepada penjarakan Hellinger. Algoritma yang disarankan terdiri daripada beberapa fasa analasis statistik untuk mengenalpasti penyerang. Ciri-ciri yang dipilih daripada paket yang diterima oleh pelayan SIP disemak dengan peraturan yang

ditakrifkan untuk mengkategorikan paket daripada penyerang. Mekanisme yang dicadangkan mampu mengesan semua paket penyerang yang bertujuan untuk membanjiri pelayan SIP dalam peringkat awal lagi. Keputusan penilaian analisis mekanisme yang dicadangkan menunjukkan bahawa algoritma yang disarankan mampu memberikan kadar pengesanan dengan ketepatan yang amat tinggi dan dapat mengurangkan masa komputasi sebanyak 0.2293 saat untuk mengesan penyerang.

A HELLINGER DISTANCE BASED ALGORITHM TO DETECT DISTRIBUTED DENIAL OF SERVICE ATTACKS ON VOICE OVER INTERNET PROTOCOL ENVIRONMENTS

ABSTRACT

Voice communication over the Internet has experienced rapid growth in homes and businesses with the development of Voice over Internet Protocol (VoIP). The growth in number of VoIP subscribers is due to VoIP flexibility, Quality of Service and being low in cost. This growth has prompted a major shift from the traditional public switched telephone network (PSTN) which is circuit-switched to a packet-switched VoIP. The Session Initiation Protocol (SIP), protocol used in VoIP, is responsible in creating session between a caller and a callee for bidirectional communication using SIP messages. The VoIP, as with other services on the Internet, also suffers from various security issues and vulnerabilities, arising from new protocols and the existing infrastructure of traditional data network. Distributed Denial of Service (DDoS) attack is more severe compared to other attacks. This thesis discusses different types of VoIP attacks along with the existing VoIP DDoS detection and mitigation techniques. The proposed work put forward an algorithm based on Hellinger distance to effectively detect and mitigate DDoS attack on VoIP service without putting additional burden on the SIP server. The proposed algorithm comprises of multiple statistical analysis phases to identify the attacker. The statistical phase helps to extract the features from the incoming packets. Then the data from the feature is processed and checked with dynamic threshold to categorize the attacker packets. The proposed algorithm is able to detect all the attacker packets flooding the SIP server in the early stage itself. Evaluation

results of the proposed algorithm indicates that the algorithm has a very high detection accuracy and reduce the computation time for detecting the attacker to 0.2293 seconds.

CHAPTER 1

INTRODUCTION

1.1 Introduction

One of the emerging technology rapidly embraced by the market is Voice over Internet Protocol (VoIP). This new technology that implements the services of Public Switched Telephone Network (PSTN), is changing the trend of voice communication services over the Internet. Traditional PSTN is now being replaced by VoIP whose services are replaced abundantly in homes and enterprises (Cao et al., 2005). Telephone, Internet and Internet Protocol (IP) are the fundamental technologies in the evolution of VoIP. Alexander Graham Bell and Elisha Gray invented the first telephone in 1870's (Gorman & Carlson, 1990). The earlier telecommunication systems involved switches, buttons and relay systems. Then, Shannon's concept of communicating in binary code transformed the entire digital communication from phone to the Internet. The Defence Advanced Research Projects Agency (DARPA) created time-sharing network of computers known as Advanced Research Projects Agency Network (ARPANET) in the year 1968 to develope Internet (Tronco, 2010). The development of online service companies provided proprietary information and email services during the popularity of Internet and personal computers. Dr. Vint Cerf invented the Transmission Control Protocol / Internet Protocol (TCP/IP) (Leiner et al., 1997). This protocol directs the data packets to travel from the source to the destination.

In 1995, Vocaltech Inc., introduced VoIP and their Internet phone allowed the users to communicate via computers (Schulzrinne & Rosenberg, 1999). VoIP helped

to transmit multimedia data in a single infrastructure. VoIP calls are made using peer to peer VoIP through computer, IP telephony as well as traditional phones. It paved the way for monetary savings by lowering the cost of user services such as unlimited long distance international calls as the data is transmitted through Internet. The call that is dependent on bandwidth increased the flexibility and popularity of VoIP as stated in (Zhao & Ansari, 2012). It provides better Quality of Service (QoS) than PSTN at comparatively less cost. The local call rates are reduced up to 40% and international call rates are reduced up to 90% using VoIP technology as stated in (Heckstall 2016). Hence, the voice network along with data network is integrated to lower the overall management cost and effort.

In the early days, VoIP was unpopular due to its lack of high speed and low-cost Internet. As Internet connection became faster and cheaper, voice or data packet were used instead of PSTN. Furthermore, VoIP leverages on existing Internet infrastructure and does not require additional infrastructure requirements which made VoIP popular. In 1998, VoIP used less than 1% of all voice calls. There was a slow increase in VoIP users, which accounted for 3% in 2000 and raised to 25% by 2003 (Hallock, 2004). In 2013, the Point Topic organization tracked the global VoIP operators and recorded a total of 155.2 million global subscribers (Topic 2013). Subscriptions for VoIP have increased substantially worldwide (Wansink 2016) and is predicted to grow further by 2020. IBISWorld states that the VoIP industry's contribution is expected to increase 15.3% every year until 2017 as stated in (IBIS 2015). Due to this estimated increase in the near future, the flexibility for both residential customers and businesses in VoIP technology will substantially increase. Figure 1.1 shows the growth of VoIP subscribers indicated by Statista (Topic 2013).

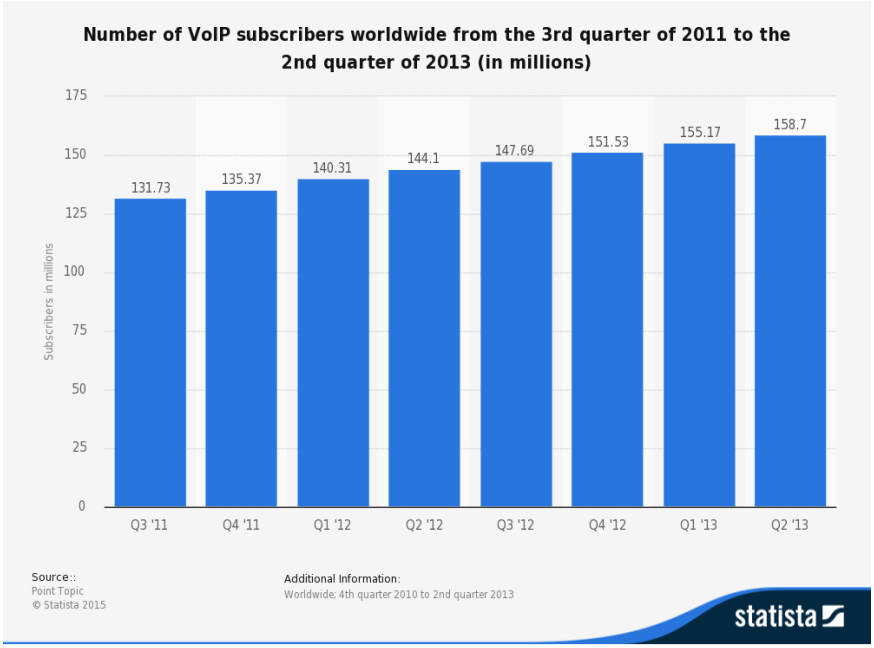

Figure 1.1: Growth of VoIP Subscribers

The survey conducted by (Wansink 2016) states that the fall of fixed-line PSTN subscriptions is compensated by the rise of the VoIP subscriber base. Another advantage of VoIP is phone portability where the device uses the same number all over the world. But in a legacy phone, the device is assigned a fixed number for a fixed location and this device number change when moved to a different location. The survey reported by Telco (Global, Services, & Report, 2015) states that the migration of PSTN to VoIP is inevitable due to the decline of PSTN revenue and growth of VoIP subscribers.

