A DISTRIBUTED ARCHITECTURE FOR SPAM MITIGATION ON 4G MOBILE NETWORKS

ELIAS BOU HARB

A THESIS

IN THE

CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING (CIISE)

PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF APPLIED SCIENCE (INFORMATION SYSTEMS SECURITY)

CONCORDIA UNIVERSITY

MONTRÉAL, QUÉBEC, CANADA

SEPTEMBER 2011

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Elias Bou Harb**

Entitled: **A Distributed Architecture for Spam Mitigation on 4G Mobile Networks**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Information Systems Security)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining commitee:

Chair
Dr. J. Bentahar

Supervisor
Dr. C. Assi

Supervisor
Dr. M. Debbabi

CIISE Examiner
Dr. R. Glitho

External Examiner (ECE)
Dr. A. Agarwal

Approved by

Dr. Robin Drew, Dean

Faculty of Engineering and Computer Science

Abstract

A Distributed Architecture for Spam Mitigation on 4G Mobile Networks

Elias Bou Harb

The 4G of mobile networks is considered a technology-opportunistic and user-centric system combining the economical and technological advantages of various transmission technologies. Part of its new architecture dubbed as the System Architecture Evolution, 4G mobile networks will implement an evolved packet core. Although this will provide various critical advantages, it will however expose telecom networks to serious IP-based attacks. One often adopted solution by the industry to mitigate such attacks is based on a centralized security architecture. This centralized approach nonetheless, requires large processing resources to handle huge amount of traffic, which results in a significant over dimensioning problem in the centralized nodes causing this approach to fail from achieving its security task.

In this thesis, we primarily contribute by highlighting on two Spam flooding attacks, namely RTP VoIP SPIT and SMTP SPAM and demonstrating, through simulations and comparisons, their feasibility and DoS impact on 4G mobile networks and subsequent effects on mobile network operators. We further contribute by proposing a distributed architecture on the mobile architecture that is secure by mitigating those attacks, efficient by solving the over dimensioning problem and cost-effective by utilizing ‘off the shelf’ low-cost hardware in the distributed nodes. Through additional simulation and analysis, we reveal the viability and effectiveness of our approach.

I dedicate this work to my family, especially my mother.

It would have been extremely hard for me to leave home and come here to pursue my future without her blessings, support and love.

Acknowledgments

In the beginning, I would like to thank my supervisor Dr. Chadi Assi for his supervision and support. If it was not for him, I would not have been at Concordia University in the first place. He believed in me and trusted me that I would be a disciplined productive student and I can not thank him enough for that. Although he was on a sabbatical leave for the past two years, he made sure that we keep in touch for updates and provided constructive feedback during meetings. He always pushed me to be the best that I can be and without his support and guidance for the past two years, I would not have been able to write this thesis. Basically, I consider Dr. Assi as my idol, my friend, and my wise older brother.

My utmost appreciation and gratefulness also goes to my co-supervisor Professor Mourad Debbabi. I have always appreciated what Dr. Debbabi does for our Institute, and his advices for me throughout the past two years were vital. He had confidence in me and I'll always be thankful for that. I can never forget his words when he told me "Elias, you are smart and I know you are good". He said that to greatly motivate me and to encourage me to be always energetic and productive. I'll never forget his charisma, determination and humbleness. I know I was lucky to know a person such as Professor Debbabi.

Of course, I would also like to express my appreciation to Dr. Makan Pourzandi, who is a full time researcher at Ericsson, Canada and an adjunct assistant professor at Concordia University. Dr. Pourzandi was our guide and leader in this research work and he was a perfect example of a professor that is successful in both academia and industry.

I would also like to acknowledge the work of Mr. Todd Wease, who is the senior software engineer at Sourcefire, the company that developed Snort. Mr. Wease was a great support for our research team and he answered a lot of the critical questions we had when we were working with Snort in the profiling phase of this research project.

I won't forget my research mate, Feras Al Jumah, who effectively contributed towards this project and provided very creative and constructive ideas.
I would also like to express my warmest gratitude to the entire Concordia University family for being helpful, supportive and professional for the past two years.

Finally, last but not least, many thanks to my best friends Hagop Koulakezian, Saleem Khoury and Claude Fachkha for their support and friendship, also to the members of my closest social environment and of course my beloved family.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Thesis Introduction

Cellular or mobile networks have enabled impressive advances, trends and changes in telecommunications over the last two decades, and mobile operators have significantly matured to dominate the industry, providing their subscribers an extremely rich service package that competes with their wire-line competitors in addition to providing mobility. Nevertheless, with the broadband market success in cable, xDSL and Wi-Fi, the competitive landscape is shifting.

Even though 3G technologies deliver considerably higher bit rates than 2G technologies and contribute to the average revenue per user growth for wireless data services, there is still more possibilities for wireless operators to capitalize on the ever increasing demand for wireless broadband, as well as lower latency and increased throughput services. Figure 1.1 reveals that broadband subscriptions are expected to reach 3.4 billion by 2014 and about 80% of these consumers will use mobile broadband [1]. Consequently, there is a mounting revenue opportunity from an expanding

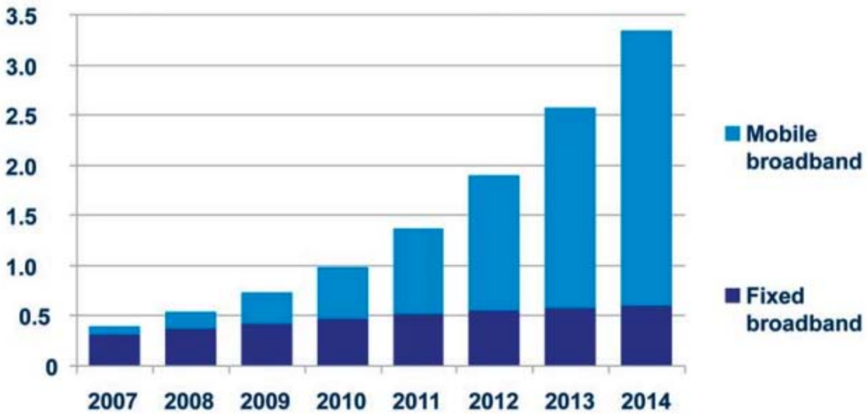


Figure 1.1: Broadband growth 2007–2014 [1]

pool of undeserved consumers that can only be satisfied with next generation networks. Indeed, the solution is the Long Term Evolution (LTE) Project 3GPP [3], dubbed as the next-generation network beyond 3G. The fourth generation of mobile networks will be a technology-opportunistic and user-centric system combining the economical and technological advantages of various transmission technologies to provide a ubiquitous, context-aware adaptive service. Besides offering fixed to mobile migrations of Internet applications such as voice over Internet protocol, video streaming, music downloading, pictures uploading, mobile TV and several others, LTE 4G mobile networks will as well provide the capability to support an explosion in demand for connectivity from a new generation of consumer equipment tailored specifically to those new innovative mobile applications.

Part of its new architecture that is branded as the System Architecture Evolution (SAE), LTE 4G mobile networks will implement a packet switched approach in its evolved network core. This all IP approach, however, is a double edged sword. On one hand, it will enable the support of universal IP access from any network to and from LTE 4G networks in addition to providing various critical advantages including multi-megabit bandwidth, seamless and improved mobility, extensive quality of service and significant latency reduction among various others. On the other hand, it will pave the way to serious security concerns since theoretically, any security attack that is feasible on an IP network will as well be viable on 4G mobile networks.

Two important application services that may be vulnerable to such attacks on 4G mobile networks are VoIP and SMTP which are introduced and discussed next.

1.2 VoIP and SPIT Flooding

Voice over Internet protocol (VoIP), an ever flourishing supported and provided application service on those networks, refers to the technology that enables routing of voice conversations over a network. It is governed by certain protocols for signaling and transport such as the Session Initiation Protocol (SIP) [4] and the Real Time Protocol (RTP) [5]. It is disclosed that 45% of today's Internet traffic is VoIP (voice & video) and this number is anticipated to increase to 60% in 2016 [6]. Moreover, with the booming of mobile Internet broadband, an increasing number of devices such as tablets (ipads/playbooks), netbooks and handhelds is connected to high speed mobile Internet through 3G and soon 4G USB sticks or built-in modems. These devices in addition to smart-phones, will contribute in increasing the demand for VoIP in 4G mobile networks. These facts convey that VoIP is and will be playing an increasingly critical role in communications that attracts both businesses and end users. However, in a recent report [7], Cisco Systems predicted that VoIP abuse will grow significantly in the very near future. The report highlights the facts that VoIP is widely deployed, may not be well protected and possibly there exist various methods to abuse it. A specific misdemeanor against VoIP is coined SPAM Over Internet Telephony (SPIT) [8]. SPIT refers to unsolicited calls intended for advertising, social engineering and more severely bandwidth and processing utilization. As mentioned earlier, the fact that 4G will offer increased bandwidth coupled with the flourishing of various user equipments, is expected to make VoIP SPIT a very serious threat in the near future. The latter statement is greatly supported by 3GPP in their technical report [9], where they quantified that approximately 250 GB of SPIT traffic per month could be generated from only one SPIT bot. In a typical SPIT scenario, the Spitter fabricates an INVITE request carrying an SDP (Session Description Protocol [10]) body, given arguments such as the destination information, codec and other media attributes. When the call is answered, the Spitter retrieves the audio record and streams it to the intended target. The core threat resides when a synchronized, highly effective botnet of Internet Spitters flood the mobile network with such unsolicited traffic. As a result, the VoIP SPIT campaign can severely decrease the voice QoS of mobile users and ultimately denies the service on the LTE 4G mobile network.

1.3 SMTP SPAM Flooding

Another highly relied on application service on LTE 4G networks is the Simple Message Transfer Protocol (SMTP) [11]. SMTP is the Internet standard for electronic mail (email) transmission across IP networks. It is a text-based protocol, in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel. Often, mobile operators put into service SMTP servers in the network to provide outgoing email access to their clients. However, the critical issue arises when exploited malicious clients' user equipments from within the LTE network flood the operator's SMTP server with email SPAM in order to launch a SPAM campaign towards the Internet. As a result, this SPAM campaign will 1) cause a DoS to the SMTP server by overloading it with unsolicited emails and hence denying it from processing legitimate email requests in a timely manner and 2) more critically will cause the operator's SMTP server to be blacklisted by Internet DNS servers after being detected as a SPAM server. Consequently, this will have a major adverse influence on the operator's business, reliability and reputation. Furthermore, the mobile operator will face serious legal issues under, for example, the Canadian House Government Bill C-28 Act [12], for misusing the mobile infrastructure for Spamming purposes.

1.4 Defining DoS in Attack Scenarios

In this thesis, we focus on RTP VoIP SPIT flooding and SMTP SPAM flooding in order to demonstrate their DoS feasibility and impact on 4G mobile networks and subsequent effects on mobile network operators. Our intention is to shed the light on the fact that LTE 4G networks are vulnerable to IP-based attacks which forces mobile network operators to preventively react to preserve their provided application services and thus their business and reputation. Moreover, for clarification purposes, we explain in the following when exactly will a DoS occur in both attack scenarios.

1.4.1 DoS for VoIP SPIT Flooding

When using VoIP, there are three critical metrics that determine the QoS:

- One-way Latency,
- One-way Jitter,
- Packet Loss Rate.

One-way latency or end-to-end delay for voice packets is the ‘mouth-to-ear’ delay. It includes network delay (the measured time from when the sender node provides the voice packet to RTP to the time the receiver retrieves it from RTP), encoding and decoding delays and compression and decompression delays. The International Telecommunication Standardization Union (ITU-T) recommends the following limits for voice one-way transmission time [13]:

- 0 to 150 ms: Acceptable for most user applications,
- 150 to 400 ms: Acceptable provided that administrations are aware of the transmission time impact on the transmission quality of user applications,
- above 400 ms: Unacceptable for general network purposes.

On the other hand, jitter is defined as the variation in the delay of received packets. Generally, at the sending side, packets are sent in a continuous stream with constant delay between them. However, due to network congestion, improper queuing, or routing configuration errors, this steady stream can become unstable and hence the delay between each packet can vary. If the jitter is so large, it can cause packets to be received out of the range of the ‘playout delay buffer’ (a mechanism to buffer packets with variable delay and sent them out with constant delay), causing packets to be discarded and consequently voice dropouts will be heard in the transmitted audio. The ITU-R advocates that the average one-way jitter should be targeted at less than 30 ms [14]. Furthermore, packet loss rate is the percentage of dropped VoIP packets along the data path, which severely degrades the voice application service. ITU recommends a packet loss rate less than 1% [15].

In this work, we assert that if the average end-to-end delay for voice packets metric exceeds the 400 ms threshold and the one-way jitter metric surpasses 30 ms and the VoIP packet loss rate is over 1%, then a severe and unacceptable degradation in VoIP QoS will occur, prohibiting or denying the service on the 4G mobile network. Additionally, we will use those metrics to show relative service improvements, under the attack, after implementing our proposed distributed architecture.

1.4.2 DoS for SMTP SPAM Flooding

Generally, overloading SMTP servers does not cause a system crash. In fact, the SMTP protocol contains countermeasures for DoS attacks. If the load is too high, the server will cease to receive emails with temporary errors or simply by refusing connections. As SMTP is a delay tolerant service, the other party can send a particular email later. Thus, defining a DoS condition as a system crash or lost emails is inadequate. Note that, the most important point is the user experience. Therefore, if a single email is processed by the server after an unacceptable threshold because of a severe server performance bottleneck, then it can be correctly inferred as a DoS. Therefore we assume that SMTP DoS will occur when:

1. The SMTP server's CPU Utilization metric reaches 100%. This result will guarantee that

the server is overloaded with SPAM email requests which will affect its ability to process legitimate emails in a timely manner.

2. The SMTP server's Email Processing Time metric (measured from the time when a single request arrives at the server to the time it is completely processed) exceeds 200 ms. [1]

1.5 Problem Statement

Motivated by the fact that RTP VoIP SPIT and SMTP SPAM flooding are two alarming attacks coupled with the new evolution in mobile networks and the adoption of an IP-based network core, there is a critical need to investigate the feasibility and impact of such attacks, their effects on the network QoS metrics and mitigating architectures on LTE 4G mobile networks. Particularly, there is a need to answer questions, including the following: Can RTP VoIP SPIT and SMTP SPAM flooding attacks take advantage of the evolved IP-based network core to trigger a DoS? Moreover, what is the impact of that DoS and subsequent effects? Furthermore, what are the adopted approaches to mitigate the effects of these attacks? Additionally, how can we propose a security architecture on the mobile network infrastructure that mitigates the effect of such attacks yet is efficient and cost-effective?

In this thesis, we try to answer those questions by revealing that RTP VoIP SPIT and SMTP SPAM flooding attacks will indeed trigger a DoS, benefiting from LTE's evolved packet core. On

[1] This threshold is based on our Opnet simulation results that we had performed on 3 different SMTP servers. The least performant server was a single core windows 2000 server, the others were 4 and 8 core machines running Ubuntu server 9.04. Although this may not reflect realistic benchmark results, however as we will demonstrate in Section 4.3.2, this metric measured 2 ms under normal load and peaked at a significant 4 sec under attack load. Thus we consider the 200 ms threshold as a reference to a timely manner behavior and not as an absolute value.

one hand, we disclose, after performing large scale simulations, that RTP VoIP SPIT flooding by exploited Internet workstations targeting user equipments (UEs) on the mobile network, will cause a momentous degradation in VoIP QoS that ultimately denies the service on the LTE network. On the other hand, We demonstrate that SMTP SPAM flooding by exploited UEs targeting the mobile network operator's SMTP server, will cause a significant performance bottleneck on the server which will drastically affect its ability to process legitimate requests in a timely manner. Consequently, a crucial subsequent effect of that attack is the eventual blacklisting of the operator's SMTP server in addition to liability and negative reputation that will affect the mobile network operator. Additionally, by studying and analyzing specific detection algorithms employed by various intrusion detection systems (IDSs) and undergoing profiling on various hardware, we estimate the cost of those algorithms in terms of processing/detection delay on 4G networks specific infrastructure nodes. Having achieved that, we discuss and compare two mediating approaches based on two different mobile security architectures. Through measurement, simulation and analysis we compare the conventional centralized architecture and our proposed distributed architecture on the 4G infrastructure. As a result, we demonstrate that the distributed approach is secure by mitigating the effects of those attacks, is more efficient by solving the over dimensioning problem caused by the centralized approach and cost-effective by utilizing 'off the shelf' low-cost hardware in the distributed nodes.

1.6 Thesis Contribution

To summarize the above, in this thesis, we contribute by:

- Demonstrating, through large scale simulations, the feasibility and DoS impact of two SPAM flooding attacks on 4G mobile networks,

- Computing and quantifying the practical complexity in terms of packet processing filtering delay for the two most widely adopted content filtering algorithms on 4G mobile networks specific infrastructure nodes. We achieve that by undergoing profiling of rule matching on various hardware using an open source network intrusion detection and prevention system.

- Proposing a distributed architecture on the 4G mobile network infrastructure that is secure, efficient and cost-effective.

1.7 Thesis Organization

This thesis is organized as follows. Chapter 1 presented the need for LTE and highlighted on two protocols that may be vulnerable to flooding attacks on 4G mobile networks. Moreover, we defined DoS under both attack scenarios, discussed the problem statement and research questions and summarized our thesis contributions. Chapter 2 conveys some background and related work. Furthermore, Chapter 3 demonstrates the working environment and thus explains the 4G architectural infrastructure, reviews the mitigation methods including content filtering detection algorithms and discusses secure mobile architectures. Additionally, Chapter 4 reveals the algorithms' profiling discussion and results, portrays our topological simulation scenarios and illustrates the attack and countermeasure simulation results. Finally, Chapter 5 summarizes our contributions, reveals our future work and concludes this thesis.

Chapter 2

Background

2.1 General Vulnerabilities and Attacks

Wireless technology has opened up a new and exciting area for research. This emerging technology is advancing and changing every day. Moreover, networks enabled by such technology continue to be developed and their use have grown significantly and flourished ubiquitously. However, the broadcast nature of such networks and their mobility features created new kinds of intrusions and anomalies taking advantage of their wireless vulnerabilities. Because of the radio links and the mobile equipment features of wireless networks, wireless intrusions and attacks are more complex because they add to the intrusions developed for wired networks, a large spectrum of complex attacks targeting wireless environments. Hence, the biggest concern with wireless communications has been and will always be security.

Since LTE 4G mobile networks are part of these wireless networks, it is significant to discuss vulnerabilities and attacks in Wireless Networks. Therefore, this section will highlight on general threats, in both LAN-like wireless networks and cellular networks, and then discuss certain attacks on those networks.

2.1.1 Wireless Vulnerabilities

A vulnerability is a weakness (or fault) in the communication medium or protocol that compromises the security of a network component [16]. Most of the existing vulnerabilities in wireless networks are caused by the medium. Because transmissions are broadcast, they are easily available to anyone who has the appropriate equipment. According to [17], threats in wireless communications include device theft, malicious hacker, malicious code, theft of service, and espionage. Furthermore, there are numerous wireless vulnerabilities and threats that have been studied in the literature for the purpose of detecting attacks that exploit them. In the following, we distinguish between two categories of vulnerabilities and threats: those existing in a LAN-like wireless (WLAN) networks and those existing in cellular-like wireless networks.