As with any services on the Internet, VoIP too suffers from security issues due to the protocol design and components of the network which embraces the VoIP services (Anwar et al., 2008). The first and foremost concern about communication protocol were reliability and efficiency and security concerns were given less consideration. In July 2016, AT&T identified and reported malicious scans which

reached more than 30 billion and 245,000 of them were DDoS alerts (Jason Porter, 2016).

1.2 Security Issues faced by VoIP

Many existing VoIP devices and programs have vulnerable spots for intruders with a wide attack space. Confidentiality, Integrity and Availability (CIA) must have a high priority while considering the security issues (Coulibaly & Hao Liu, 2010). Various threats affect the CIA of VoIP systems. VoIP switches are more vulnerable to a wide range of network attacks like DoS, DDoS, eavesdropping, man in the middle attack as the Internet being the transition medium among the internal and external users (McGann & Sicker, 2005). The vulnerability is due to the lack of adequate control policies (Ur Rehman & Abbasi, 2014). Flood-based DoS and DDoS attack (Cha, Choi, & Cho, 2007; Hussain, Djahel, Zhang, & Naït-Abdesselam, 2015) have been identified as major threats among the other attacks.

1.2.1 Malformed Message Attack

A SIP message consists of header field and the message body. Malformed Message Attack uses the vulnerability of text-based protocol (Su & Tsai, 2015). These attackers manipulate Session Initiation Protocol (SIP) header deletion, overflow-space, non-ASCII code to malfunction the proxy server or end user's terminals (Sonkar, Singh et al. 2012). The attacker uses the malformed SIP Invite message to discover security flaws in the victim's system. Figure 1.2 shows the absence of Request-URI followed by Invite method as per the standard SIP protocol syntax. The depicted Invite message is invalid as it is given null in the first line which violates SIP protocol specification.

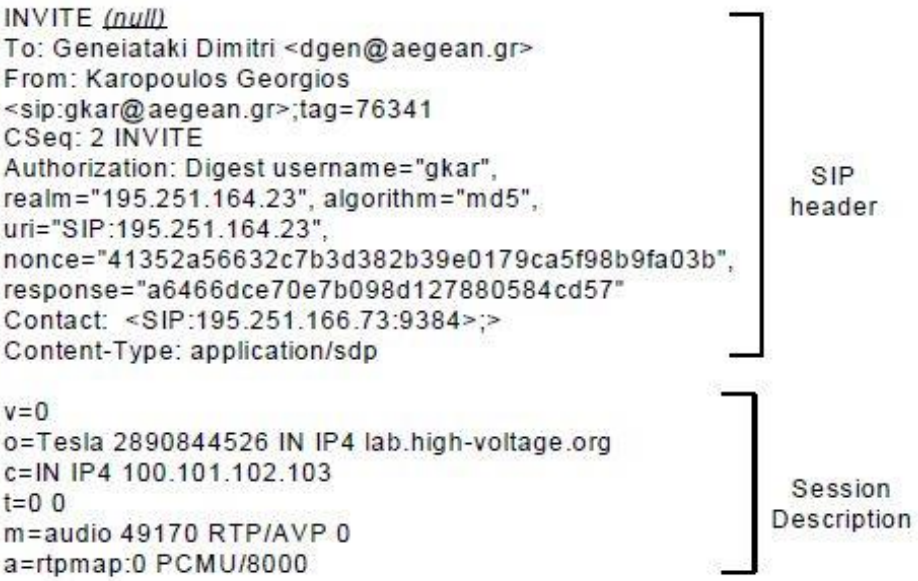

Figure 1.2: Malformed Message Attack

1.2.2 Spoofing Attack

Spoofing attack involves an attacker masquerading as a legitimate user. Fraudulent emails, fake websites and wireless access point are provided to trick victims in collecting their personal data (Jayamali et al., 2016).

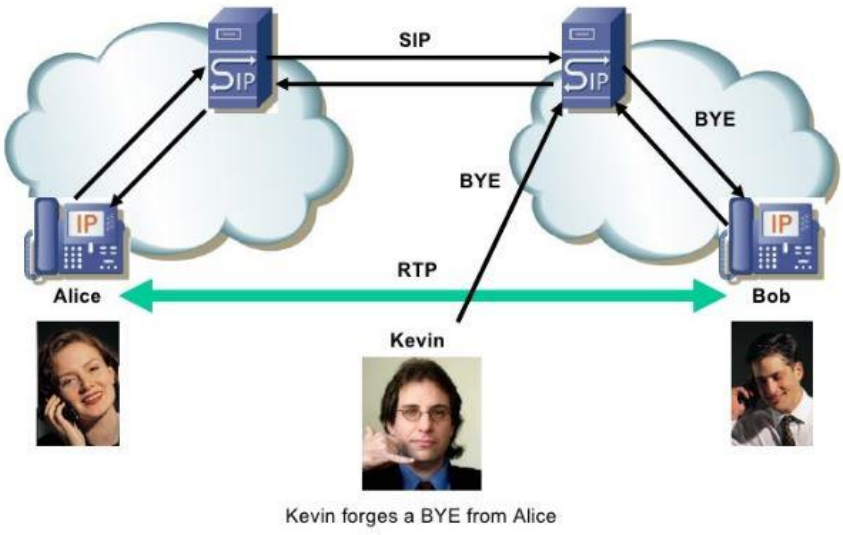

Figure 1.3: Spoofing Attack

Spoofed BYE messages can be used to terminate ongoing sessions between the users (Sonkar, Singh et al. 2012). In Figure 1.3, the attacker (Kevin) forges SIP BYE message from the caller (Alice). Now the attacker acts as a legitimate user and send BYE message to callee (Bob) thereby terminating the legitimate session between the legitimate caller and callee.

1.2.3 Eavesdropping Attack

Eavesdropping affects the confidentiality of the VoIP user agent. The attacker secretly listens to the signalling and data streams between the user agents (Kolhar, Alameen, & Gulam, 2017) by sniffing the conversation between them. They can reply to the conversation and obtain secured information as shown in Figure 1.4.