WLAN Threats & Vulnerabilities

The subsequent are common vulnerabilities existing in the main component of WLANs, which is the Access Point (AP) [18].

- **Signal range of an authorized AP:** This vulnerability lies in the possibility of extending the AP signal strength beyond a given perimeter. Consequently, the AP's placement and signal strength have to be modified to make sure that the transmitting coverage is just enough to cover the intended area and not some other area that could be compromised.

- **Physical security of an authorized AP:** The physical placement of an AP is critical. An AP has to be correctly placed in order to avoid accidental damage, such as direct access to the physical network cable or access to it by unauthorized personnel that may comprise its security.

- **Rogue AP:** This vulnerability is a sort of man-in-the middle attack, where an attacker can place an unauthorized (or rogue) AP on the network and configure it to look legitimate to gain access to wireless users' sensitive data. This vulnerability can succeed because by default, users' devices connect to the strongest available AP signal.

- **The AP configuration:** If the AP is poorly configured, then it can provide an open door to hackers. This is caused by using a default configuration that annihilates the recommended security controls and encryption mechanisms.

- **Protocol weaknesses and capacity limits on authorized AP's:** These limitations can cause DoS from hackers using unauthorized AP's where they may flood authorized APs with traffic forcing them to reboot or deny service access.

Cellular Threats & Vulnerabilities

The subsequent are typical vulnerabilities existing in cellular systems [19].

- **Service interruption:** The increased capacity provided by high speed mobile technologies have resulted in fewer cable routes necessary to meet capacity requirements. Consequently, this has decreased the number of switches. The lack of overall diversity in cabling and switching has increased the vulnerability of telecommunication infrastructures. Coupled with malicious hosts taking advantage of such technologies in an illicit way, this can cause DoS on various mobile cells.

- **Natural threats:** Natural threats comprise the category of threats caused by climatic, geological, or seismic events. Severe damage resulting from natural disaster can cause long-term damage to telecommunication infrastructures.

- **Handset vulnerabilities:** Unlike computer systems, handsets are limited regarding their security features. With the flourishing of custom created mobile applications, mobile handsets executing malicious code is one issue. Another closely related issue are botnets which are being tailored nowadays to run and exploit mobile handsets. On the other hand, cellular messages encryption can cause a threat to handsets, since the receiver of these messages have no means of detecting what the encrypted messages actually contain.

2.1.2 Wireless Attacks

In this section, we discuss certain attacks that are generally feasible on both, WLANs and cellular-like wireless networks.

Wireless network sniffing

When wireless packets traverse the air, attackers equipped with appropriate devices and software can capture them. Sniffing attack methods [17] include:

- **Passive scanning:** This attack aims at listening to each channel and capturing packets without sending any information.

- **Service set identifier (SSID) detection:** This attack consists of retrieving the SSID by scanning frames of the following types: beacon, probe requests, probe responses, association requests, and re-association requests [18].

- **Gathering of MAC addresses:** For the purpose of performing attacks such as frame spoofing, the attacker collects and stores legitimate MAC addresses.

- **Probing and network discovery:** This attack aims to identify various wireless targets. It uses two forms of probing [20]: active and passive. Active probing involves the attacker actively sending probe requests with no identification using the SSID configured in order to solicit a probe response with SSID and other information from any active AP. When an attacker uses passive probing, he listens on all channels for all wireless packets.

- **Inspection:** The attacker can inspect network information using various hardware and software tools. He could identify MAC addresses, IP address ranges, gateways and packet payloads.

Wireless Spoofing

The purpose of spoofing attacks is to modify identification parameters in data packets. New values of selected parameters can be collected by sniffing. Typical spoofing attacks include [21]:

- **MAC address spoofing:** MAC spoofing aims at changing the attacker's MAC address by the legitimate MAC address. This attack is made easy to launch because some client-side software allows the user to view and modify their MAC addresses.

- **IP spoofing:** IP spoofing attempts to change source or destination IP addresses by communicating directly with the network device [22]. IP spoofing is used in various attacks such as DoS attacks.

- **Frame spoofing:** The attacker injects frames having the 802.11 specification with spoofed information. Due to lack of authentication, spoofed frames cannot be detected.

Man in the Middle Attacks

This attack attempts to insert the attacker in the middle of a communication for purposes of intercepting client's data and/or modifying them before discarding them or sending them out to the real destination. Two main forms of the this attack exist: eavesdropping and manipulation [23]. Eavesdropping can be done by intercepting radio waves on the wireless network. On the other hand, manipulation requires not only having the ability to receive the victim's data but to be able to retransmit the data after modifying it without being detected.

Denial of Service Attacks

DoS attacks can target different network layers as explained in the following [22]:

- **Application layer:** DoS occurs when a large amount of legitimate requests are sent. It aims to prevent other users from accessing the service by forcing the server to respond to a large number of request's transactions.

- **Transport layer:** DoS is successful when many connection requests are sent. It targets the operating system of the victim's computer. The typical attack in this case is a SYN flooding [24].

- **Network layer:** DoS succeeds if the network allows to associate clients. In this case, an attacker can flood the network with traffic to deny access to other devices. This attack could consist of the following tasks [20]:

  -The malicious node participates in a route but simply drops several data packets. This causes a deterioration in the quality of the connection.

  -The malicious node transmits falsified route updates or replays stale updates. These might cause route failures thereby deteriorating performance.

  -The malicious node reduces the time-to-live field in the IP header so that packets never reach their destinations.

- **Data link layer:** DoS targeting the link layer can be performed as follows:

  -Since we assume that there is a single channel that is reused, keeping the channel busy in the node leads to a DoS attack at that node.

  -By using a particular node to continually relay spurious data, the battery life of that node may be drained. An end-to-end authentication may prevent these attacks from being launched.

- **Physical layer:** This kind of DoS can be executed by emitting a very strong RF interference on the operating channel. This will cause interference to all wireless networks that are operating at or near that channel.

2.2 On VoIP Attacks and SPIT Prevention

In the past few years, a plethora of papers discussed attacks against VoIP. Sisalem et al. [25] addressed the issue of denial of service attacks targeting the hardware and software of VoIP servers by misusing specific features in the session initiation protocol. The authors delivered an overview of different attack possibilities and explained some attacks in more details, including attacks utilizing the DNS system and those targeting the parser. In another closely related work, Luo et al. [26] investigated the impact of DoS attacks on the SIP infrastructure, using a popular open source SIP server as a test bed. They identified four attack scenarios that can exploit vulnerabilities in existing SIP authentication protocols, and then they demonstrated the practical impact of these attacks on the target server. Moreover, the authors in [27] examined how the vulnerabilities of SIP can be exploited to compromise the reliability and trustworthiness of the billing of SIP-based VoIP systems. Specifically, they focused on the billing attacks that will create inconsistencies between what the VoIP subscribers received and what the VoIP service providers have provided. Additionally, they presented four billing attacks on VoIP subscribers. In another interesting study, Zhang et al. [28] demonstrated that a remote attacker who is not initially in the path of VoIP traffic can indeed launch all kinds of man-in-the-middle (MITM) attacks on VoIP by exploiting DNS and VoIP implementation vulnerabilities. They showed that the remote attacker can effectively wiretap and hijack targeted VoIP calls after becoming the remote MITM. Their results demonstrated that (1) the MITM attack on VoIP is much more realistic than previously thought; (2) securing all nodes along the path of VoIP traffic is not adequate to prevent MITM attack on VoIP; (3) vulnerabilities of non-VoIP-specific protocols (e.g., DNS) can indeed lead to compromise of VoIP.

Detection methods for such attacks and others on VoIP were also discussed thoroughly in the literature. In [29], the author proposed a method to detect DoS attacks that involve flooding SIP entities with illegitimate SIP messages. The author modified the original finite-state machines for SIP transactions in such a way that transaction anomalies can be detected in a stateful manner. He also proposed to use four threshold parameters to confirm an attack. Furthermore, Sengar et al. [30] presented an online statistical detection mechanism, called vFDS, to detect DoS attacks in the context of VoIP. The authors stated that the core of vFDS is based on Hellinger distance method, which computes the variability between two probability measures. Using Hellinger distance, they characterized normal protocol behaviors and then detected the traffic anomalies caused by flooding attacks. Additionally, the authors of [31] proposed a change-point detection method to prevent DoS attacks on VoIP systems based on SIP behavior analysis. They developed efficient adaptive sequential change-point method to detect attacks which lead to changes in network traffic. Their experimental results showed that the method achieves a very small delay, high rate and low false alarm rate of VoIP-specific DoS detection.

To detect and mediate SPIT, several approaches were proposed. Specifically, Quittek et al. [32] presented a method to detect SPIT calls by comparing hidden turing tests that compare the calls with typical human communication patterns. Additionally, Guang-Yu et al. [33] proposed a multi-layered SPIT detection and prevention method. Their method analyzed the unique characteristics of SPIT and then utilized signal monitoring algorithms and correlation algorithms to identify the behavior trace and reconstruct the attack scenario. Last but not least, Hongchang et al. [34] discussed a multilayered fusion method for SPIT calls detection. They explained that before a call is connected, the historical signal information about the caller number is collected to judge whether it is from a suspicious caller, then during the call communication period, some acoustic parameters of the speech are calculated to judge whether it is a text to speech voice, and after the connection is released, two parameters about user behavior pattern are calculated to decide whether the call is from a machine.

2.3 On DoS and 3G Attacks

DoS Attacks and mitigation methods have been discussed thoroughly in many contexts. A plethora of papers focused on DNS systems including [35, 36], while other research focused on Web services [37]. Furthermore, SMTP services were pinpointed in [38, 39]. Additionally, DoS attacks targeted Search engines [40], VoIP servers [41, 42] and not surprisingly e-commerce services [43].

The notion of exploiting a system to utilize it to launch a DoS attack was tackled in [44], where Naoumov et al. described two approaches to create a DoS engine out of a P2P system. The authors stated that for both approaches, the targeted host does not have to be a participant in the P2P system, and could be a web server, a mail server, or even a user's desktop. Additionally, they implemented their approaches in a P2P file-sharing system and revealed that with modest effort, both attacks could direct significant amount of traffic from diverse peers to flood any target. In another closely related study [45], Defrawy et al. stated that BitTorrent enormous traffic can be converted into a firepower for launching a distributed denial of service attack that can exhaust a victim's resources, including access bandwidth and connection resources. Moreover, the authors identified novel exploits in the BitTorrent system and conducted real-life experiments that demonstrated the feasibility and severity of such attacks.

The evolution of mobile devices from basic voice terminals into advanced computing platforms makes attacks originating from within the mobile network a reality. Lee et al. [46] introduced a signaling attack which seeks to overload the control plane of 3G mobile networks using low-rate, low-volume traffic. They affirmed that the low-volume nature of the signaling attack allows it to avoid detection by existing intrusion detection algorithms. In another approach, Traynor et al. [47] characterized a DoS attack using selected service request types on the Home Location Register (HLR), the central repository of user location and profile information in a 3G mobile network, by a botnet composed entirely of mobile phones. Their results showed that botnets as small as 11,750 phones can cause a reduction of throughput of more than 90% to area-code sized regions supported by most currently deployed systems. Moreover, Enck et al. [48] evaluated the security impact of the SMS interface on the availability of the cellular phone network. Specifically, they demonstrated the ability to deny voice service to cities, the size of Washington D.C. and Manhattan, using a regular cable modem. Another interesting study was conducted by Zhao et al. [49], where they presented a DoS attack against IMS. They stated that by congesting the presence service, a core service of IMS, a malicious attack can cause chained automatic reaction of the system, thus blocking all the services of the IMS.

While some basic form of malware targeting mobile devices has surfaced in the past, including Cabir [50], Mabir [51] and Skulls [52], advanced malicious applications exploiting today's full-featured powerful UEs are yet to be reported. However, with the adoption of LTE's evolved system architecture, vulnerabilities in mobile operating systems, non-safety of developed applications and software and the evolution of various types of botnets, their consequences and impacts must be investigated.

2.4 Security in 4G Networks

As 3G communication is moving to 4G communication, many standardization societies such as ITU, 3GPP and IEEE are working on the next generation of communication networks. Since security plays a critical role for the adoption of 4G network services, it is significant to discuss the need for secure architectures and their corresponding objectives on such networks, the threat model and various security threats on fourth generation networks.

2.4.1 Security Objectives

Traditionally, network security has focused on securing network edges to prevent external threats from accessing network resources. However, this approach is not adequate because attackers seek to discover security vulnerabilities in networking protocols, operating systems or applications, and exploit these vulnerabilities to propagate malware that may evade security measures at the edges. Hence, there is a need for comprehensive, network-wide security architecture integrated into both the network core and the end-user devices. The key objectives in designing the security architecture can be summarized as:

- Availability: that enforces networks and services not to be disrupted or interrupted by, for example, malicious attacks.
- Interoperability: that ensures the security solutions can avoid interoperability problems, e.g., by using generic solutions applicable to most applications and service scenarios.
- Usability: that makes it easy for the end-users to use the security-enabled services.
- QoS guarantee: that requires security solutions like cryptographic algorithms to meet QoS constraints of voice and multimedia traffic.
- Cost-effectiveness: that minimizes the additional cost of security and makes it lower than the cost of risks.

2.4.2 Threat Model

Possible threats to 4G include: IP address spoofing, user ID theft, Theft of Service (ToS), DoS, and intrusion attacks. Among them, network operators are most concerned about ToS and DoS attacks because they harm their revenue, reputation and service availability.

Besides this general categorization, protocol-specific attacks must be identified. For example, SIP-targeted attacks include: (i) malformed message attacks, (ii) buffer overflow attacks, (iii) Denial-of-Service (DoS) attacks, (iv) RTP session hijacking, (v) injection of unauthentic RTP, (vi) reuse of compromised SIP credentials, and (vii) bogus SIP network elements.

It is almost impossible to make a 100% secure system because new threats and vulnerabilities will continue to arise and take place. Additonally, there exist different stakeholders including at least network operators, service providers and users, having their own, sometimes mutually contradictory interest, leading to different security requirements. Hence, the 4G security architecture must be flexible enough to adapt itself to future threats and vulnerabilities as well as varying security requirements.

2.4.3 4G Security Analysis

To manage the threats that a network infrastructure is exposed to, it is essential to clearly identify key risks and threats. In this section, we analyze the security related to well-known 4G standards including WiMAX and 3GPP LTE.

WIMAX Security

WiMAX [53] addresses the compatibility and interoperability of broadband wireless access products using the IEEE 802.16 standards consisting of IEEE 802.16-2004 and 802.16e-2005 for fixed and mobile architectures, respectively [54]. These two standards specify different sets of security mechanisms. IEEE 802.16-2004 defines a Privacy Key Management (PKM) protocol by which Mobile Station (MS) authenticates itself, obtains Authorization Key (AK) from the Base Station (BS), and derives other keys like Key Encryption Key (KEK), Traffic Encryption Key (TEK) and so on. It also supports two encryption algorithms, i.e. DES in CBC mode and AES in CCM mode, with an option to use a proprietary encryption algorithm.

However, a number of weaknesses were discovered in IEEE 802.16-2004 [54]. First, it is vulnerable to an attack from bogus BS since there's no mutual authentication between BS and MS. Second, the encryption keys are solely generated by BS instead of the two parties, MS and BS, equally contributing to the values of keys. Third, it does not support integrity protection of management frames, exhibiting a potential risk of denial-of-service (DoS) attacks. Finally, it does not define how to manage, store, renew and revoke certificates.

In IEEE 802.16e-2005 [55], an improved version of PKM is developed to fix known vulnerabilities of PKM as well as offer more options. The key difference is that the improved PKM makes it mandatory to perform mutual authentication between MS and BS via RSA and/or EAP (Extensible Authentication Protocol). Besides, most of the management frames are now signed to ensure integrity protection, and AES-based encryption (in CBC, CTR and CCM modes) is used to provide communication flow protection.

Although IEEE 802.16e-2005 corrected almost all of the security weaknesses of its precursor [55], it still suffers several security vulnerabilities [56]; for instance, TEK is still chosen by BS while certificate management is not yet comprehensive. It is, therefore, important for the researchers and standards developers to keep on improving the security protocols as well as uncovering possible unknown vulnerabilities.

3GPP LTE Security

Security in cellular systems evolved as the generation changed. In the first generation (1G) cellular system, there was not much consideration for security; there was no over-the-air encryption in place and mobile phones could be easily cloned by intercepting the serial number. Furthermore, eavesdropping of conversations could easily and practically occur.

The 2G, exemplified by Global System for Mobile (GSM), uses Authentication and Key Agreement (AKA), called GSM AKA, for encryption and authentication [57]. It uses a challenge-response mechanism, where the user proves its identity by providing a response to a time-variant challenge raised by the network. However, its security is weak in which its authentication is performed only unidirectional; the user cannot authenticate to the serving network. Moreover, authentication data (which are called triplets), authentication information and cipher keys are reused indefinitely. In 3GPP AKA [58], improvements addressed mutual authentication and agreement on an integrated key between the mobile terminal and the serving network, as well as the freshness assurance of agreed cipher key and integrity key. In addition, a sequence number is used for freshness where two counters (one for the network and one for the mobile terminal) are synchronized for the purpose of sequence number verification.

Although the 3GPP AKA has been accepted as reliable and have been used excessively, there still exist weaknesses in 3GPP AKA as shown in [59]. The weaknesses include (1) redirecting user traffic using false BS and mobile terminals, (2) given the fact that the counter value could be set to a high value by an adversary, the mobile terminals' life time may be shortened, (3) because a home network keeps a counter and dynamically synchronize for every mobile terminal, a fault in the counter database may affect all mobile terminals. Additionally, because resynchronization is requested by the MT, this may result in a resynchronization message attack to the home network [60].

2.4.4 Possible Threats on 4G

Possible security risks mostly arise from the open nature of 4G as summarized next. First of all, a large number of external connectivity points with peer operators, with third-party applications providers, and with the public Internet, as well a numerous heterogeneous technologies accessing the infrastructure, serve as potential security holes if the security technologies do not fully interoperate. Moreover, multiple service providers share the core network infrastructure meaning that a compromise of a single provider may result in collapse of the entire network infrastructure. Finally, service theft and billing fraud can take place if there are third-parties masquerading as legitimate ones.

New end-user equipment can also become a source of malicious (e.g., DoS) attacks, viruses, worms, spam mails and calls, etc... In particular, Spam over Internet Telephony (SPIT) as mentioned in the introductory chapter of this thesis, the new spam for VoIP, will become a serious problem just like the e-mail spam nowadays. For example SPITs targeting VoIP gateways can consume available bandwidth, thereby severely degrading QoS and voice quality. Clearly, the open nature of VoIP makes it easy for the attackers to broadcast SPITs similarly to the case of spam emails. Other possible threats include: (1) spoofing that misdirects communications, modifies data, or even transfer cash from a stolen credit card number, (2) general SIP registration hijacking that substitutes the IP address of packet header with attacker's own, (3) eavesdropping of private conversation that intercepts and crypt-analyzes IP packets, and (4) phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

2.5 Conclusion

In this chapter, we presented a background on some of our related work. Specifically, we commenced by pinpointing various vulnerabilities and attacks on both WLANs and cellular wireless networks. Moreover, we highlighted on VoIP attacks and misdemeanors and reviewed some SPIT prevention mechanisms. Additionally, we discussed DoS attacks and 3G UMTS exploits. More importantly, we shed the light on 4G security. Consequently, we briefed various security objectives, illustrated the threat model, provided a security analysis of 4G technologies, namely of WIMAX and LTE and finally discussed possible threats on 4G networks.