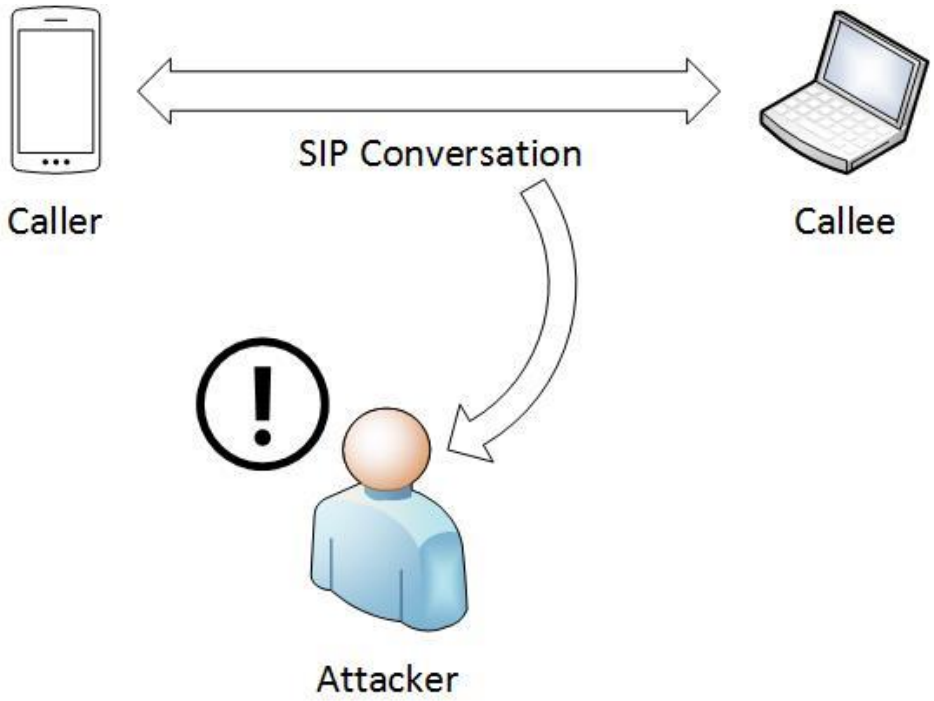

Figure 1.4: Eavesdropping Attack

1.2.4 Man in the Middle (MITM) Attack

The MITM attack affects the confidentiality and integrity of user agents. The attackers listen to the conversation between the two user agents and masquerade on both the side as a legitimate user (Conti, Dragoni, & Lesyk, 2016). In Figure 1.5, the attacker makes new independent connections with the caller and callee. The private information is relayed between the end users through the attacker. Hence, the attacker controls the entire private conversation neglecting the old conversation between the caller and callee.

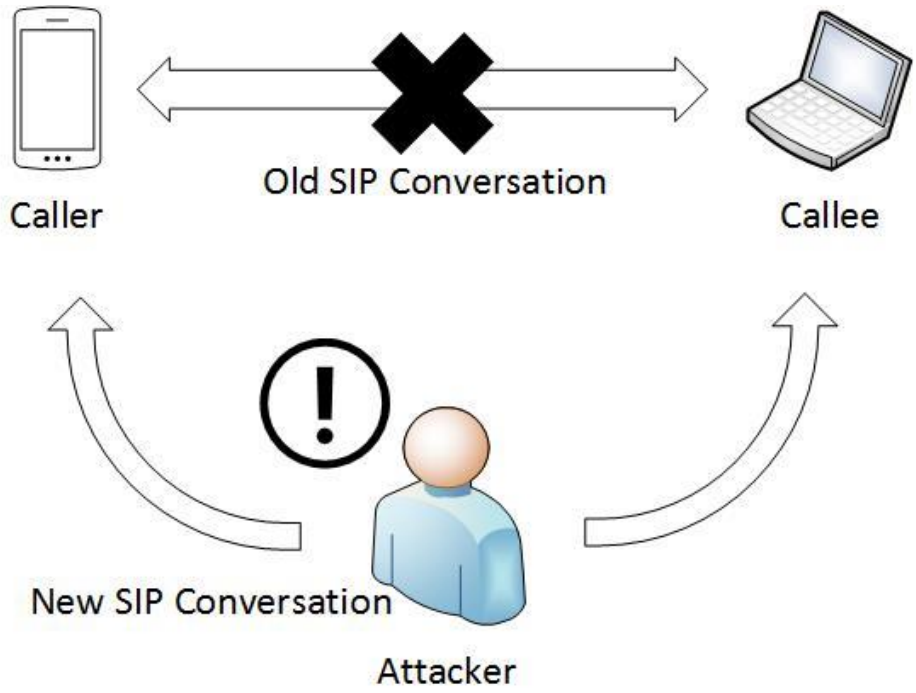

Figure 1.5: Man in the Middle Attack

1.2.5 Spam over Internet Telephony (SPIT) Attack

SPIT involves the generation of unsolicited advertisements of pre-recorded messages and unwanted calls to the users as shown in Figure 1.6. The attackers have created VoIP bots (M. A. Akbar & Farooq, 2014) capable of harvesting data and advertising

dubious services at low cost. In terms of bandwidth and cost, SPIT is a potential risk (Ekekwe and Maduka 2007) which utilizes the bandwidth of the VoIP users.