In the subsequent chapter, we aim to expand the notion of threats on LTE 4G mobile networks, by firstly presenting the 4G architecture that is responsible for triggering such threats. Furthermore, we discuss the working environment and our preventive methodology which will function as building blocks to Chapter 4 which will eventually reveal our SPAM flooding attacks and subsequent effects and ultimately show the viability and effectiveness of our proposed distributed security architecture.

Chapter 3

Architecture and Mitigation Methodology

In this chapter, we aim to present, describe and illustrate the new LTE 4G mobile network. Moreover, we present and discuss SPAM mitigation methods and secure mobile architectures.

3.1 4G Mobile Networks Overview

LTE 4G mobile networks are expected to support various types of services including extensively rich web browsing, file transfer of enormous data, multi-party audio and video streaming, online gaming, real time video, push-to-talk and push-to-view. Therefore, 4G mobile networks are being designed to be high data rate and low latency systems as indicated by the key performance criteria shown in Figure 3.1 [2].

The bandwidth capability of a user equipment (UE) is expected to be 20MHz for both transmission and reception. However, the service provider can deploy cells with any of the bandwidths

Figure 3.1: LTE Metric Requirements [2]

listed in Figure 3.1. This gives flexibility to the service providers to tailor their offering dependent on the amount of available spectrum or the ability to start with limited spectrum for lower upfront cost and grow the spectrum for extra capacity. Beyond the metrics, LTE 4G networks are as well aimed at minimizing cost and power consumption while ensuring backward-compatibility and a cost effective migration from UMTS 3G systems. Enhanced multicast services, superior support for end-to-end QoS and minimization of the number of options and redundant features in the architecture are also being targeted. Moreover, the spectral efficiency in the LTE downlink will be 3 to 4 times of that of the High-Speed Downlink Packet Access (HSDPA) while in the uplink, it will be 2 to 3 times that of the High-Speed Uplink Packet Access (HSUPA) [61]. The handover procedure within LTE networks is intended to minimize interruption time to less than that of circuit-switched handovers in 2G networks [3]. Furthermore, the handovers to 2G/3G systems from LTE are designed to be seamless.

3.2 LTE 4G Pillars

LTE encompasses the pillars of next-generation networks: [62] [63]

- Broadband wireless as the new access reality: High-throughput, low-latency mobile access based on advanced multiplexing and spectrum techniques, efficiently delivering unicast, multicast and broadcast media.

- Convergence of technology and networks: A single applications domain serving customers across multiple networks and devices.
- Intelligence at the services edge: Implementing policy enforcement and decisions at the network edge, in an access-agnostic but access-aware framework.
- Technology shift to all-IP: Simplifying and streamlining the network, improving scalability and deployment flexibility and enabling consistent access-aware policy enforcement and billing.
- Embedded security: A multi-layer multi-vendor approach to security is critical to ensure that security is endemic to the network and not just focused on point solutions.

3.3 LTE: The Evolved Wireless Access

The challenge for next-generation wireless networks is to provide wireless broadband at a cost and performance better than that achievable with DSL technologies, while maintaining seamless mobility, service control and maximizing network capacity with limited spectrum resources.

Specific technical requirements include: [64] [65]

- Low latency and high throughput,
- Efficient always-on operation, with instantaneous access to network resources,

- Support for real-time and non-real-time applications,
- Flexible spectrum allocations,
- High spectrum efficiency for unicast, multicast and broadcast data.

In addition to the requirements above, there is a set of minimum performance requirements defined by the 3GPP [66]. These objectives include:

- Increased spectral efficiency and capacity: LTE is expected to deliver three to five times greater capacity than the most advanced current 3G networks.
- Lower cost per bit: Increased spectral efficiency combined with the operational benefits of an all-IP network will reduce the cost per bit compared to 3G solutions.
- Improved quality of experience: One of the benefits LTE/SAE will bring is a reduction in latency time, which will enhance the behavior of time-sensitive applications, such as VoIP, thus improving the user experience. For example, the latency time, expressed as the time for a 32 byte Ping, is expected to reach 20 ms (compared with 120 ms for a typical 3G network).

3.4 Enabling Technologies

Two key enabling technologies will help meet and exceed the LTE performance objectives:

3.4.1 Orthogonal Frequency Division Multiplexing

Orthogonal Frequency Division Multiplexing (OFDM) is fundamentally able to handle the most common radio frequency distortions without the need for complex equalization techniques, and scales easily to fit different bandwidth requirements.

OFDM is already an extremely successful access technology currently deployed in a number of wireless and wireline applications [67]. These applications include digital audio and video broadcast [68], wireless WLAN (IEEE 802.11a and IEEE 802.11g) [69] , WiMAX (IEEE 802.16) [70] and wireline Asynchronous Digital Subscriber Loop (ADSL/ADSL2+) [71]. OFDM is widely accepted as the basis for the air interface, necessary to meet the requirements for next-generation mobile networks.

3.4.2 Multiple Input/Multiple Output

Multiple Input/Multiple Output (MIMO) increases peak throughput by transmitting and receiving multiple streams of information within the same spectrum. MIMO exploits the multi-path effects typical in wireless environments.

MIMO employs multiple transmit and receive antennas to substantially enhance the air interface. It uses space-time coding of the same data stream mapped onto multiple transmit antennas, which is an improvement over traditional reception diversity schemes where only a single transmit antenna is deployed to extend the coverage of the cell. MIMO processing also exploits spatial multiplexing allowing different data streams to be transmitted simultaneously from the different transmit antennas, to increase the end-user data rate and cell capacity. In addition, when knowledge of the radio channel is available at the transmitter (e.g. via feedback information from the receiver), MIMO can also implement beam-forming to further increase available data rates and spectrum efficiency.

The combined use of OFDM and MIMO will improve the spectral efficiency and capacity of the wireless network, and will prove to be a very valuable asset in maximizing usage of scarce spectrum typically controlled by regulatory bodies.

3.5 LTE 4G Network Architecture

In this section we present the 4G network architecture and describe its elements and corresponding functionalities. Figure 3.2 illustrates a unified view of the overall LTE mobile architecture which is marked by the elimination of the circuit-switched domain and a simplified access network.

The 4G system is comprised of two networks: the E-UTRAN (also referred to as the 'LTE' part) and the Evolved Packet Core (EPC) (part of the new System Architecture Evolution (SAE)) [3]. The result is a system characterized by its simplicity, a non-hierarchical structure for increased scalability and efficiency, and a design optimized to support real-time IP-based services.
The access network, E-UTRAN is characterized by a network of Evolved-NodeBs (eNBs) which support orthogonal frequency-division multiple access (OFDMA) and advanced antenna techniques. E-NBs interface with user equipments and perform numerous functions including radio

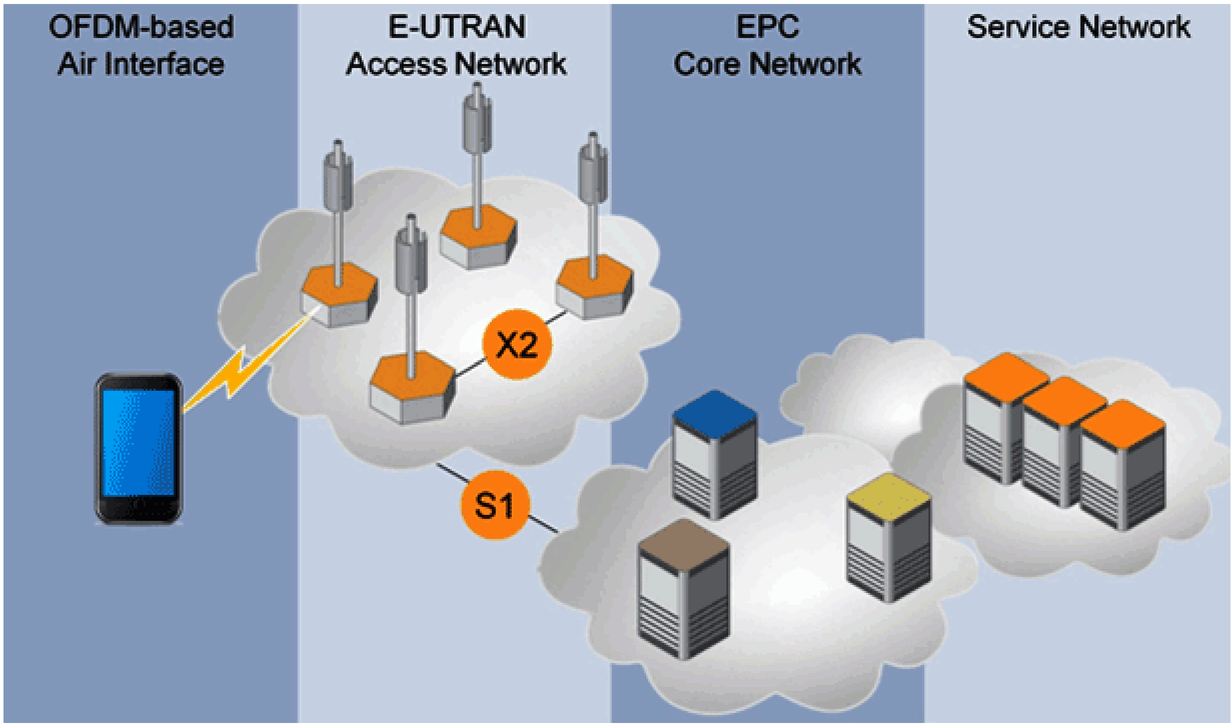


Figure 3.2: LTE 4G Mobile Architecture

resource management, admission control, scheduling, ciphering/deciphering and compression/decompression of user and control plane data. On the other hand, the packet domain of LTE network is called the Evolved Packet Core (EPC) and is depicted in Figure 3.3.

It is a flat all-IP system (ie. end to end IP based) designed to provide much higher packet data rates and significantly lower-latency. It consists of six nodes; the Mobility Management Entity (MME) which manages UEs and their sessions, additionally controls establishment of evolved packet system (EPS) bearers in the selected gateways. The Serving Gateway (SGW) which acts as the mobility anchor for the user plane during inter-eNB handovers, as well manages and stores UE contexts such as parameters of the IP bearer service and network internal routing information in addition to routing data packets between the P-GW and the E-UTRAN. The Packet Data Network

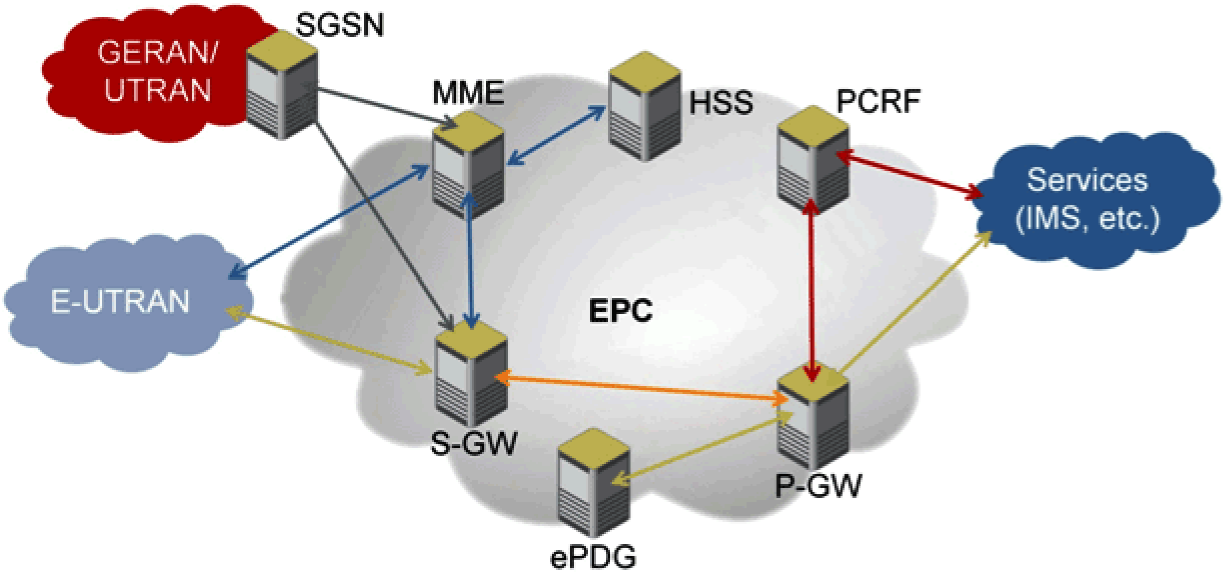


Figure 3.3: LTE Evolved Packet Core

Gateway (P-GW) provides connectivity to external packet data networks by being the point of exit and entry of traffic, also performs policy enforcement and packet filtering. Moreover, the Home Subscriber Server (HSS) is the master database that stores subscription-related information to support call control and session management entities. Furthermore, the Policy and Charging Control Function (PCRF) is the single point of policy-based QoS control in the network. It is responsible for formulating policy rules from the technical details of Service Date Flows (SDF) that will apply to users' services, and then passing these rules to the P-GW for enforcement. Finally, the evolved Packet Data Gateway (ePDG) is used for interworking with un-trusted non-3GPP IP access systems.

Hence, and as discussed in the introductory chapter of this thesis and conversed here in this section, the new 4G mobile architecture or SAE, will be vulnerable to serious IP based attacks. A specific criteria of IP based attacks that we study in this thesis and is of interest to us, are attacks based on SPAM flooding, originating from outside as well as from within the 4G mobile network. As a result, it is worthy to subsequently discuss methods for SPAM flooding mediation, in which we later, adopt them, on specific functional elements of the 4G mobile architecture for the purpose of SPAM mitigation. Having achieved that, we will be in a position to discuss secure mobile architectures, aiming to reveal that our proposed distributed architecture is secure, more efficient and cost-effective comparing with the de-facto industry widely adopted centralized architecture where both approaches will be discussed consequently in the remaining portion of this chapter.

3.6 SPAM Mitigation Methods

There are three general forms of SPAM (SPIT) flooding mitigation methods discussed throughout the literature [72].

3.6.1 Pattern Detection

These techniques seek to find patterns in requests and then determine if those patterns are associated with legitimate requests. Often these systems have predefined lists of signatures which indicate a common attack. Pattern Detection can be sub-divided into two sections:

- Exact String Matching: A special case of pattern matching where the pattern is described by a finite sequence of symbols (or alphabet Σ). It consists of finding one or more generally all the occurrences of a short pattern P=P[0]P[1]$\cdots$P[m$-$1] of length m in a large text

$T=T[0]T[1]\cdots T[n-1]$ of length n, where m, n>0 and $m \leq n$. Both P and T are built over the same alphabet Σ.

- Regular Expressions Matching: This method provides a concise and flexible means for identifying strings of text, such as particular characters, words, or patterns of characters. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification. A regular expression, often also called a pattern, is an expression that describes a set of strings. They are usually used to give a concise description of a set, without having to list all its elements.

To implement pattern detection, various algorithms were proposed which will be discussed next.

String Matching Algorithms

- **Brute Force:**

  The Brute-Force (BF) algorithm, which is the simplest, performs character comparisons between a character in the text and a character in the pattern from left to right [73]. In any case, after a mismatch or a complete match of the entire pattern it shifts exactly one position to the right. It requires no pre-processing phase and no extra space. The BF algorithm has $O(m\times n)$ worse-case time complexity. The average number of character comparisons is $n(1+\frac{1}{|\Sigma|-1})$ [74].

- **Knuth-Morris-Pratt:**

  The Knuth-Morris-Pratt (KMP) algorithm, which was the first linear time string matching algorithm discovered, performs character comparisons from left to right. In case of mismatch it uses the knowledge of the previous characters that we have already examined in order to compute the next position of the pattern to use [73]. In addition, this algorithm provides the advantage that the pointer in the text is never decremented. The pre-processing phase of the KMP algorithm requires O(m) time and space. The searching phase needs O(m+n) time in the worse and average cases [75].

- **Boyer-Moore:**

  The next algorithm is Boyer-Moore (BM) algorithm, which is known to be very fast in practice, performs character comparisons between a character in the text and a character in the pattern from right to left. After a mismatch or a complete match of the entire pattern it uses two shift heuristics to shift the pattern to the right. These two heuristics are called the occurrence heuristic and the match heuristic [75]. Note that the length of the shift is the maximum shift between the occurrence heuristic and the match heuristic. These heuristics are pre-processed in O(m+|Σ|) time and space. The searching phase of the BM algorithm needs O(n×m) time in the worse case. Finally, the expected performance of the BM algorithm is sub linear requiring about $\frac{n}{m}$ character comparisons on average [74].

- **Boyer-Moore-Horspool:**

  The Boyer-Moore-Horspool (BMH) algorithm does not use the match heuristic. In case of mismatch or match of the pattern, the length of the shift is maximized by using only the occurrence heuristic for the text character corresponding to the rightmost pattern character (and not for the text character where the mismatch occurred) [74]. The pre-processing phase of the BMH algorithm requires O(m+|Σ|) time and reduces the space requirements from O(m+|Σ|) to O(|Σ|). Finally, the searching phase requires O(m×n) time in the worse case but it can be proved that the average number of character comparisons is $|\frac{n}{\Sigma}|$ [75].

- **Shift-Or:**

  The Shift-Or (SO) algorithm represents the state of the search as a number and each search step costs a small number of arithmetic and logical operations, provided that the numbers are large enough to represent all possible states of the search. Assuming that the pattern length is no longer than the computer word of the machine, the time complexity of the preprocessing phase is O((m+|Σ|)×($\lceil m/w \rceil$)) using O(m×|Σ|) extra space [74]. Finally, the time complexity of the searching phase is O(n×($\lceil m/w \rceil$)) in the worse and average cases, where ($\lceil m/w \rceil$) is the time to compute a shift or other simple operation on numbers of m bits using a word size of w bits [75].

Regular Expression Algorithms

- **Non-Deterministic Finite Automata:**

  A non-deterministic finite automaton (NFA) is a mathematical model that consists of

  1. A set of states S
  2. A set of input symbols Σ (the input symbol alphabet)
  3. A transition function that maps state-symbol pairs to sets of states

4. A state s0 that is distinguished as the start (or initial) state

5. A set of states F distinguished as accepting (or final) states

An NFA accepts an input string x if and only if there is some path in the transition graph from the start state to some accepting state, such that the edge labels along this path spell out x. A path can be represented by a sequence of state transitions called moves. Regarding the NFA's complexity, if given an NFA N, an input string x, a set of final states and a regular expression r, then the time complexity is $O(|N|\times |x|)$ where $|N|$ is the number of states in N and $|x|$ is the length of x. N has at most twice as many states as $|r|$. Thus, space complexity is $O(|r|)$.

- **Deterministic Finite Automata:**

  A deterministic finite automaton (DFA) is a special case of a non-deterministic finite automaton in which

  1. No state has an ε-transition, i.e., a transition on input ε, and

  2. For each state s and input symbol a, there is at most one labeled edge a leaving s. If we convert NFA to DFA, it generates at most $2^{2\times|r|}$ states. Therefore, the space complexity for the DFA is $O(2^{2\times|r|})$. The time complexity is $O(|x|)$.

- **Extended Finite Automata:**

  As we have stated, representing network intrusion detection signatures as deterministic finite-state automata (DFAs) results in very fast signature matching but for several classes of signatures, DFAs can blow-up in space. On the other hand, using non-deterministic finite-state automata (NFA) to represent NIDS signatures result in a concise representation but at the expense of higher time complexity for signature matching. The main idea of Extended Finite Automata (XFA) is to find an ideal case in which we implement the advantages of both DFA and NFA. As a result, XFAs have time complexity similar to DFAs and space complexity similar to NFAs. According to the authors of [76], XFAs use 10 times less memory than a DFA-based solution, yet achieve 20 times higher matching speeds. Additionally, according to [75], the authors provide a small example and reveal that the space complexity of he XFA is linear in n and hence the time complexity is O(n).

- **Delayed Input DFA:**

  In [77] , the authors introduce a new representation for regular expressions, called the Delayed Input DFA (D^2FA), which substantially reduces space requirements as compared to a DFA. A D^2FA is constructed by transforming a DFA via incrementally replacing several transitions of the automaton with a single default transition. Their approach dramatically reduces the number of distinct transitions between states. According to the authors, for a collection of regular expressions drawn from current commercial and academic systems, a D^2FA representation reduces transitions by more than 95%. Furthermore, the time complexity is O(n^2logn) and the space complexity is O(n^2) where n is the number of states. Note that in [78], the authors proposed another algorithm based on D^2FA that produced the following enhanced complexities: time complexity is O(n^2) and space complexity is O(n).

- **Content Addressed Delayed Input DFA:**

  Although D^2FA decreased the space requirement needed for DFA, however, it sacrificed throughput (performance). For that reason, in [79], the authors propose Content Addressed Delayed Input DFA (CD^{2}FA), which provided a compact representation of regular expressions that match the throughput of traditional uncompressed DFA's. A CD^{2}FA addressed successive states of a D^{2}FA using their content, rather than a 'content-less' identifier. This makes selected information available earlier in the state traversal process, which makes it possible to avoid unnecessary memory accesses. Moreover, CD^{2}FAs use as little as 10% of the space required by a conventional compressed DFA and match the throughput of an uncompressed DFA. Concerning the complexities, the time complexity is $\approx$ O($|x|$) where x is the input string and the space complexity is $\approx$ O($2^{2\times|r|}$)$\times$(10%).

It is extremely worthy to mention that the Boyer-Moore algorithm coupled with NFA regular expressions detection algorithms are the two most widely adopted content filtering mechanisms in which they are implemented in various approaches and forms in leading SPAM/IDS detection tools such as Snort [80], Barracuda [81], Bro IDS [82], Suricata [83], CleamMyMail [84], Cloudmark Desktop [85] and Spamfighter [86].

3.6.2 Anomaly Detection

In this method, a base line for 'normal' traffic is generated and then used to identify possible attacks. These anomalies may be in the form of unusual traffic flows (for example, a large amount of traffic to a machine which generally receives little traffic), or a behavior (for example, a failure to respect TCP flow control mechanisms for a TCP flow). This is hard to achieve on real networks, as traffic flows can be highly variable whilst not being malicious. However, this approach holds the most promise for SMTP as anomalies would present themselves as unusual traffic flows, either in a larger than normal number of emails being delivered to one recipient, or a larger number of emails than usual coming from a limited number of clients.

3.6.3 Third Party Detection

These are systems which do not perform any attack detection themselves, but act on instructions from an external source. This might be in the form of a commercial service or a network wide traceback mechanism such as CenterTrack [87].

In this thesis, we implement a pattern detection approach and we assert that it will be effective in mediating the effect of the SPAM flooding attacks. As mentioned in Section 1.5, in this work we aim to study and analyze specific detection algorithms and undergo profiling on various hardware to estimate the cost of those algorithms in terms of processing/detection delay on LTE 4G specific infrastructure nodes. Having achieved that, we will be in a position to discuss and compare two mediating approaches based on two different mobile security architectures. Through measurement, simulation and analysis we will be capable to compare the conventional centralized architecture and our proposed distributed architecture on the 4G mobile infrastructure.

3.7 Secure Mobile Architectures

In the past few years, we have witnessed an explosion in demand for security measures motivated by the proliferation of mobile/wireless networks, the fixed-mobile network convergence, and the emergence of new application services. 4G systems play a key role in this network evolution, and, thus, all stakeholders are interested in the security level supported in the new evolved emerging mobile environment.

In this thesis, we intend to shed the light on the fact that 4G mobile networks are vulnerable to IP-based attacks which forces mobile network operators to preventively react to preserve their provided application services and thus their business and reputation. Hence a security architectural solution is required and for those reasons may be proposed on the LTE 4G network infrastructure.

The notion of a secure mobile architecture was initiated by the Open Group in their technical report [88] that was published in 2004. The report mainly describes an integration architecture that provides a framework and various building blocks for implementing a secure mobile environment. The report concluded with the following recommended practices and approaches concerning three areas:

- Session Management: Until ubiquitous wireless coverage is a reality, session management is a necessary part of doing business in a mobile environment. Thus, there is a need to plan for and develop a secure and efficient session management client-server solution for mobile and roaming users.
- Security: Develop a security architecture that takes into account all the layers of wireless security and is an integrated approach to end-to-end security. The critical point is to adopt a 'host payload inspection mechanism' as the core security feature of the network architecture

to move away from address-based security.

- Vision: Create an IT body to deal with wireless and mobility issues. Create an architecture that technically and efficiently meets the wireless and mobility requirements within an organization.

Following the 'Security' recommended practice by the Open Group community, we adopt in our appraoch a security mechanism on 4G architectural elements.

Although there exist various mobile network architectures for mitigation methods deployment, in this thesis we present, compare and analyze two major design trends; the conventional centralized architectural approach and our proposed distributed architectural approach. By doing so, we would be providing the scientific and the industrial communities with a unique approach on the placement of SPAM flooding mitigating mechanisms on LTE 4G mobile networks. In this work, we aspire to show that the proposed distributed approach is:

1. Secure by mitigating the effects of the SPAM flooding attacks,
2. Efficient by solving the over dimensioning problem caused by the conventional centralized architectural approach,
3. Cost-Effective compared with the centralized approach; by utilizing commercial less performant less expensive 'off-the-shelf' hardware in the distributed nodes rather than utilizing specialized immensely performant expensive hardware in the centralized node.

In an LTE 4G mobile network and in the centralized security architectural approach, all mitigating mechanisms are concentrated in only one node, mainly in the P-GW as illustrated in Figure

3.4. This approach can be considered the de facto in current real world implementations since the

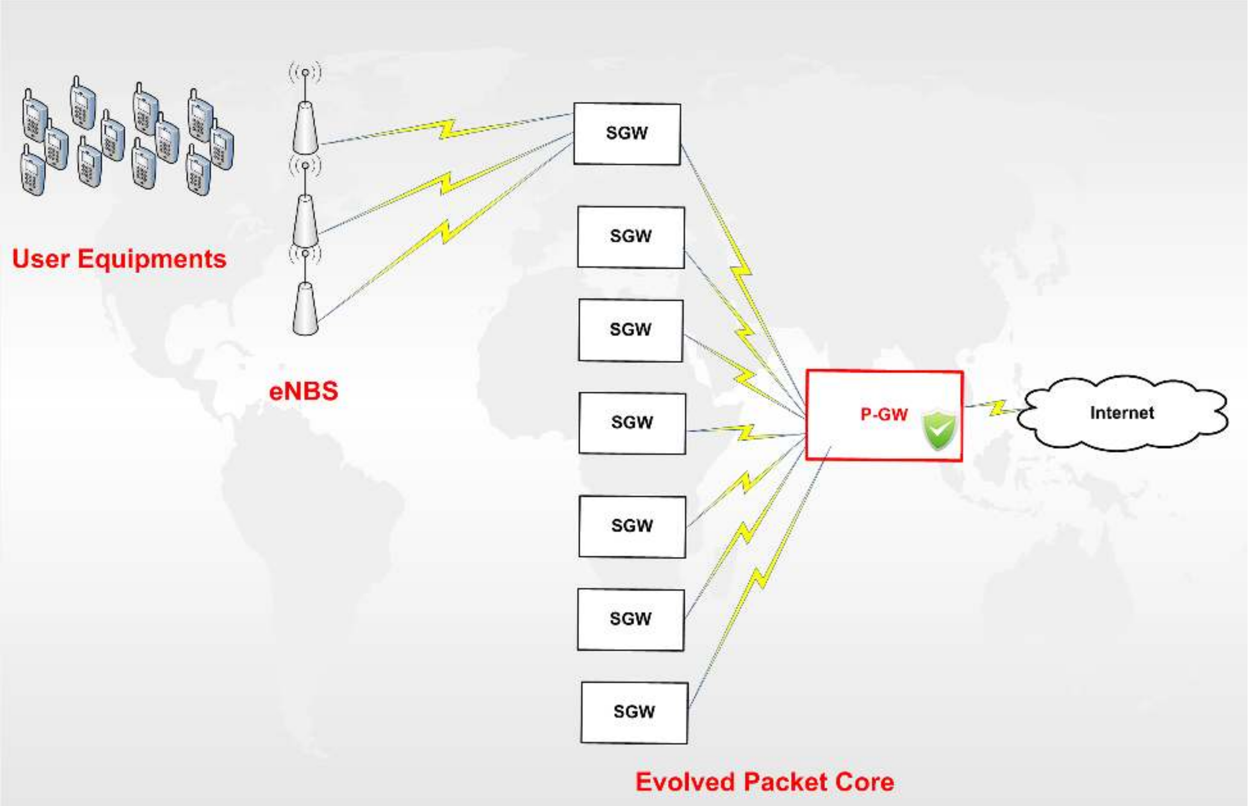


Figure 3.4: Centralized Security Architecture

P-GW acts as the exclusive point of entry from and exit to the Internet. Hence, all traffic passes through it and thus ingress and egress filtering can be practically achieved in it. In contrast, in a distributed security architectural approach, mitigating mechanisms are distributed on various LTE nodes. Although there are several valid candidates for that task, we believe that the S-GW has the right granularity to be a strong candidate. The S-GW, similar to the P-GW, covers all ingress and egress traffic from and to the Internet. However, the traffic on the S-GW is some order of magnitude less than on the P-GW, thus the overall filtering load is distributed over the entire set of S-GWs and is consequently, far less than the filtering load on the centralized P-GW. Moreover, the S-GW is the only node other than the P-GW that deals with data plan traffic during an active data connection (other nodes deal with signaling, control or policy enforcement and/or charging). Figure 3.5 depicts this approach. The rationale behind this scheme states that if we re-allocate the mitigating algorithms from the P-GW and distribute them unto the S-GWs, even after we acknowledge the fact that the S-GWs are less performant in terms of processing power than the P-GW, we will still be able to achieve the security task of mediating the effect of the SPAM flooding attacks while in addition preserve the efficiency on the LTE network by solving the over dimensioning problem in the P-GW caused by the centralized approach. Moreover, since the S-GWs can utilize 'off the shelf' hardware compared to the P-GW that uses dedicated high-priced hardware, this countermeasure is also cost-effective.

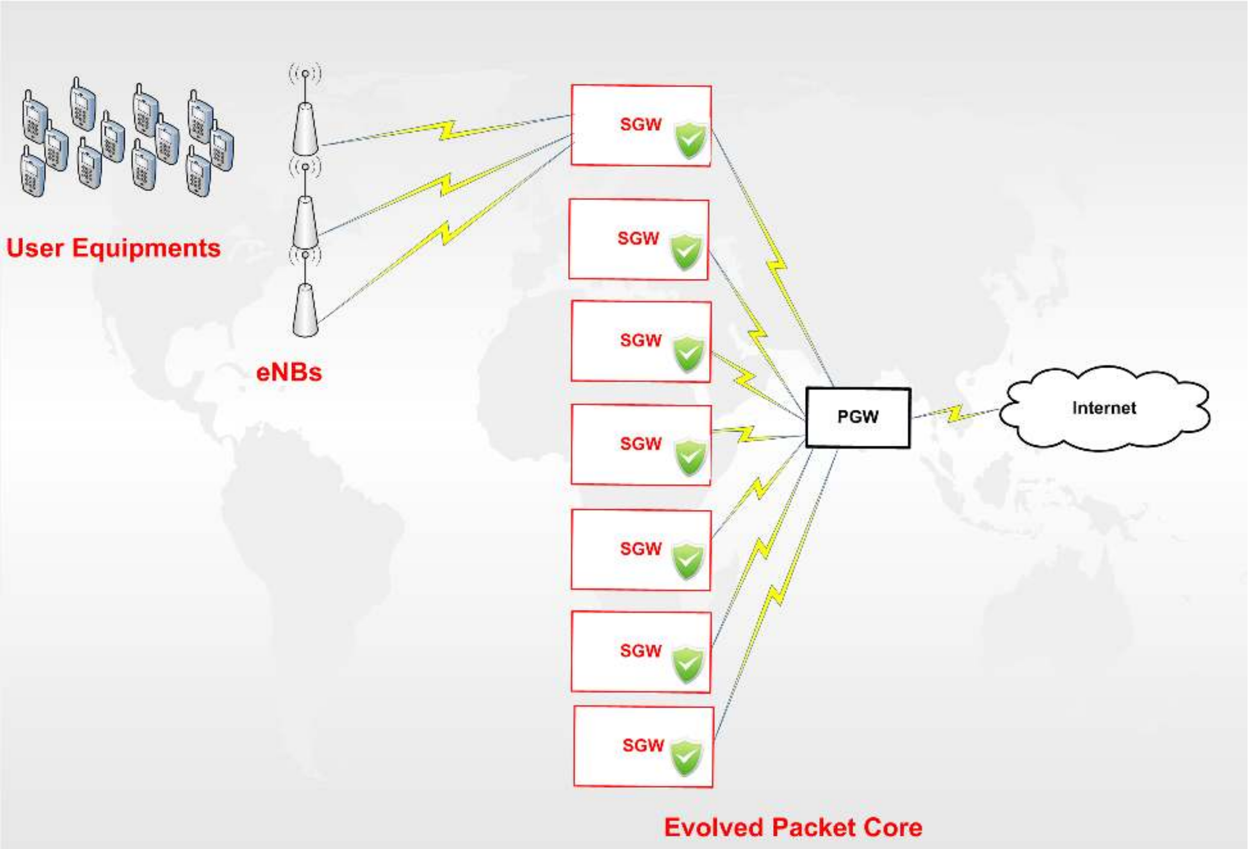


Figure 3.5: Distributed Security Architecture

Furthermore, and since in this thesis we are discussing two various security approaches and eventually validating the advantages of the distributed security architecture on the 4G mobile architecture, it would be creditable to pinpoint as well some of the general advantages and disadvantages of a generic distributed design approach.

Advantages of Distributed Systems:

- Performance: very often a collection of processors can provide higher performance (and better price/performance ratio) than a centralized node.
- Distribution: many applications involve, by their nature, spatially separated machines (banking, commercial, automotive system).
- Reliability (fault tolerance): if some of the distributed machines crash, the system can still operate.
- Incremental growth: as requirements on processing power increase, new nodes can be added incrementally and practically.
- Sharing of data/resources: shared data is essential to many applications (banking, computer-supported cooperative work, reservation systems).

Disadvantages of Distributed Systems:

- Difficulties of developing distributed software: how should operating systems, programming languages and applications be implemented on the distributed nodes?

- Networking problems: several problems are created by the network infrastructure, which have to be dealt with; ie: loss of messages, overloading, etc...
- Security problems: sharing generates the problem of data security.
- Maintenance: the cost of maintenance can skyrocket because each distributed node has its own share of problems and errors.

It is worthy to note that in this thesis and in our proposed distributed security architecture, the set of distributed nodes (the SGWs) function individually and independently on the traffic to perform the filtering and the detection. Hence, many disadvantages of a collaborative distributed design approach such as signaling, inter-node communications overhead and combining and coordinating of data are not present in our proposed distributed architecture.

3.8 Conclusion

In this chapter, we presented, explained and illustrated the evolved 4G mobile architecture. By doing so, we highlighted on the fact that its new SAE 'All IP' architecture is vulnerable to IP based attacks. Moreover, and since in this thesis we focus on SPAM flooding attacks and their effects on network metrics and subsequent effects on mobile network operators, we consequently discussed SPAM mitigation approaches. Furthermore, we presented and compared two secure mobile architectures, namely the de-facto centralized approach and our proposed distributed approach.

In the next chapter, we present the SPAM flooding attacks use cases and reveal their effects on the 4G network and consequent effects on mobile network opertors. More importantly, we put our proposed distributed security architecture under investigation in which we demonstrate its feasibility and effectiveness under the SPAM flooding attacks compared with the centralized security architecture.

Chapter 4

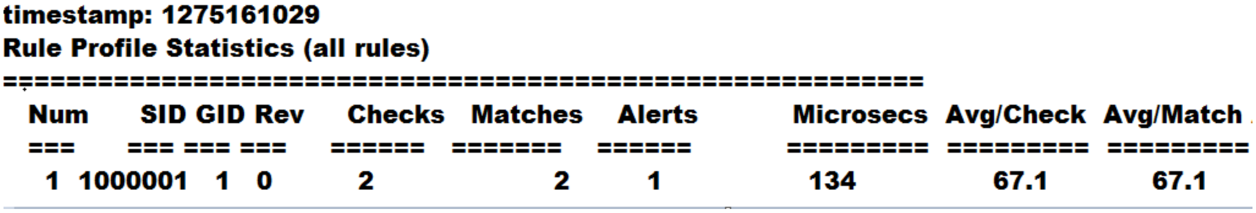
Attack and Defense Scenarios

4.1 Profiling for SPAM Flooding Mitigation

As we have stated in Section 3.6.3, we intend to measure specific pattern mitigating algorithms in terms of detection/packet processing delay. Our ultimate goal is to identify how much time an algorithm will require to inspect a packet on specific LTE nodes (S-GWs & P-GWs). Having achieved that, we will be in a position to simulate their effect when implemented on the 4G network infrastructure for the purpose of SPAM flooding mediation.

To accomplish that task, Snort [80] an open source network intrusion prevention and detection system, combining the benefits of signature, protocol and anomaly-based inspection, was investigated. Snort, and part of its content signature detection, implements the Boyer-Moore (BM) exact string matching detection algorithm in addition to a non-deterministic finite automata regular expression (NFA RegEx) detection algorithm. In fact, those generic algorithms are as well widely adopted in various forms in many intrusion detection systems such as Bro [82] and Suricata [83]. However, we have selected Snort since it is very well established and supported and employs a very descent scientific profiling engine which was vital in our case.