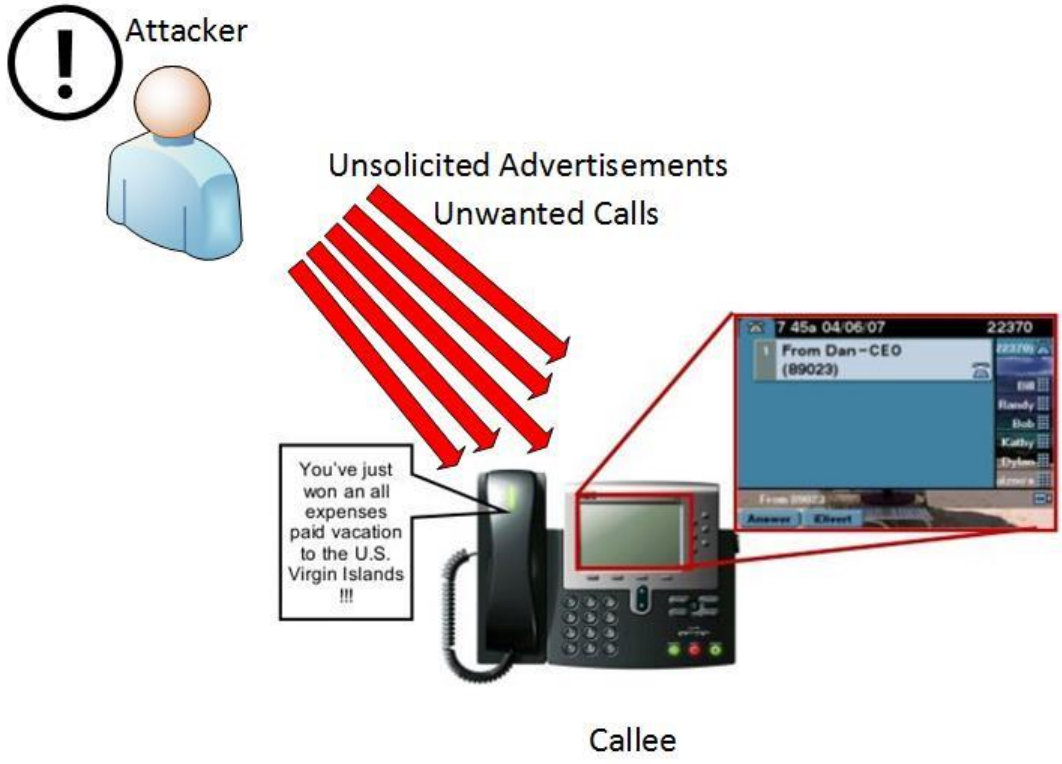

Figure 1.6: SPIT Attack

1.2.6 Call Hijacking Attack

Call Hijacking involves the attacker impersonating a user agent by spoofing the identity of the phone device (Butcher, Li, & Guo, 2007). The VoIP device is setup with the victim's identity. Hence, incoming calls can be redirected to the attacker's phone as shown in Figure 1.7. The attacker hijacks the call between user agent A and user agent B. Thereby, the attacker sends 301 moved permanently SIP response message to the user agent A along with the attacker's own forwarding address. After which the conversation will be between the attacker and user agent A. Registration hijacking involves an attacker replacing the legitimate registration with false data

(Rasol, Al Kasasbeh, & Al Adwan, 2016). Thus, future calls to the legitimate users are redirected to the attacker using false registration message.

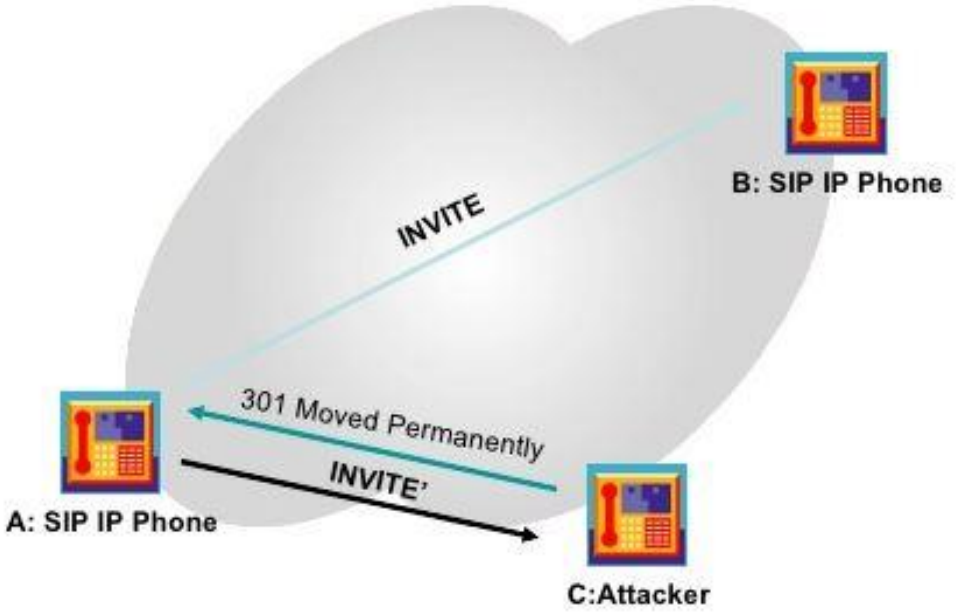

Figure 1.7: Call Hijacking Attack

1.2.7 Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack

Flooding attacks involve SIP phones generating massive number of SIP messages to a specific user agent within a short period. This hampers the services rendered by the user agent. Invite flooding is one of the more annoying attack for VoIP users. The major problem based on availability is DoS. VoIP network is susceptible to DoS attacks which degrades QoS quickly to an unacceptable level (Koutepas, Stamatelopoulos, & Maglaris, 2004). In DoS, VoIP telephony services are interrupted by the attacker due to excessive requests from a source agent to the destination user agent or the SIP server. In DDoS, a number of source user agent acts as botnets. These botnets are controlled by the attackers which can flood the destination user agent with minimal request from each.

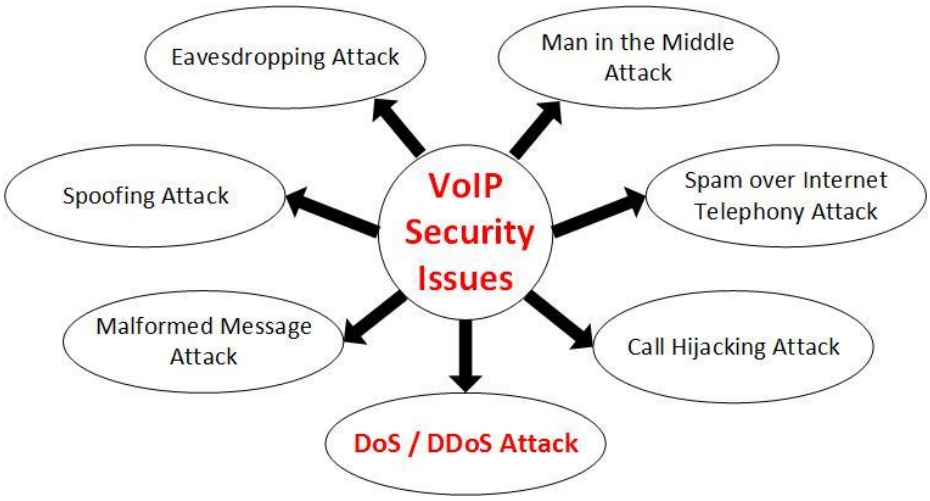

Figure 1.8: VoIP Security Threats

Hence DoS and DDoS try to disrupt legitimate user's services causing service unavailability (Zeb, Baig, & Asif, 2015). Figure 1.8 depicts the different types of VoIP security threats. Based on the above threats, it is clearly seen that DoS and DDoS are the most vulnerable attack in real-time VoIP system.

1.3 Problem Statement

The motive of the attacker is to deny the service delivered by the VoIP server to its end users. The service is denied by exhausting the resources of the SIP server like bandwidth, CPU and RAM. Moreover, a DDoS attack damages the SIP server's resource as VoIP is a real-time service. Thus, the excessive traffic generated by the attacker lead to service unavailability.

The distributed flooding of SIP Invite packet provides new challenges to mitigate DDoS attack. As a result, a better DDoS mitigation solution is required to protect the users. Therefore, this thesis addresses the following issues:

1. Various proposed DDoS detection and mitigation techniques fail to distinguish between the DDoS attack and flash crowds from legitimate users (Jeyanthi &

Sriman, 2012), which leads to monetary issues to the business in both private and corporate sectors.

2. Most of the existing detection and mitigation techniques were tested in simulated environment and not in test bed environment.