To obtain the measurement results for the BM and NFA RegEx algorithms, we performed profiling of rule-matching. This procedure enabled us to take advantage of the detection rules to trigger the detection algorithms and consequently measure the time they require to inspect and detect Spam in data packets. The procedure was executed on two Linux machines operating an Ubuntu 9.10, Snort Version 2.8.5.3 (Build 124) with PCRE version 7.8. The first machine was dual core with 4GB of memory. This machine will model the Serving Gateway (S-GW) in terms of processing power in our simulations. The second was a dual quad core (8 core) machine with 160GB of memory which will model our Packet Data Network Gateway (P-GW) in our simulations in terms of processing power. Furthermore, we took advantage of the 'config profile_rules' command in Snort's configuration file to acquire profiling statistics similar to Figure 4.1. To obtain the most precise scientific results possible, we followed the subsequent methodology. We progressed with just two rules; one rule that takes advantage of the BM algorithm (using the 'content' keyword) and the other takes advantage of NFA RegEx algorithm (using the 'pcre' keyword). We profiled



```
timestamp: 1275161029
Rule Profile Statistics (all rules)
==========================================================
   Num     SID GID Rev    Checks   Matches   Alerts        Microsecs  Avg/Check  Avg/Match
   ===     === === ===    ======   =======   ======        =========  =========  =========
     1 1000001   1   0       2           2      1             134        67.1       67.1
```

Figure 4.1: Rule Profiling Snapshot

Algorithm/ Machine Type	Boyer-Moore/ 160 Bytes VoIP Packet (μs)	NFA-RegEx/ 160 Bytes VoIP Packet (μs)	Total Time/ 160 Bytes VoIP Packet (ms)
Dual Core (S-GW)	2671.8	8465.63	11.3
Dual Quad-Core (P-GW)	641.25	1021.25	1.67

Table 4.1: VoIP SPIT Profiling Results

Algorithm/ Machine Type	Boyer-Moore/ SMTP Packet (ms)	NFA-RegEx/ SMTP Packet (ms)	Total Time/ SMTP Packet (ms)
Dual Core (S-GW)	23.96	75.34	99.3
Dual Quad-Core (P-GW)	5.79	6.29	15.08

Table 4.2: SMTP SPAM Profiling Results

those rules independently using ten data samples ranging from 2KB to 1024KB and for each sample we ran the profiling procedure ten times. To further develop the results, and after using simple Linux commands including 'grep, pipe and wordcount (wc)' on Snort rule-set directory, we unveiled that in a default Snort distribution there is approximately 4000 rules in which 57% of them utilize Boyer-Moore and 43% utilize NFA Regular Expressions. Moreover for practical reasons, we assumed that only 20% of the rules will actually be employed to inspect the traffic [2]. As a result and acting upon the above assumptions, the results are summarized in Tables 4.1 & 4.2. According to our profiling results, the overhead of analyzing VoIP packets using both BM and NFA RegEx would be 11.3 milliseconds on a dual core machine (the S-GW) and 1.67 milliseconds on a dual quad core machine (the P-GW). On the other hand, the overhead of inspecting SMTP packets using both algorithms would be 99.3 milliseconds on the S-GW and 15.08 milliseconds on the P-GW.

[2] During the profiling procedure, we noticed that the percentage of rules being employed to inspect the traffic varied from 15% to 25%.

The previous outcome will be employed to simulate and analyze the effect of the mitigating algorithms when implemented on the 4G network infrastructure and that will be the foundation of our presented mobile security architectures and ultimately our proposed distributed approach.

4.2 Scenario I: RTP VoIP SPIT Flooding

In this section, we focus on RTP VoIP SPIT flooding in order to demonstrate its DoS impact on the LTE 4G mobile network. Our intention is to shed the light on the fact that 4G mobile networks are vulnerable to IP-based attacks which forces mobile network operators to preventively react to preserve their provided application services. Hence a security architectural solution is required and for that reason may be proposed on the 4G mobile network infrastructure.

4.2.1 Simulation Setup

For our simulations, we have utilized Opnet Modeler version 16.0 with the LTE specialized model [89] on a Windows 7 machine, running a quad core 2.5GHZ CPU with 4GB of memory. The simulated architecture illustrated in Figure 4.2, consists of 720 Internet connected nodes [3], 1 PDN-GW, 7 S-GWs, 7 eNBs/1S-GW (49 eNBs in total) and 100 UEs/1eNB (4900 simultaneous UEs). We believe that this topology is very close to depict a realistic 4G network deployment in a large city. Additionally, the links configuration [4] is given in Table 4.3.

[3] According to our simulations, this number of nodes is the minimum number that will cause a VoIP DoS

[4] Our intention by selecting this broad bandwidth links configuration is to eliminate any possible delay caused by the links

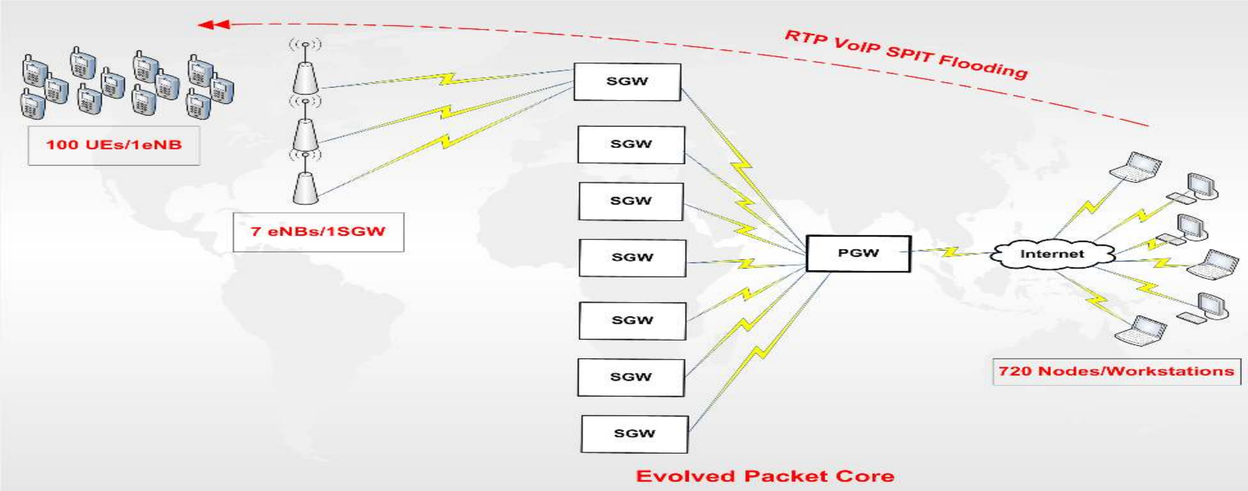


Figure 4.2: SPIT Flooding Topology

Link	Type	Bandwidth
eNode-EPC	Ethernet-1000BX	1 Gbps
EPC-Internet	PPP-Sonet-OC48	2.37 Gbps
Internet-WorkStation	PPP-Sonet-OC24	1.18 Gbps

Table 4.3: Links Configuration

4.2.2 RTP VoIP SPIT Flooding Impact

In this section, we aim at manipulating the traffic parameters of the scenario of Figure 4.2 to model the network environment in two cases; the first case illustrates the network under normal functionality and the second case demonstrates the network under an RTP VoIP SPIT flooding attack. Having accomplished that, we will be capable to compare both scenarios, specifically the average end-to-end delay for voice packets metric, the one-way jitter metric and the VoIP packet loss rate metric, and thus analyze the feasibility and impact of the attack on the QoS and availability of the VoIP application service on LTE 4G mobile networks.

Normal Network Load

According to [6], the mobile broadband data traffic is divided according to the following: 40% is data (Http/Ftp/Email), 20% is peer-to-peer, 10% is audio and 30% is video traffic. Therefore, modeling those distributions on the 4G mobile network will provide us with a baseline that highly replicates a normal network functionality scenario. We simulated that traffic for 30 minutes in accordance with the proposed scenario of Figure 4.2 and the simulation parameters of Section 4.2.1. Specifically, we configured the workstations to initiate the various traffic services and communicate with the UEs in a random manner.

Network Load Under RTP SPIT Flooding Attack

To model the network under the RTP VoIP SPIT flooding attack, we presume that the workstations have been exploited by malicious bots and aim to flood the mobile network, more specifically, the user equipments with VoIP SPIT. Under the same parameters defined in Section 4.2.1, we setup and ran the simulation for 30 minutes. Figures 4.3, 4.4 and 4.5 depict our simulation results of both case scenarios. Under a normal network load, the three critical VoIP QoS metrics are acceptable, tolerable and conform with ITU recommendations as discussed in Section 1.4.1. This is demonstrated when the average end-to-end delay for voice packets ranges from 69 ms to 75 ms (Figure 4.3), the average one-way jitter is below 30 ms (Figure 4.4) and the VoIP packet loss rate is almost negligible (Figure 4.5). On the other hand and under the RTP VoIP SPIT flooding attack, the results disclose the severe impact of the attack on the QoS and availability of the VoIP service on the LTE 4G mobile network. This is revealed in Figure 4.3 when the average end-to-end delay for voice packets surpasses the 400 ms threshold just after 5 minutes of attack simulation time.

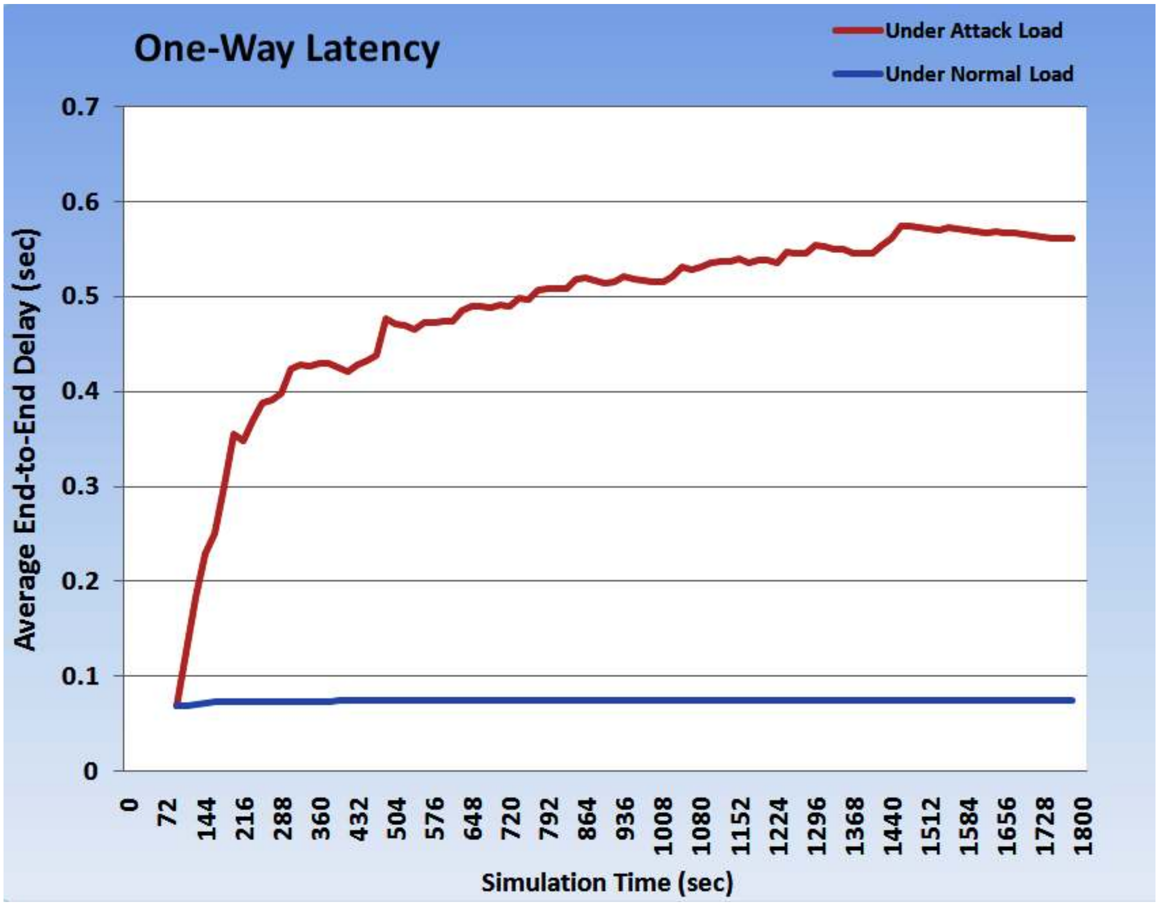


Figure 4.3: Avg.One Way Latency - Normal Load Vs Attack Load

Moreover, the average one-way jitter peaks at 460 ms (Figure 4.4) and the VoIP packet loss rate is around 33% (Figure 4.5). These indicators [5] strongly imply the feasibility of RTP VoIP SPIT flooding attacks on LTE mobile networks, in which a severe unacceptable and intolerable degradation in VoIP QoS occurs, causing a DoS to the VoIP application service on the mobile network as confirmed by the discussion in Section 1.4.1.

[5] These simulation based results should not be taken as absolute values on real LTE network systems, rather they depict the feasibility and severity of such attacks. In addition, we use them to show relative service improvements under our proposed distributed architecture.

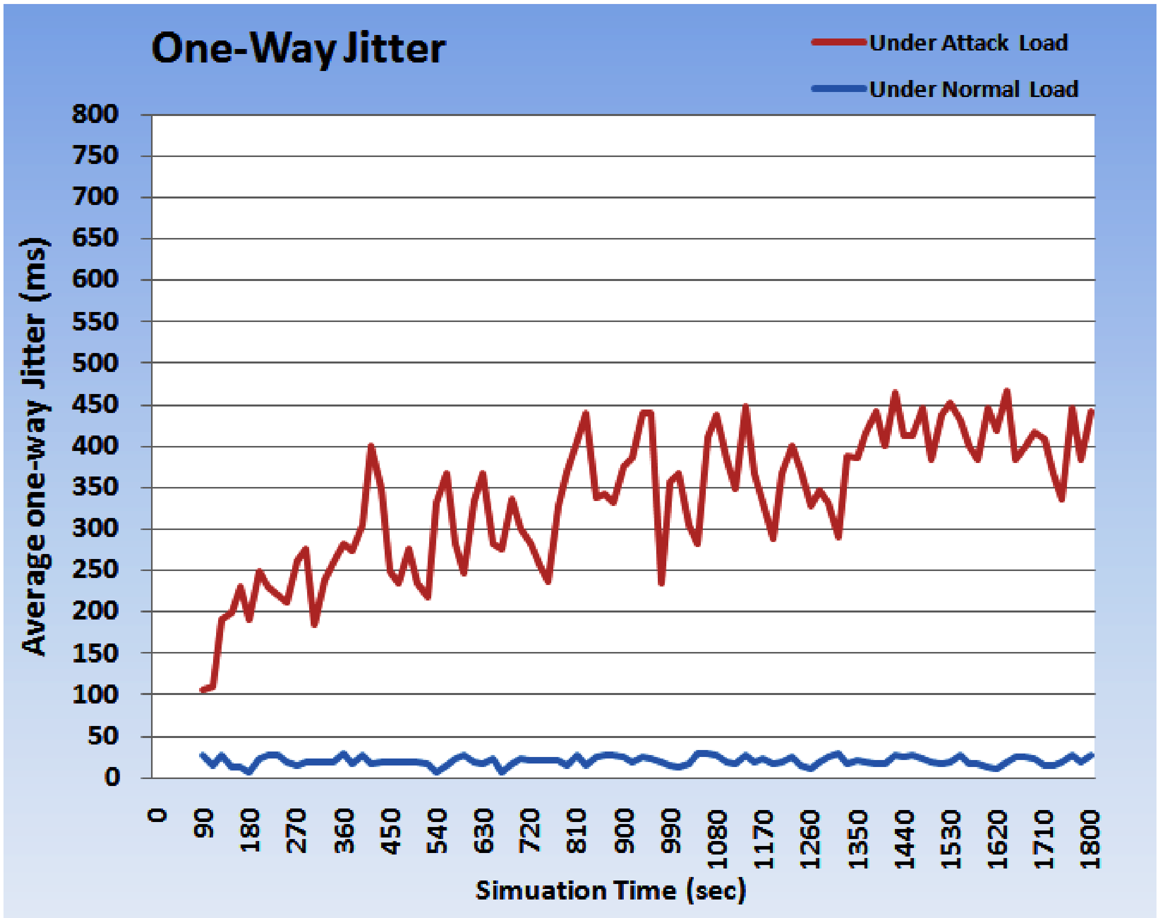


Figure 4.4: Avg. One-Way Jitter - Normal Load Vs Attack Load

Therefore, in order for mobile network operators to mediate all the effects of the attack and preserve the VoIP service on the LTE network, a mitigating security architecture must be implemented and validated.

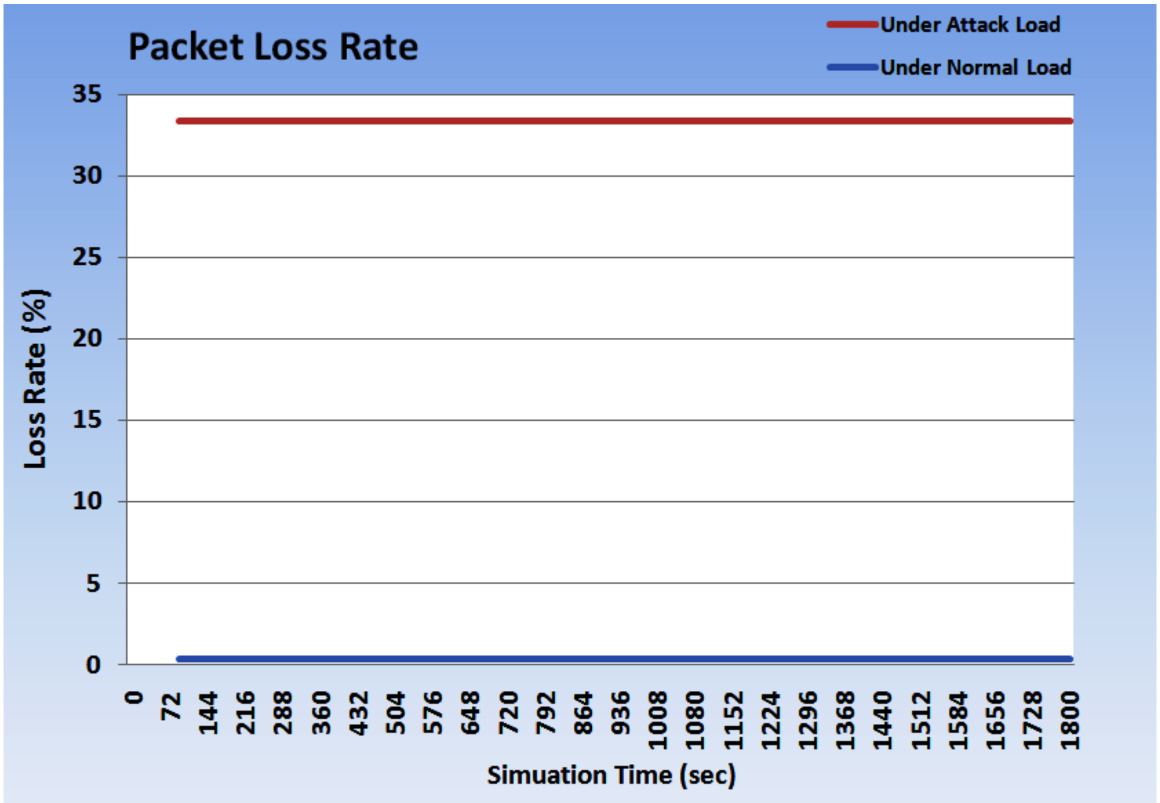


Figure 4.5: VoIP Packet Loss Rate - Normal Load Vs Attack Load

4.2.3 Simulation Results: SPIT Flooding Security Architectures

Centralized Architecture

In this scheme that is based on the conventional centralized network security architecture, we propose to add both mitigating algorithms (BM & NFA RegEX) in the Packet Data Network Gateway as discussed in Section 3.7 and depicted in Figure 3.4. We achieve this by adding the detection/packet filtering delay that we acquired from the profiling results of Section 4.1 to the P-GW as packet processing delay. Note that our profiling results take into consideration the processing power of the P-GW and thus represent a realistic approach to the filtering/detection power of the P-GW.

Distributed Architecture

This scheme proposes a distributed architecture as discussed in Section 3.7 and depicted in Figure 3.5. Hence, we distributed the mitigating algorithms on the S-GWs, utilizing the profiling results from Section 4.1 and implementing them as packet processing delay. It is worthy to mention that we assume that the different S-GW nodes act independently on the traffic to perform the detection. Additionally, note that our profiling results take into consideration the processing power of the S-GWs and thus represent a realistic approach to the filtering/detection power of S-GWs.

To demonstrate relative service improvements under our proposed distributed security architecture, we setup, implemented and simulated both security architectures under the RTP VoIP SPIT flooding attack for 20 minutes. It is creditable to note, that since we are implementing the same algorithms in both mitigating architectures where the algorithms are solely based on IP packets, we expected and assumed the same rate for false positives and false negatives.

Although the centralized architectural approach may be secure, however under the attack, it will cause an over dimensioning problem in the P-GW; since the exploited Internet workstation are generating huge number of RTP VoIP SPIT sessions, the P-GW will struggle to process and filter all the sessions. This fact is depicted in Figure 4.6 where the CPU Utilization of the P-GW hits 100% at the end of the simulation. Furthermore, this fact negatively affected the VoIP QoS metrics under this architecture. This is proven when the end-to-end delay for voice packets metric exceeds the 400 ms threshold (Figure 4.7), the average one-way jitter metric ranges from 80 ms to 140 ms (Figure 4.8) and the VoIP packet loss rate metric is around 19% (Figure 4.9).

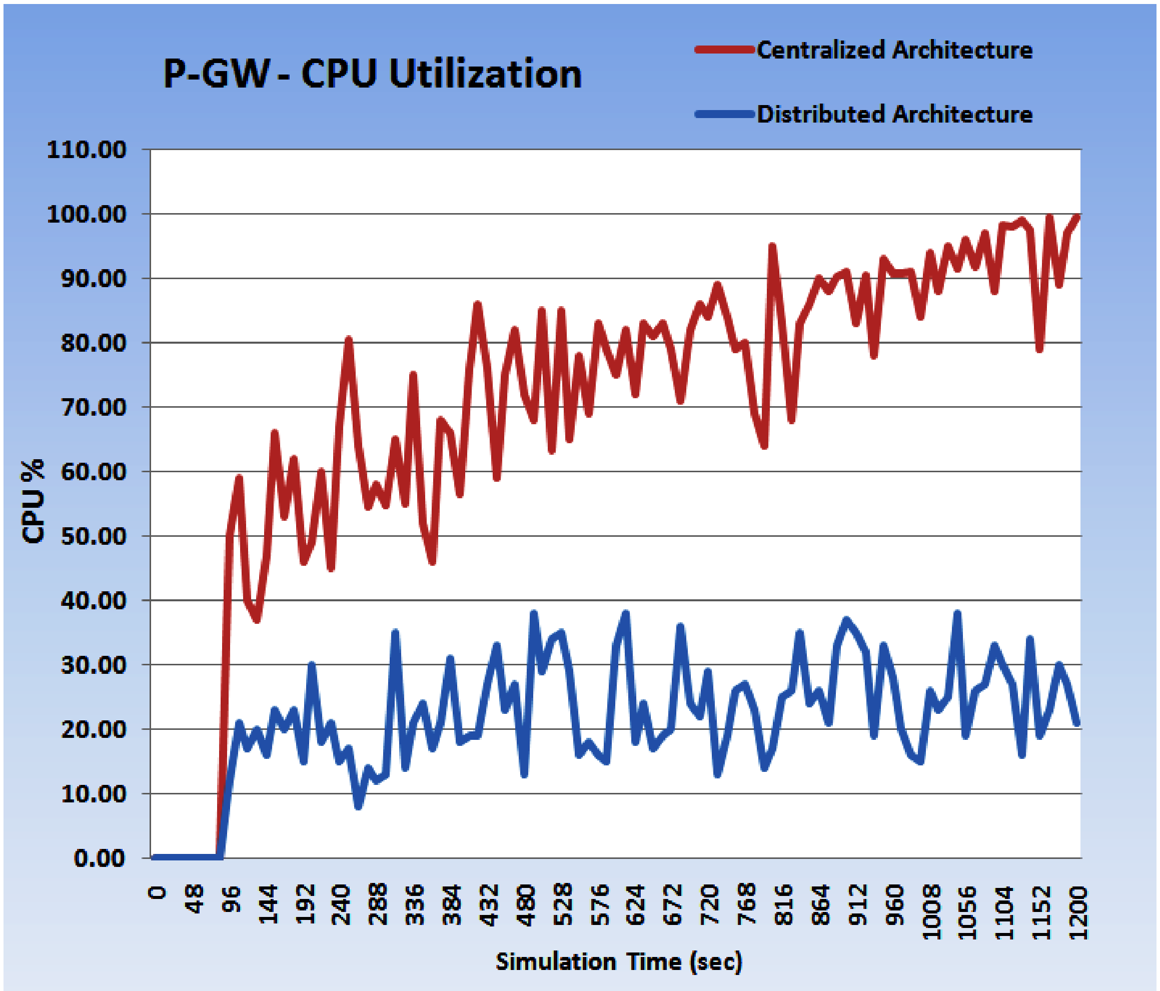


Figure 4.6: P-GW: CPU Utilization in Both Security Architectures

On the other hand, and comparing with the centralized architecture, our proposed distributed architectural approach, under the attack, is secure yet efficient. According to the simulation results, this architecture solves the over dimensioning problem in the P-GW as depicted in Figure 4.6 and preserves the VoIP service on the LTE network. The latter statement is confirmed and backed up by Figures 4.7, 4.8 and 4.9 where the end-to-end delay for voice packets metric, the one-way jitter metric and the VoIP packet loss rate metric were respectively more efficient, on average and

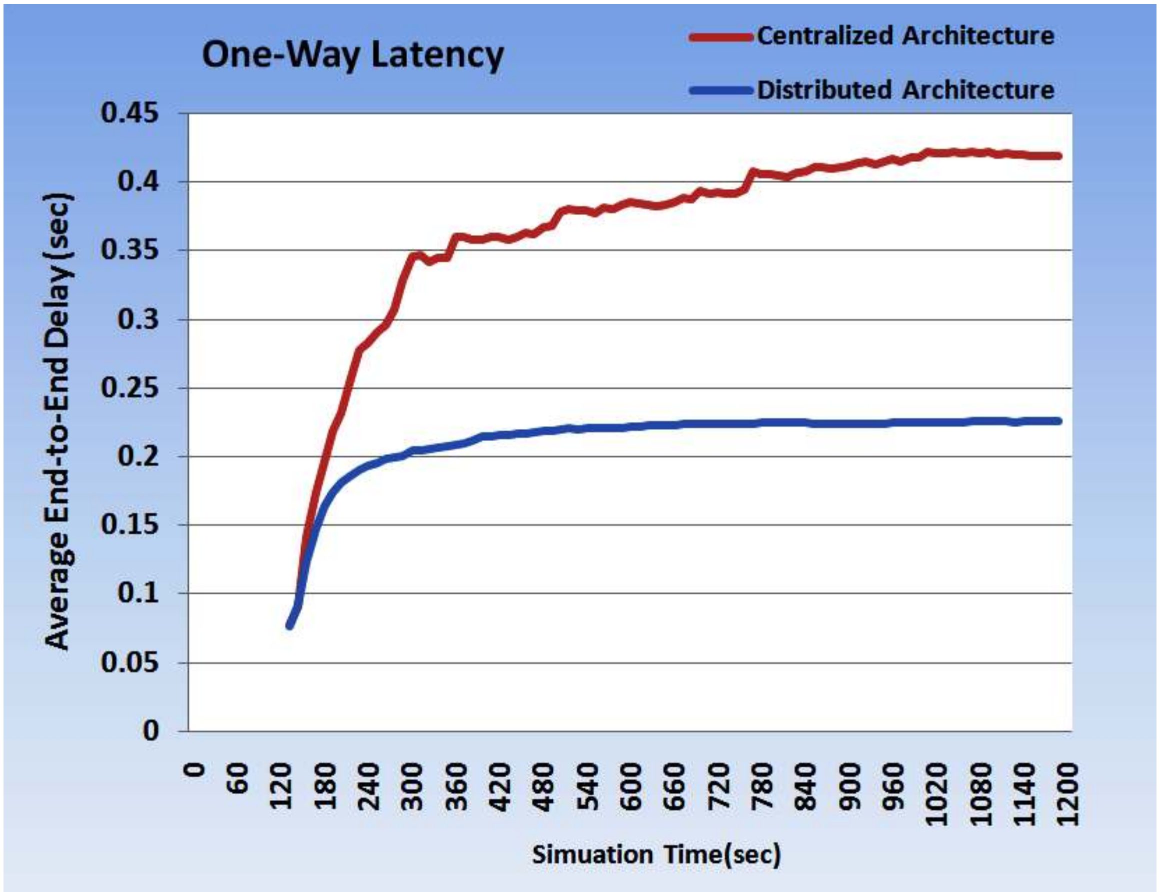


Figure 4.7: Avg. One Way Latency In Both Security Architectures

approximately, by 50%, 66% and 16% comparing with the conventional centralized architecture.

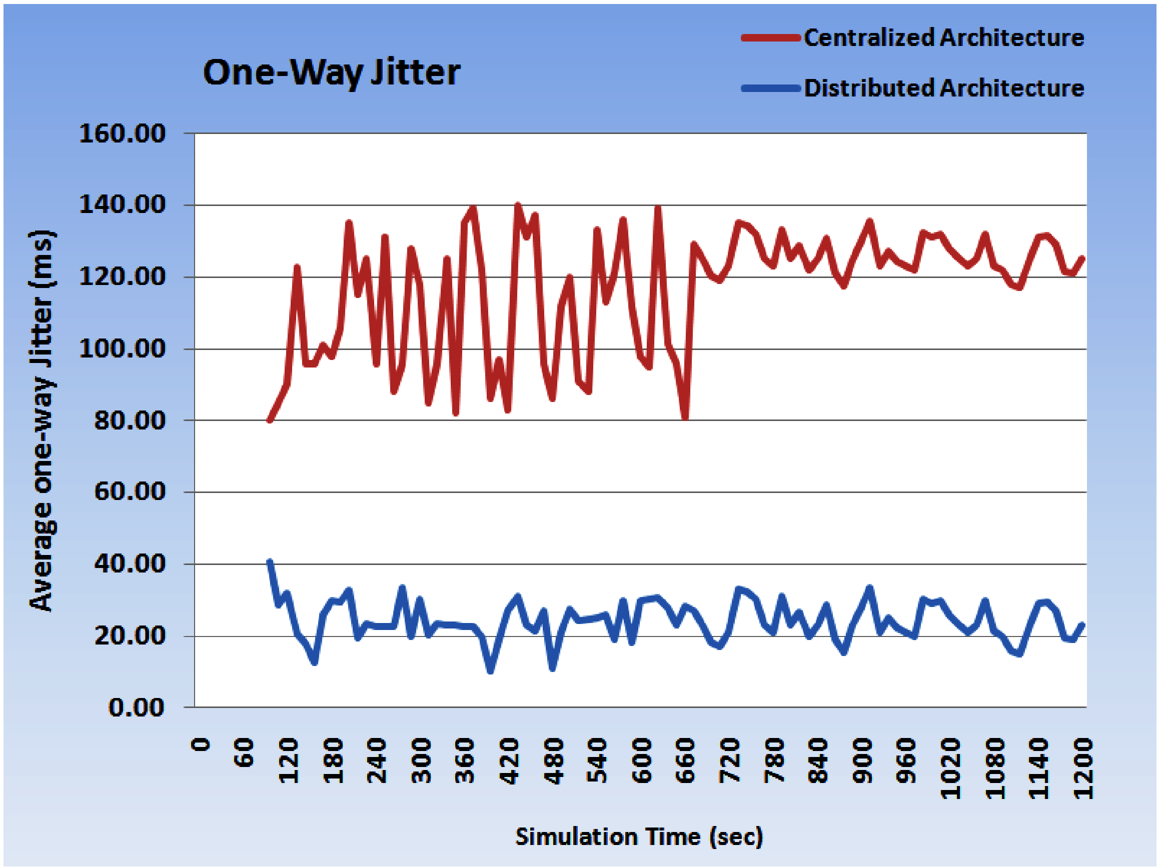


Figure 4.8: Avg. One-Way Jitter In Both Security Architectures

As a result, we affirm that this proposed scheme that is based on a distributed mobile network security architecture will not only achieve the security task of mediating the effects of the attack which will consequently preserve the VoIP application service on LTE 4G mobile networks, but will also preserve and provide efficiency to the mobile network in addition to being cost-effective for the reason mentioned in Section 3.7.

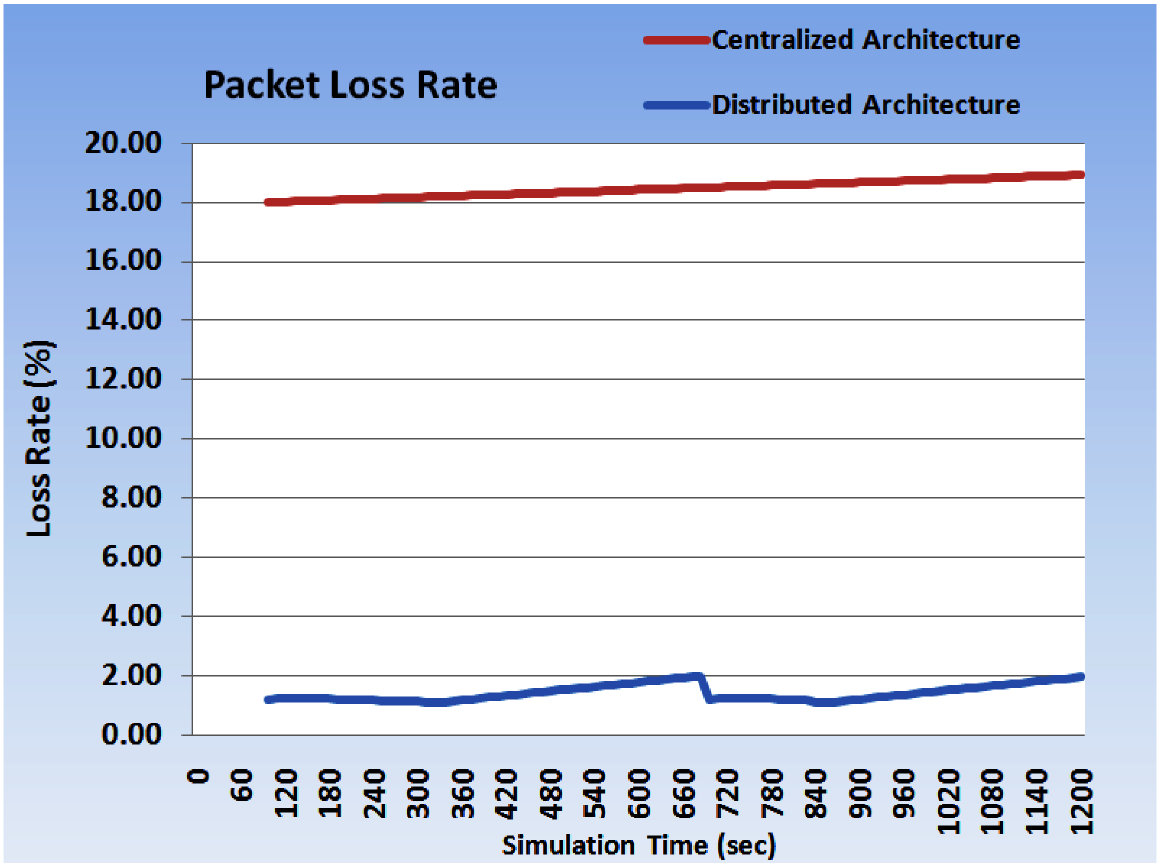


Figure 4.9: VoIP Packet Loss Rate In Both Security Architectures

4.3 Scenario II - SMTP SPAM Flooding

In the previous scenario, we have demonstrated that RTP VoIP SPIT flooding launched from the Internet towards the LTE network will trigger a DoS by denying the VoIP voice service. However, by implementing our proposed distributed architecture on the 4G network, we were able to mediate the effect of the attack and at the same time provide and preserve the efficiency of the network. In this scenario, we further experiment the feasibility of triggering a DoS from within the LTE network and consequently the effectiveness of our proposed distributed security architecture by studying another application service under a different attack scenario which is illustrated in Figure 4.10. The topology consists of the operator's SMTP Server, 1 P-GW, 7 S-GWs, 7 eNBs/1S-GW

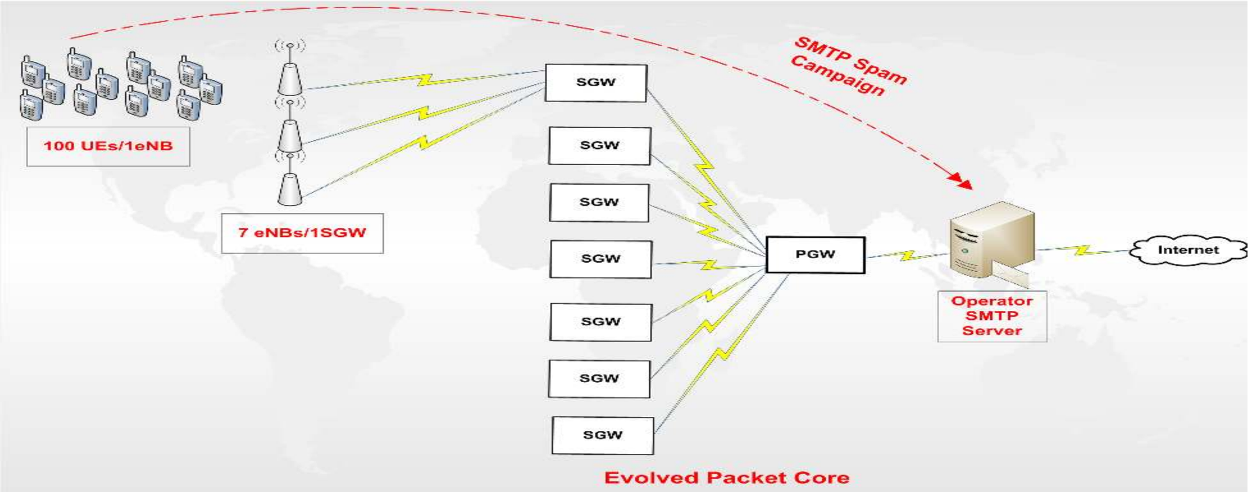


Figure 4.10: SMTP SPAM Flooding Topology

and 100 UEs/1eNB. Other parameters are similar to those mentioned in Section 4.2.1.