3. Existing detection and mitigation techniques are not effective in addressing DDoS attack since these methods detect the attack and manipulate only after the attack session reaches the SIP server.

1.4 Thesis Aim and Objectives

The main aim of this research is to detect DDoS attack on SIP server efficiently to ensure the service disruption due to such attacks can be reduced. This is culminated by the following objectives:

- To propose a Hellinger distance based algorithm to detect DDoS attack.
- To propose an approach which distinguishes the DDoS attack traffic and the flash crowds from legitimate users.
- To evaluate the effectiveness of the proposed algorithm during DDoS attack in terms of detection accuracy and false positive rate.

1.5 Research Steps

The key objective of this thesis is to design a behaviour algorithm to detect and mitigate DDoS attack effectively. To achieve this goal, we performed number of key research steps as illustrated in Figure 1.9.

In the first phase, the research problem is systematically demarcated and evaluated by exploring the concept of VoIP. The research objectives and scopes are formulated by identifying the problems in VoIP Security especially DDoS attack.

In the second phase, critical review of the existing DDoS detection and mitigation techniques discover the requirements of these techniques. Furthermore, the strength and limitations are formulated by investigating existing techniques against DDoS attack in VoIP environment.

In the third phase, a VoIP environment is designed to study the impact of DDoS attack. Then, a algorithm is designed and developed to detect DDoS attack after obtaining information from the previous step. The design of the modules in the proposed algorithm is based on statistical analysis techniques which is integrated into VoIP environment. This algorithm comprises of four phases, namely Data Preparation, Feature Extraction, Anomaly Detection and DDoS Mitigation.

In the fourth phase, the proposed algorithm is implemented in a test bed environment. The effectiveness of the proposed algorithm and its detection accuracy is tested and evaluated under different incoming SIP traffic rate.

In the final phase, the results obtained from the evaluation process is justified. Finally, the output of all the phase is finalized and documented.

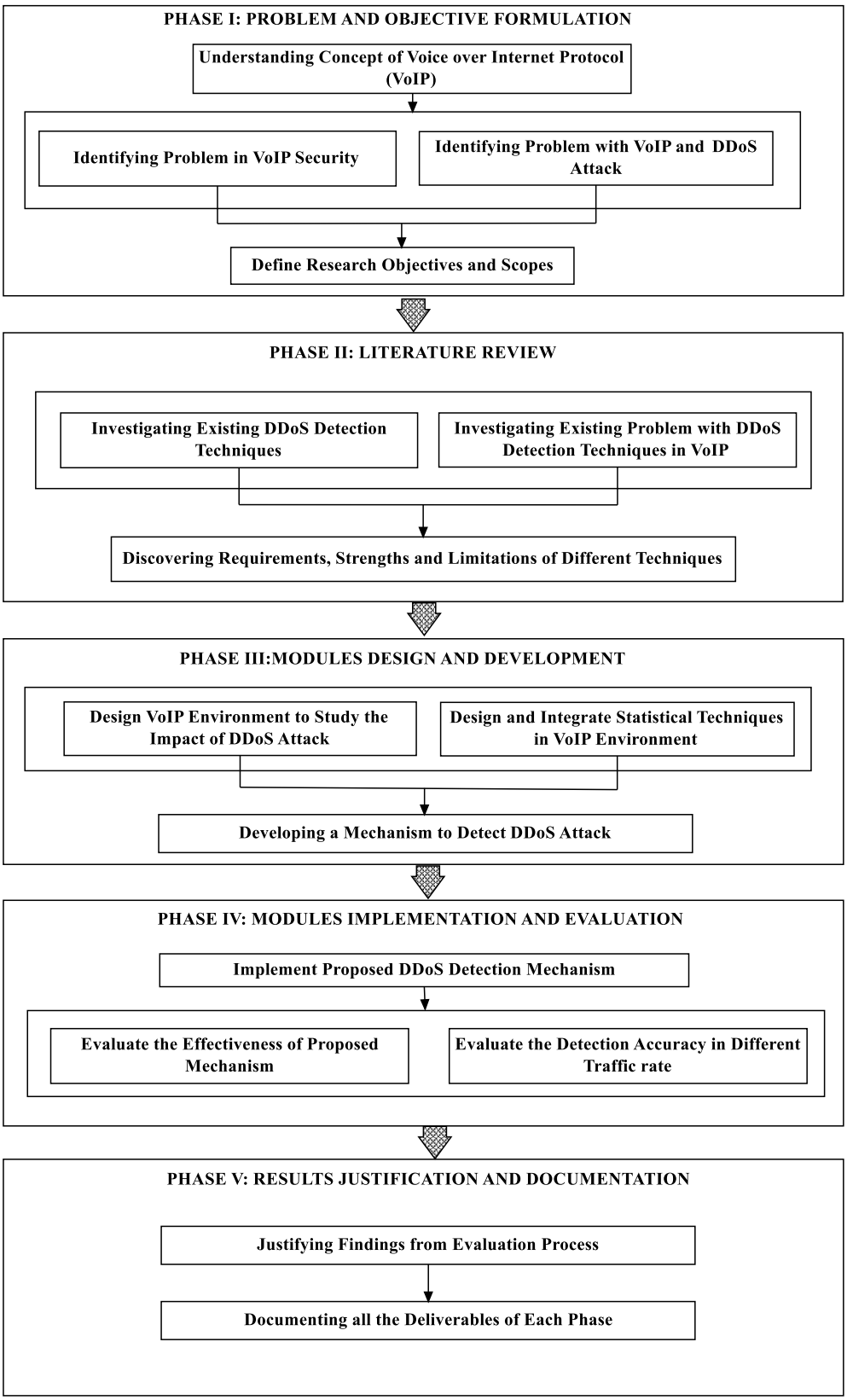

Figure 1.9: Research Steps

1.6 Research Scope and Limitation

The proposed algorithm in this thesis is based on signalling DDoS attack at the application layer in the IPv4 VoIP environment. The scope of this research is limited to the detection of flood-based SIP Invite DDoS attack on VoIP servers. Multi attribute attacks like BYE flooding attacks are not considered in this research. The scope of the proposed DDoS detection and mitigation algorithm is based on the following assumptions:

1. The proposed algorithm assumes the optimal feature selection as connections per second.
2. The proposed algorithm bypasses the least number of DDoS SIP packets.
3. The attacker's objective is to generate a high or low rate DDoS attack with a duration of more than one second against the VoIP server.

1.7 Research Contribution

The proposed algorithm can detect and mitigate DDoS attack in VoIP with improved detection accuracy. The main contributions of this thesis can be summarized as:

- Implement the Queue steps to flush out the blacklist table under normal traffic.
- Design and implement the anomaly analyser module to analyse the anomalies from the incoming SIP packets and calculate dynamic threshold.
- Design and implement the anomaly detector module to detect the SIP DDoS attack packets from flash crowds corresponding to legitimate users.
- To evaluate the experiment in the real VoIP environment, a private test-bed is required because DDoS attacks on a production environment may lead to disruption of services.