4.3.1 Scenario Rationale

With the ever increase flourishing of multi-vendor UEs and various complex applications being developed for diverse, advanced and unsecured mobile operating systems, it is deemed that UEs will be exploited for malicious purposes. According to [90], approximately 40% of all Android applications are low quality applications. This means that these applications may have not been verified and most probably will contain issues with programming, functionality and more critically security. This fact was greatly established recently when Google removed a group of applications from its Android Market after it was discovered that they contained malicious code that could be used to send SMS SPAM [91]. Moreover in 2009, a major mobile botnet was identified by the name ‘Ikee.B’ [92] that targeted UEs running Apple’s mobile operating system. Hence specifically in this scenario, we demonstrate the feasibility of malicious exploited UEs from within the LTE network flooding the opertator’s SMTP server with email SPAM. As a result, this will cause a

DoS to the SMTP server by overloading it with unsolicited emails and hence denying it from processing legitimate email requests in a timely manner. Furthermore more critically, will cause the operator's SMTP server to be blacklisted by Internet DNS servers after being detected as a SPAM server. Consequently, this will adversely affect the operator's business, reliablity and reputation in addition to facing serious legal issues (e.g., under the Candian House Government Bill C-28 Act) for misusing the mobile infrastructure for Spamming purposes.

4.3.2 SMTP SPAM Flooding Impact

Similar to Section 4.2.2, we aim at manipulating the traffic parameters of the scenario of Figure 4.10 to model the network environment in two cases; the first case illustrates the network under normal functionality and the second case demonstrates the SMTP SPAM flooding attack targeting the operator's SMTP server. Having accomplished that, we will be capable to compare both scenarios and analyze the impact of the attack on the SMTP server in terms of its CPU Utilization and Email Processing Time (measured time from when a single email request arrives at the server to the time it is completely processed) as discussed in Section 1.4.2. Furthermore, we will be able to show the subsequent impacts of the attack on the mobile network operator.

Normal Network Traffic

Following the traffic distributions highlighted in [6], we simulated this scheme for 20 minutes. Specifically, we configured the UEs to initiate the various traffic services and communicate with the corporate SMTP server and their corresponding Internet servers.

SMTP Spam Flooding Attack

To model the SMTP Spam flooding against the SMTP server, we presume that the UEs have been exploited and aim to flood the operator's server with Spam email. In accordance with the topology of Figure 4.10, we setup and ran this attack scenario for 20 minutes.

Figures 4.11 and 4.12 respectively depict our simulation results of the operator's SMTP server's CPU Utilization and Email Processing Time in a normal network behavior scenario and under the SMTP SPAM flooding attack. The results reveal that under a normal load, the SMTP server is able to process emails in a very (almost negligible) timely manner (0.002 sec/email) and its CPU Utilization is very acceptable (max 15%).

On the other hand, the results disclose the severe impact of the SPAM flooding attack on the SMTP server. This is revealed when the server hits a steady 100% CPU Utilization after the 15th minute. Moreover, this fact drastically affected the server's ability to process email requests in a timely manner in which this task took an additional highly significant 4 seconds to complete causing a drastic bottleneck. Relating this to our DoS definition and discussion from Section 1.4.2, we assert that this attack successfully caused a DoS targeting the operator's SMTP Server.

It is extremely noteworthy to mention that this SPAM flooding will force as well the operator's SMTP server to be utilized as a SPAM server which will be ultimately identified and blacklisted by Internet DNS servers. Furthermore, the mobile network operator will be liable under the law since its infrastructure was misused. Therefore, to mediate all those effects, a security architecture

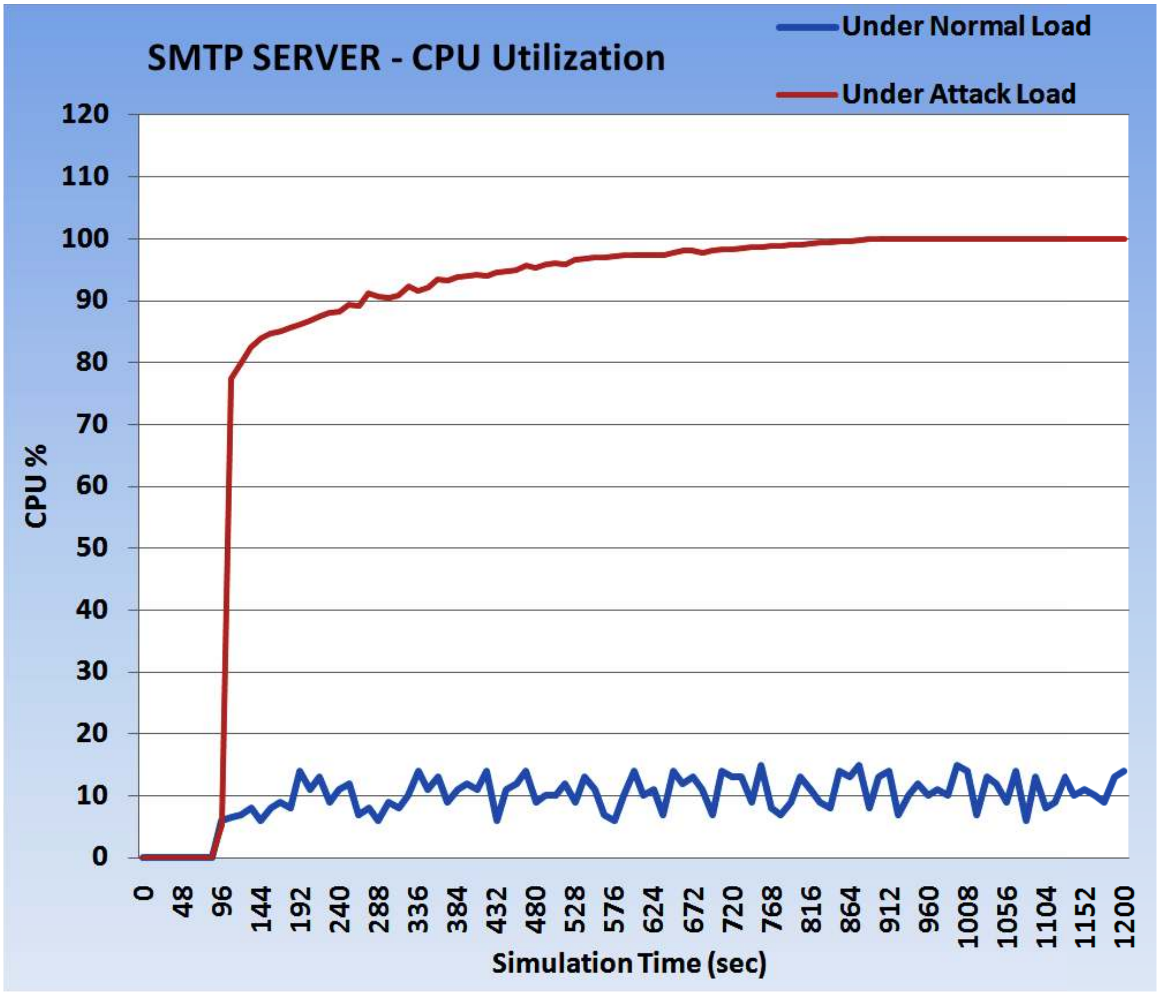


Figure 4.11: SMTP Server: CPU Utilization in Both Scenarios

must be implemented and validated.

4.3.3 SMTP Spam Flooding Security Architectures

Similar to Section 4.2.3, this section aims to implement and compare the conventional centralized security architecture and our proposed distributed architecture. Through additional simulation, we intend to reveal that our approach is secure and more efficient.

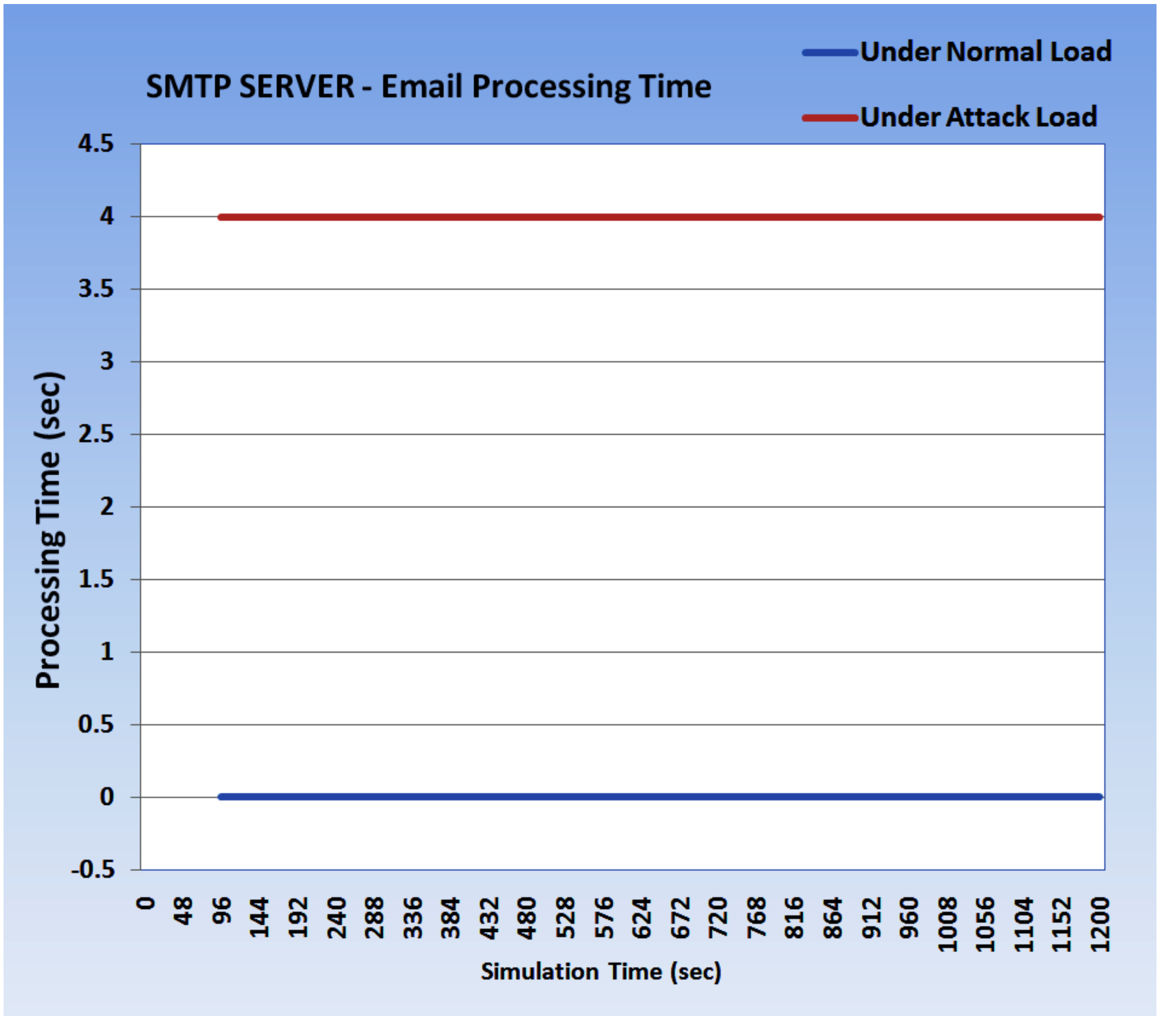


Figure 4.12: SMTP Server: Email Processing Time/Email in Both Scenarios

Centralized Vs Distributed Architectures

Following the same methodology of Sections 4.2.3 and 4.2.3, we implemented and simulated both security architectures for 20 minutes.

Although the centralized architecture may be secure, however under the attack, it will cause an over dimensioning problem in the P-GW; since the exploited UEs are generating huge number of SMTP SPAM sessions, the P-GW will struggle to process and filter all the sessions. This fact is depicted in Figure 4.13 where the CPU Utilization of the P-GW hits 70% and keeps steadily increasing. Thus, we confirm that the centralized architecture may be secure but not efficient and will affect the functionality of the LTE network.

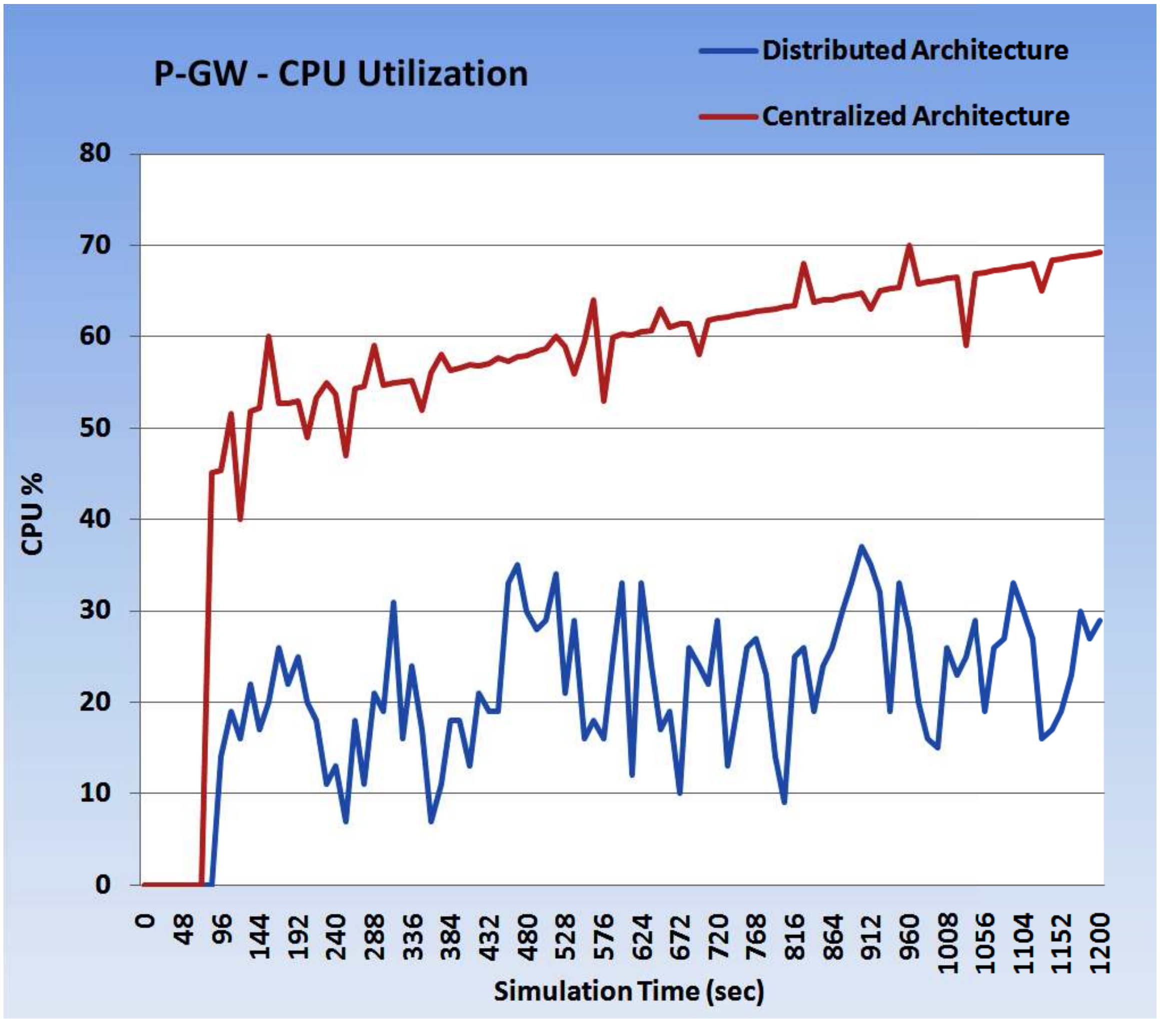


Figure 4.13: P-GW: CPU Utilization in Both Architectures

On the other hand and under the SMTP SPAM flooding attack, the results of our proposed distributed architecture on the SMTP Server's performance are illustrated in Figures 4.14 and 4.15. According to the simulation results, the distributed security architecture is secure and efficient. On one side, it will be able to mediate the effect of the SPAM flooding attack targeting the SMTP Server and at the same time preserve the efficiency of the LTE network. This is confirmed when the SMTP Server's CPU Utilization reaches a very reasonable maximum 30% (Figure 4.14) still permitting the server to process emails in a timely manner as depicted in Figure 4.15. In addition, this distributed architecture solved the over dimensioning problem caused by the centralized architecture as demonstrated in Figure 4.13. On the other side, it will mediate the significant subsequent effects of the attack which are characterized by the blacklisting of the operator's SMTP server and related legal issues.