1.8 Thesis Organization

This thesis is organized into six interconnected chapters as follows.

Chapter 1 presents the objective of this thesis and provide brief background on the security issues in VoIP. The problem statement, objective, scope, limitations and research contributions are also provided in this chapter. The security issues on VoIP and the concerns related with it are also discussed.

Chapter 2 provides the background of VoIP, SIP and Dos/DDoS attack. This chapter discusses and compares the most related research works in detecting and mitigating DDoS attack in VoIP. Furthermore, this chapter argues on the breaches in the research that has been accomplished so far and reports the necessity to detect and mitigate DDoS attack in real time VoIP systems.

Chapter 3 introduces the methodology and the design of proposed framework. Modules involved in designing this algorithm have also been discussed. The behaviour-based algorithm for the detection and mitigation of DDoS attack in VoIP is discussed in detail.

Chapter 4 discusses the overview of test bed setup. This chapter presents the implementation details of the proposed algorithm along with the tools and technologies used to run the experiments.

Chapter 5 covers in-depth analysis of the proposed algorithm's detection accuracy through detailed experiments. The comparison results between the proposed algorithm and other algorithms are stated in this chapter.

Chapter 6 summarizes the entire discussions and concludes the research covered in this thesis. Some future directives are also highlighted in this chapter.

CHAPTER 2

BACKGROUND AND RELATED WORK

2.1 Introduction to VoIP Architecture

The components of VoIP include the source agent, ATA (Analog Telephone Adapter), SIP server, gateway and destination agent as in (Miliefsky, 2010). The VoIP architecture is shown in Figure 2.1.

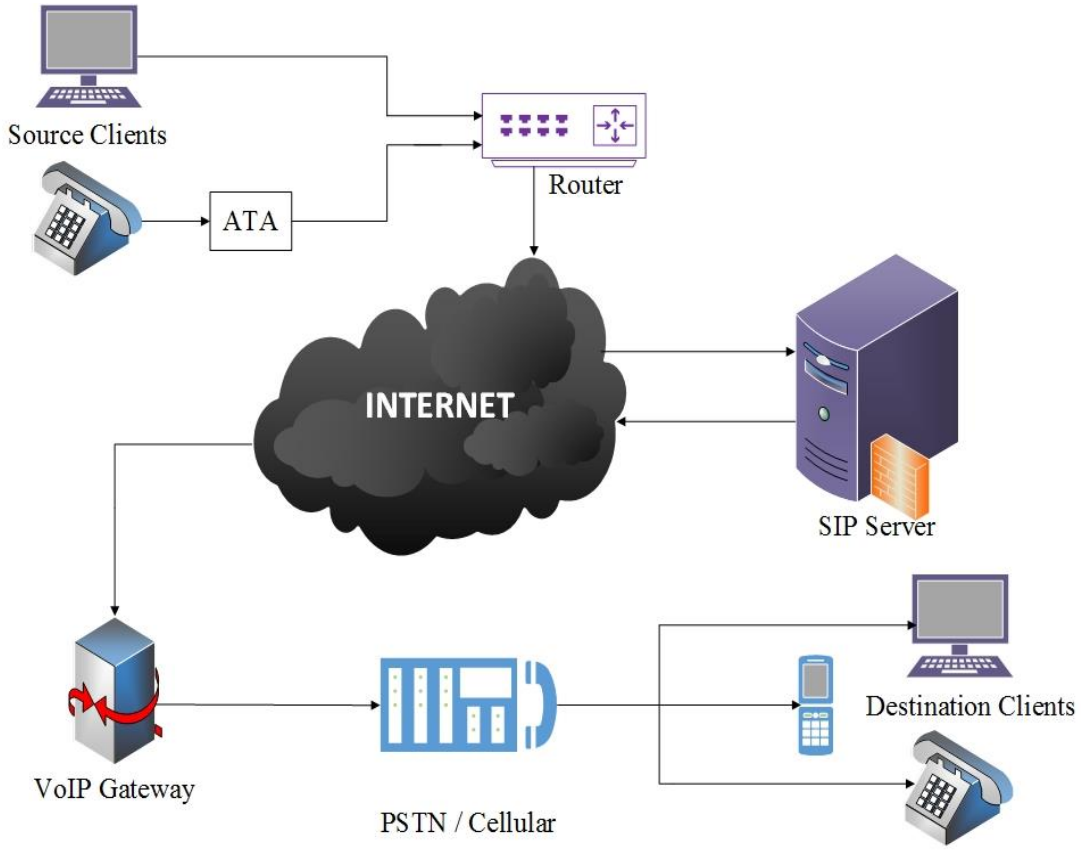

Figure 2.1: VoIP Architecture

The voice signal from the source user agent is transmitted to ATA and then to the router to generate IP packets. A dial tone from ATA signifies connection to the

Internet. When a number is dialed, the tone is converted to digital data. The packets passing through the IP network reach the SIP server. The SIP server locates the destination user agent with the help of a location server. Here the phone number is checked for its validity and then they are mapped to an IP address. The packets are then passed on to the termination carrier which acts as the gateway to be connected to the destination user agent. Thus, a session is established between the two agents. To communicate between these agents, a uniform protocol should be used among them. The communication among the source user agent, SIP server and the destination user agent is linked by the SIP protocol. The ATA at the receiver's end converts the packets back to analogue audio signals. The session is terminated by hanging up the phone.

2.1.1 Importance of VoIP

VoIP, which is employed for transferring voice data, is deployed internally for telephone services in a wide range of the military and government departments. It uses packet switched network carrying multiple calls on the same space (Keromytis, 2012). For instance, an IP network allows 5 to 10 times the amount of voice calls over the provided bandwidth. VoIP streamlines several calls through a circuit switch and then into an IP gateway reducing the consumption of bandwidth. On the other hand, PSTN uses circuit switching which occupies only one call per space. This requires a dedicated line for telecommunication activity (Meisel & Needles, 2005). Skype, Hangouts, Facebook, Myspace, WhatsApp and WeChat are examples of free Internet phone services (H. J. Abdelnur, State, & Festor, 2007). DOTA, a real-time game played via the Internet, uses VoIP technology. This helps the players to interact directly with other players as they play.

Traditional phone can be connected to the Internet via ATA. The analogue signal from the telephone is converted to digital signals which is sent to the Internet and vice versa. IP phones being used as a VoIP device differ from a traditional phone in the connector which uses a RJ-45 Ethernet connector. But the traditional phone is provided with RJ-11 phone connector for voice services. Hence, IP phones can be connected to the modem directly. Softphones are the software in the computer which make VoIP communication easier irrespective of the distance. Several free softwares are available for placing a VoIP call.

VoIP can be deployed on a private network or on a public network. In private networks, PSTN and VPN integrate with VoIP. Users can be connected to this network internally but not externally, thus, avoiding attacks from external users. However, they are susceptible to internal attacks. In public network services, the users can access the system via Internet. This deployment is vulnerable to flooding issues from both internal users as well as external users. The topological implementation differs on theses VoIP deployments, but the attack algorithm and impact remains constant in both the systems. The SIP proxy server forwards SIP requests to the end users and receives responses from the corresponding users. The effect of SIP flooding on a SIP server was examined first. This research detects and mitigates SIP flooding attacks using the proposed algorithm to deliver better service to the end users. The VoIP test bed with the proposed algorithm in private network was used to analyse and verify the effectiveness of a SIP proxy server.

2.1.2 VoIP Protocols

VoIP technology consists of signalling and data transfer protocols. The functions of signalling protocols are to set up, manage and terminate a session. The supporting

signalling protocols are H.323, SIP, Media Gateway Controller Protocol (MGCP) and Stream Control Transport Protocol (SCTP). The data transmission protocols oversee transmitting voice data. The data transfer protocols are Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP). The widely-used protocols are H.323 and SIP which are discussed in detail in this thesis.

H.323: H.323 is a recommendation set from the International Telecommunication Union (ITU) (H. Abdelnur, Cridlig, & Festor, 2006). It is a protocol suite designed for the transfer of IP based multimedia communications in real time. They consist of a family of core protocols transported over TCP or UDP protocols (McNeill, Liu et al. 2006). H.225 helps in registration, admission and call signalling. H.245 is responsible for establishing and controlling the media sessions. It is also responsible for capacity and codec negotiation. T.120 is used in conferencing applications. The audio and video codec are defined by G.7xx series and H.26x series respectively. The media data are transmitted using RTP. RTCP is used for controlling RTP sessions (H. Schulzrinne, S. Casner, R. Frederick, 2003).

Drawbacks of H.323: The main drawback of H.323 is its lack of scalability. H.323 locates users across zones. But in case of multiple domains, performance of loop detection is void, which leads to scalability issues. Development of supplementary extensions is challenging for this protocol. With several protocol components, H.323 faces complexity and complicates firewall traversal (Shore 2000).

SIP: The standardization of SIP by Internet Engineering Task Force (IETF) is used by VoIP and other multimedia bidirectional communication like voice calls, video conferencing and data sharing (Rosenberg & Schulzrinne, 2002). SIP is an application layer protocol which creates, modifies and terminates sessions in VoIP

communications. Since SIP is a simple and flexible protocol, features can be added. It allows multiple multimedia sessions in one call as seen in online gaming, instant messaging and various services. The Uniform Resource Locators (URL) addressing scheme in SIP does not depend on the physical location (Berners-Lee, Masinter et al. 1994). They are addressed by either a phone number, an IP address, or an e-mail address. It is similar to the HTTP web protocol as the messages comprise of headers and body message. The default port for SIP is 5060 for either TCP or UDP. The user datagram protocol (UDP) over the transmission control protocol (TCP) at the transport layer is favoured by SIP because of the connection orientation of SIP and the simple behaviour of UDP as in (Information Sciences Institute University of Southern California, 1981).

2.2 SIP Architecture

The three major components in a SIP communication are User Agent Client (UAC), the SIP proxy server and User Agent Server (UAS). The main network elements involved in the SIP communications are described in Figure 2.2. The User agent (UA) generates or receives SIP messages. It acts as a UAC for transmitting SIP messages. The receiver act as UAS. The SIP client acts as both a SIP UAC and SIP UAS. The SIP request from user agents are received by the SIP server and forwards them to the corresponding host. The Registrar server processes REGISTER messages and then the user's URI are mapped to the present location of the user. The registrar server can be placed separately or inside the SIP proxy server. The Location server helps to store the location of registered users. The proxy finds the user's location using the location and registrar server.

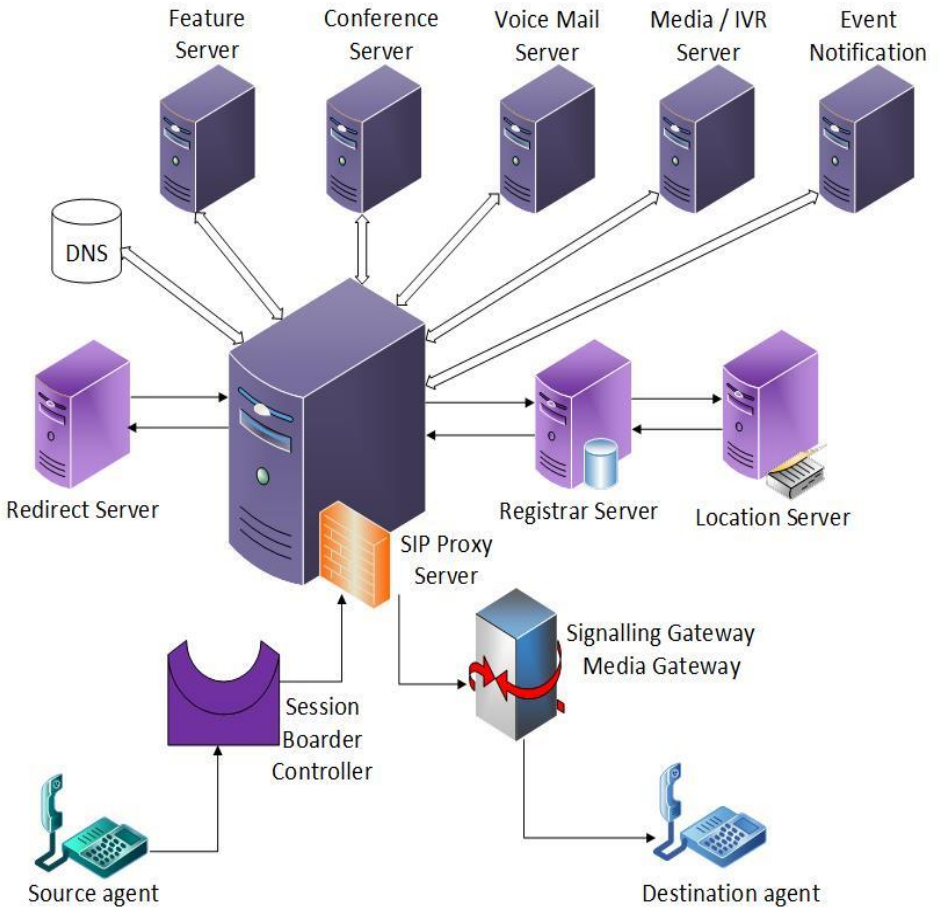

Figure 2.2: SIP Architecture

The Feature servers provide special treatment to enhance the communications experience. The proxy server uses special routing rules to control the SIP feature. The Media server record media streams, play back recorded media, collect dual tone multi frequency (DTMF) input from the user. It uses a media bridge that mixes multiple media streams as in conferencing. When a user is on a different domain, the calls are connected using a Domain Name System (DNS). The redirect server returns a forwarding address when a user is moved temporarily from the current domain to the next domain. Session Border Controller (SBC) in SIP protects the internal network from any malicious attack. Signalling and Media Gateway enables non-SIP

interactions, while Signalling Gateway translates signalling protocol and the Media Gateway transcodes media data.

2.2.1 SIP Messages

The SIP components are provided with a SIP address which resembles an email address. This address contains a username followed by a hostname. SIP operations are performed between them by exchanging messages. SIP messages used for communication purpose have message header similar to HTTP (Fielding, Gettys et al. 1999). These messages are in the form of request and response as shown in Figure 2.3.

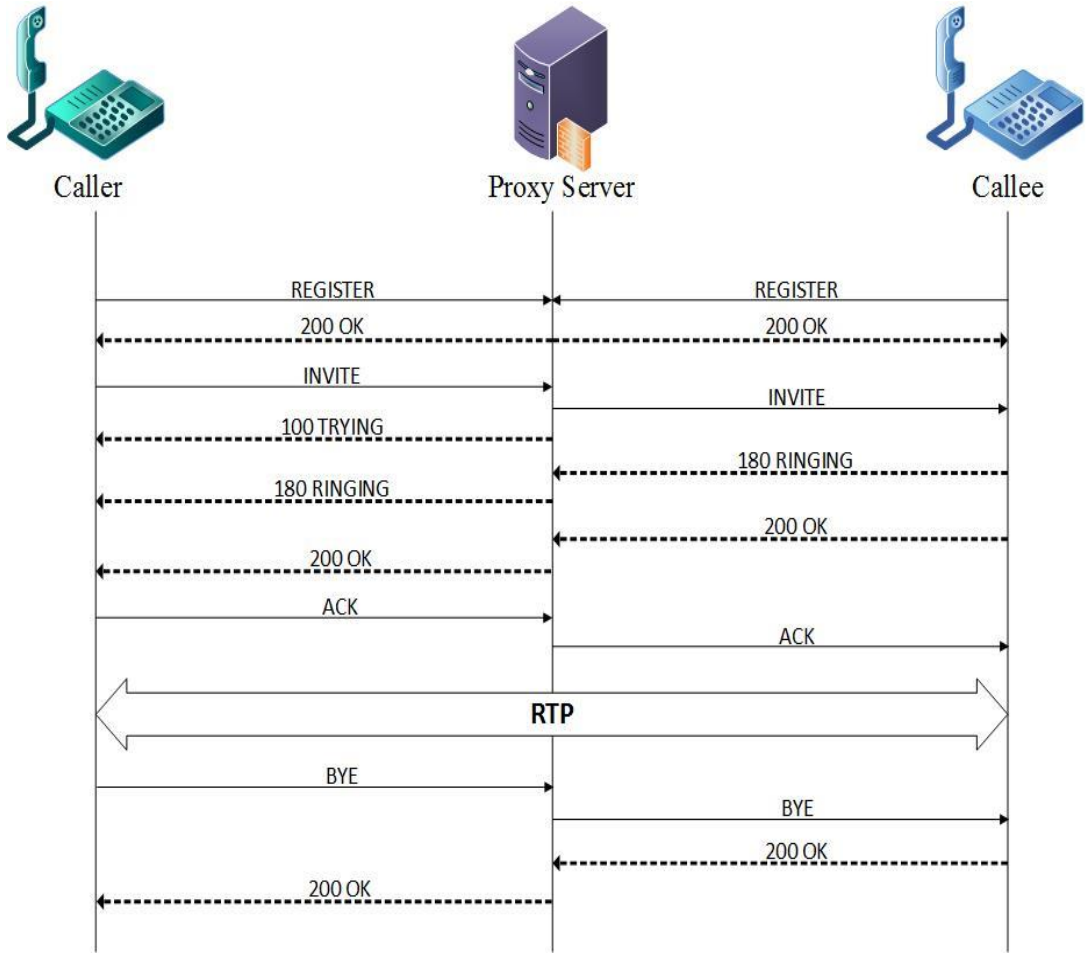

Figure 2.3: SIP Messages

UAC uses a request message and UAS uses a response message. The SIP request messages are REGISTER, INVITE, ACK, CANCEL, BYE, and OPTIONS. The SIP response messages are PROVISIONAL (1XX), SUCCESS (2XX), REDIRECTION (3XX), CLIENT ERROR (4XX), SERVER ERROR (5XX) and GLOBAL FAILURE (6XX). SIP messages in the form of a text-based presentation are vulnerable to attacks.

2.3 Denial of Service Attack

The normal services on a phone system can be disrupted by a DoS attack (Sisalem, Kuthan, & Ehlert, 2006). The DoS attack scenario is depicted in Figure 2.4. The attacker can attack the user agent or the SIP server.

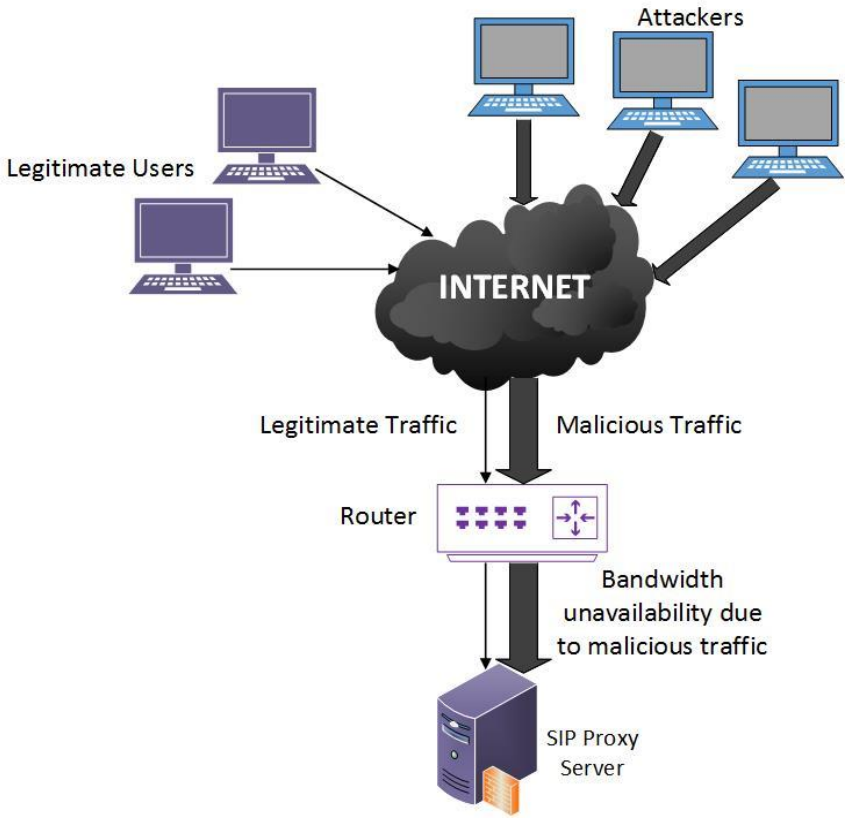

Figure 2.4: DoS Attack Scenario

When the attacker attacks on a particular user, the user is unable to respond to the calls. Similarly, when the attacker attacks the SIP server, the entire network is