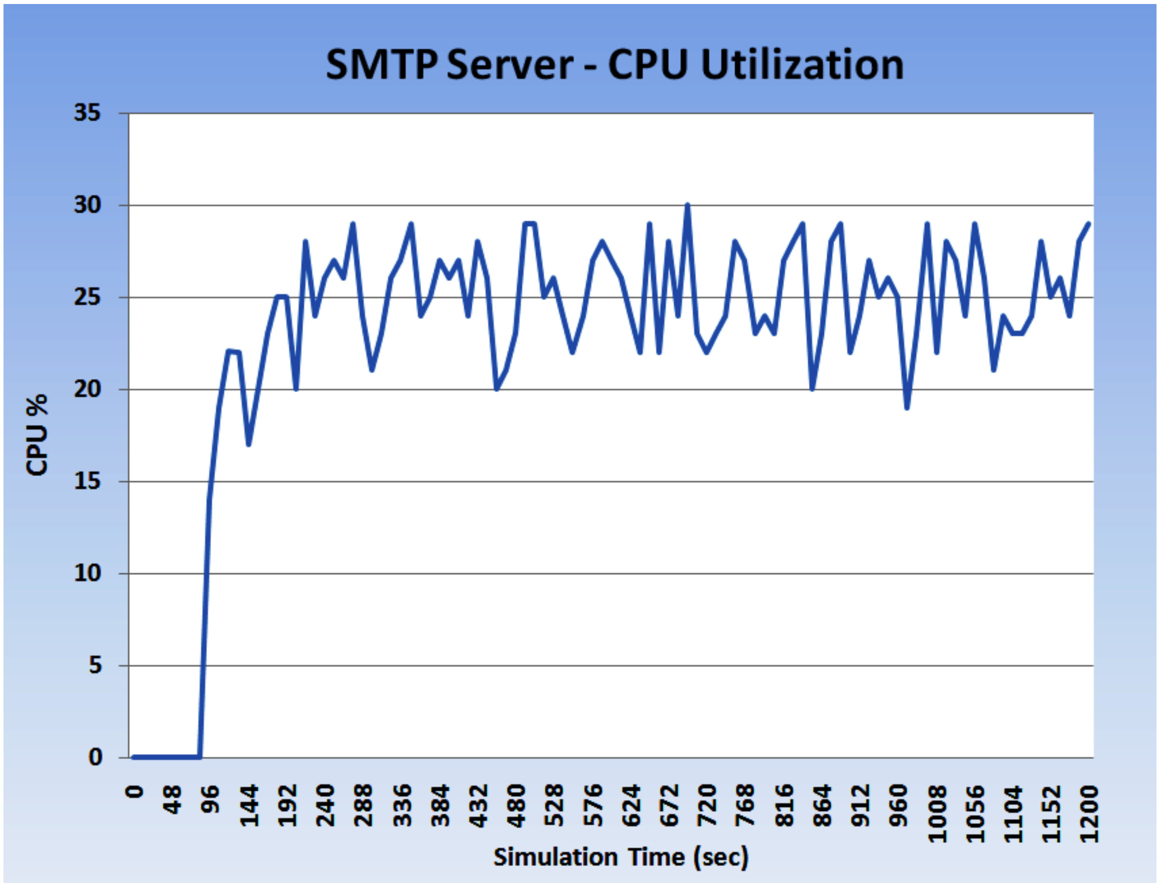


Figure 4.14: Distributed Architecture: SMTP SRV CPU Under Attack Load

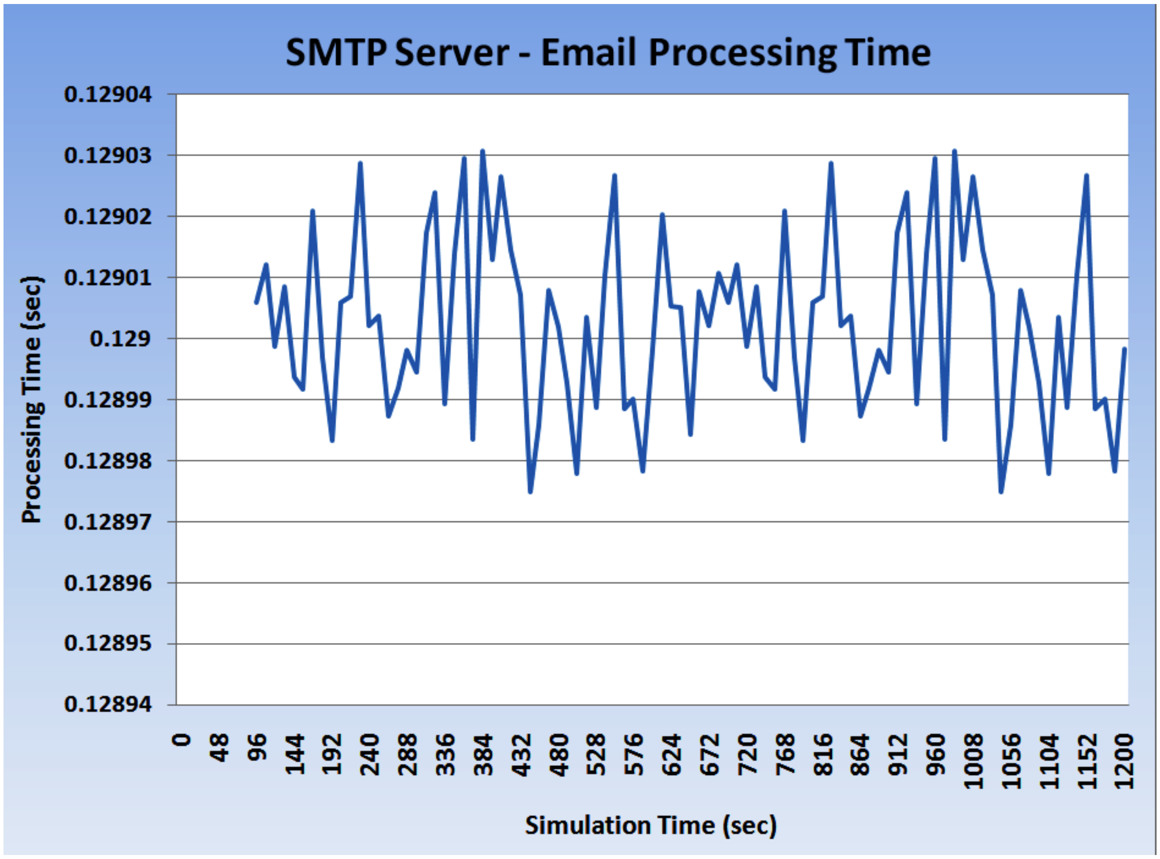


Figure 4.15: Distributed Architecture: SMTP SRV Email Processing Time/Email Under Attack Load

Chapter 5

Conclusion

In this thesis, we focused on two SPAM flooding attacks, namely RTP VoIP SPIT and SMTP SPAM and revealed, through performing large scale simulations, their feasibility and significant negative direct and indirect impacts on 4G mobile network. We confirmed that IP-based attacks, taking advantage of 4G's evolved packet core are feasible. Moreover, in an effort to mitigate the effects of the attack, we investigated generic detection algorithms employed by various IDSs. By utilizing Snort and performing profiling of rule-matching, we predicted the cost of the detection/filtering delay of the Boyer-Moore and NFA Regular Expression detection algorithms on LTE 4G's Serving Gateways and Packet Data Network Gateways. Consequently, we discussed various mitigating methods and secure mobile architectures. Additionally, we simulated, compared and analyzed the conventional centralized mobile security architecture and our proposed distributed security architecture. We concluded that our proposed architecture is secure by mitigating the effects of the RTP VoIP SPIT flooding attack, more efficient by solving the over dimensioning problem caused by the centralized architectural approach and cost-effective by utilizing 'of the shelf' low-cost hardware in the S-GW nodes.

5.1 Future Work

For future work, we are planning to target the following:

- Investigate the impact of other content matching algorithms such as the Aho Corasick string matching algorithm on the LTE network infrastructure,
- Study the feasibility of other IP based attacks and prevention mechanisms on the mobile network,
- Work on collaborative design approaches between various LTE nodes for SPAM flooding mitigation in 4G mobile networks.

Bibliography

[1] Skold Dahlman, Parkvall and Beming. *3G Evolution: HSPA and LTE for Mobile Broadband*. Academic Press, Oxford, UK, Second edition, 2008.

[2] 3gpp tr 25.913. requirements for evolved utra (e-utra) and evolved utran (e-utran). Available at: `http://www.3gpp.org`.

[3] LTE 3GPP Home Page. Available at: `http://www.3gpp.org/LTE`.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, 2002. Available at: `http://www.ietf.org/rfc/rfc3261.txt`.

[5] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications, 2003. Available at: `http://www.ietf.org/rfc/rfc3550.txt`.

[6] Mobile broadband traffic across regions 2009-2017-coda research consultancy ltd. laptops and netbooks, 2009.

[7] CISCO Systems. 3 simple reasons voip abuse will grow. Available at: http://www.networkworld.com/news/2011/030811-3-simple-reasons-voip-abuse.html?page=1.

[8] Spam over internet telephony. Available at: http://searchunifiedcommunications.techtarget.com/definition/SPIT.

[9] 3GPP. Technical specification group services and system aspects. Available at: ftp://ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_55_Shanghai/Docs/S3-090773.doc.

[10] Session description protocol. Available at: http://tools.ietf.org/html/rfc4566l.

[11] Simple Mail Transfer Protocol. Available at: http://tools.ietf.org/html/rfc5321t.

[12] Candian House Government Bill C-28 Act. Available at: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Bill=C28&Language=E&Mode=1&Parl=40&Ses=3.

[13] Itu-t recommendation g.114 : One-way transmission time, 2000. Available at: http://www.itu.int/rec/dologin_pub.asp?lang=e\&id=T-REC-G.114-200305-I!!PDF-E\&type=items.

[14] Recommendation itu-r bt.1363-1. Available at: www.catr.cn/radar/itur/201007/P020100714476973477437.pdf.

[15] Quality of service design overview. Available at: http://www.ciscopress.com/articles/article.asp?p=357102.

[16] Paul Ammann, Duminda Wijesekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, pages 217–224, New York, NY, USA, 2002. ACM.

[17] Hossein Bidgoli. *Handbook of Information Security*. John Wiley, 2006.

[18] K Hutchison. Wireless intrusion detection systems. Available at: http://www.sans.org/reading_room/whitepapers/wireless/ .

[19] R. K. Nichols and P. C. Lekkas. *Telephone System Vulnerabilities*. McGraw-Hill, 2002.

[20] Marco Domenico Aime, Giorgio Calandriello, and Antonio Lioy. A wireless distributed intrusion detection system and a new attack model. *Computers and Communications, IEEE Symposium on*, 0:35–40, 2006.

[21] Gavrilenko K. V. Mikhai-lovsky A. A Vladimirov, A. A. *Counterintelligence: Wireless IDS systems*. Pearson/Addison-Wesley, 2004.

[22] C. Low. Understanding wireless attacks & detection, 2005. Available at: http://www.hackerscenter.com/public/Library/782_wireattacks.pdf.

[23] V. Gupta, S. Krishnamurthy, and M. Faloutsos. Denial of service attacks at the MAC layer in wireless ad hoc networks. In *MILCOM 2002. Proceedings*, volume 2, pages 1118 – 1123 vol.2, 2002.

[24] Livio Ricciulli, Patrick Lincoln, and Pankaj Kakkar. TCP SYN Flooding Defense. In *In Proceedings of CNDS*, 1999.

[25] D. Sisalem, J. Kuthan, and S. Ehlert. Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms. *Network, IEEE*, 20(5):26 –31, sept.-oct. 2006.

[26] Ming Luo, Tao Peng, and C. Leckie. CPU-based DoS attacks against SIP servers. In *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, pages 41 –48, april 2008.

[27] Ruishan Zhang, Xinyuan Wang, Xiaohui Yang, and Xuxian Jiang. Billing attacks on SIP-based VoIP systems. In *Proceedings of the first USENIX workshop on Offensive Technologies*, pages 4:1–4:8, Berkeley, CA, USA, 2007. USENIX Association.

[28] Ruishan Zhang, Xinyuan Wang, Ryan Farley, Xiaohui Yang, and Xuxian Jiang. On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ASIACCS '09, pages 61–69, New York, NY, USA, 2009. ACM.

[29] E.Y. Chen. Detecting DoS attacks on SIP systems. In *VoIP Management and Security, 2006. 1st IEEE Workshop on*, pages 53 – 58, april 2006.

[30] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia. Fast Detection of Denial-of-Service Attacks on IP Telephony. In *Quality of Service, 2006. IWQoS 2006. 14th IEEE International Workshop on*, pages 199 –208, june 2006.

[31] Hongli Zhang, Zhimin Gu, Caixia Liu, and Tang Jie. Detecting VoIP-specific Denial-of-Service using change-point method. In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, volume 02, pages 1059 –1064, feb. 2009.

[32] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel. On spam over internet telephony (spit) prevention. *Communications Magazine, IEEE*, 46(8):80 –86, august 2008.

[33] He Guang-Yu, Wen Ying-You, and Zhao Hong. Spit detection and prevention method based on signal analysis. In *Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on*, volume 2, pages 631 –638, nov. 2008.

[34] Chen Hongchang, Chen Fucai, and Li Shaomei. A multilayered fusion method for spits detection. *Intelligent Computation Technology and Automation, International Conference on*, 1:30–33, 2011.

[35] Jun Wu, Xin Wang, Xiaodong Lee, and Baoping Yan. Detecting DDoS Attack towards DNS Server Using a Neural Network Classifier. In Konstantinos Diamantaras, Wlodek Duch, and Lazaros Iliadis, editors, *Artificial Neural Networks âĂŞ ICANN 2010*, volume 6354 of *Lecture Notes in Computer Science*, pages 118–123. Springer Berlin / Heidelberg, 2010. 10.1007/978-3-642-15825-415.

[36] Changhua Sun, Bin Liu, and Lei Shi. Efficient and Low-Cost Hardware Defense Against DNS Amplification Attacks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1 –5, 30 2008-dec. 4 2008.

[37] Ashley Chonka, Yang Xiang, Wanlei Zhou, and Alessio Bonti. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*, In Press, Corrected Proof:–, 2010.

[38] Michael Still and Eric Charles McCreath. DDoS Protections for SMTP Servers. *International Journal of Computer Science and Security (IJCSS)*, abs/0912.1815:537 – 550, 2011.

[39] Rajinder Kumar, Amandeep Jindal, and Kunal Pandove. Article: Launching email spoofing attacks. *International Journal of Computer Applications*, 5(1):21–22, August 2010. Published By Foundation of Computer Science.

[40] New York Times. Yahoo attributes a lengthy service failure to an attack. `http://partners.nytimes.com/library/tech/00/02/biztech/articles/08yahoo.html`.

[41] M.Z. Rafique, M. Ali Akbar, and M. Farooq. Evaluating DoS Attacks against Sip-Based VoIP Systems. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1 –6, 30 2009-dec. 4 2009.

[42] Hongli Zhang, Zhimin Gu, Caixia Liu, and Tang Jie. Detecting voip-specific denial-of-service using change-point method. In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, volume 02, pages 1059 –1064, feb. 2009.

[43] ZDnet. Leading web sites under attack. `http://news.cnet.com/2100-1017-236683.html`.

[44] Naoum Naoumov and Keith Ross. Exploiting P2P systems for DDoS attacks. In *Proceedings of the 1st international conference on Scalable information systems*, InfoScale '06, New York, NY, USA, 2006. ACM.

[45] Karim El Defrawy, Minas Gjoka, and Athina Markopoulou. BotTorrent: misusing BitTorrent to launch DDoS attacks. In *Proceedings of the 3rd USENIX workshop on Steps to reducing unwanted traffic on the internet*, pages 1:1–1:6, Berkeley, CA, USA, 2007. USENIX Association.

[46] P.P.C. Lee, Tian Bu, and T. Woo. On the Detection of Signaling DoS Attacks on 3G Wireless Networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1289 –1297, May 2007.

[47] Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 223–234, New York, NY, USA, 2009. ACM.

[48] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting open functionality in SMS-capable cellular networks. In *Proceedings of the 12th ACM conference on Computer and communications security*, CCS '05, pages 393–404, New York, NY, USA, 2005. ACM.

[49] Bo Zhao, Caixia Chi, Wei Gao, Sencun Zhu, and Guohong Cao. A Chain Reaction DoS Attack on 3G Networks: Analysis and Defenses. In *INFOCOM 2009, IEEE*, pages 2455 –2463, 2009.

[50] SecureList. Worm.symbos.cabir.a. Available at: http://www.securelist.com/en/descriptions/old60663.

[51] Symantec. Symbos.mabir. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2005-040414-1543-99.

[52] F-Secure. Trojan:symbos/skulls.a. Available at: http://www.f-secure.com/v-descs/skulls.shtml.

[53] IEEE. Ieee standard association. Available at: http://standards.ieee.org/about/get/802/802.16.html.

[54] IEEE. Ieee standard 802.16. Available at: ieee802.org/16/docs/02/C80216-0205.pdf.

[55] Taeshik Shon and Wook Choi. An analysis of mobile wimax security: Vulnerabilities and solutions. In Tomoya Enokido, Leonard Barolli, and Makoto Takizawa, editors, *Network-Based Information Systems*, volume 4658 of *Lecture Notes in Computer Science*, pages 88–97. Springer Berlin / Heidelberg, 2007. 10.1007/978-3-540-74573-010.

[56] D. Johnston and J. Walker. Overview of ieee 802.16 security. *Security Privacy, IEEE*, 2(3):40–48, may-june 2004.

[57] Muxiang Zhang and Yuguang Fang. Security analysis and enhancements of 3gpp authentication and key agreement protocol. *Wireless Communications, IEEE Transactions on*, 4(2):734 – 742, march 2005.

[58] Wen-Shenq Juang and Jing-Lin Wu. Efficient 3gpp authentication and key agreement with robust user privacy protection. In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pages 2720 –2725, march 2007.

[59] Muxiang Zhang and Yuguang Fang. Security analysis and enhancements of 3gpp authentication and key agreement protocol. *Wireless Communications, IEEE Transactions on*, 4(2):734 – 742, march 2005.

[60] Frederik Armknecht, Joseph Lano, and Bart Preneel. Extending the resynchronization attack. In Helena Handschuh and M. Hasan, editors, *Selected Areas in Cryptography*, volume 3357 of *Lecture Notes in Computer Science*, pages 19–38. Springer Berlin / Heidelberg, 2005. 10.1007/978-3-540-30564-42.

[61] Zahid Ghadialy. High speed uplink packet access (hsupa): A tutorial. Available at: `http://www.3g4g.co.uk/Tutorial/ZG/zg_hsupa.html`.

[62] Jolly Parikh and Anuradha Basu. Article: Lte advanced: The 4g mobile broadband technology. *International Journal of Computer Applications*, 13(5):17–21, January 2011. Published by Foundation of Computer Science.

[63] A. Furuskar, Jing Rao, M. Blomgren, and P. Skillermark. Lte and hspa for fixed wireless broadband: Datarates, coverage, and capacity in an indian rural scenario. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1 –5, 28 2011-march 3 2011.

[64] Ericsson. Lte-an introduction. Available at: www.ericsson.com/res/docs/whitepapers/lte_overview.pdf.

[65] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall. Lte: the evolution of mobile broadband. *Communications Magazine, IEEE*, 47(4):44 –51, april 2009.

[66] 3GPP. 3gpp specification series. Available at: http://www.3gpp.org/ftp/Specs/html-info/36-series.htm.

[67] K. Ravi and Mohammed Ali Hussain. 4G Mobile Broadband, LTE Network Architecture and Protocol Stack . *International Journal of Research and Reviews in Ad Hoc Networks*, 1(1), March 2011.

[68] DVB. Standards and bluebooks. Available at: http://www.dvb.org/technology/standards/.

[69] Cisco. Technology white paper. Available at: http://www.cisco.com/en/US/tech/tk722/tk809/tech_white_papers_list.html/.

[70] Cisco. Wimax. Available at:http://www.cisco.com/en/US/netsol/ns811/networking_solutions_solution_category.html/.

[71] Iternational Telecommunication Union. Itu g.992.5. Available at: http://www.itu.int/rec/T-REC-G.992.5/en.

[72] Malcolm Robb. Spam mitigation techniques. Available at: caia.swin.edu.au/talks/CAIA-TALK-070221A.pdf.

[73] Engineering World Academy of Science and Technology. Application of exact string matching algorithms towards smiles representation of chemical structure, 2007.

[74] Margaritis K. G. Michailidis, P. D. On-line string matching algorithms: survey and experimental results. volume 76 of *International Journal of Computer Mathematics*. Taylor and Francis, 2001.

[75] Christian Charras and Thierry Lecroq. *Handbook of Exact String Matching Algorithms*. King's College Publications, 2004.

[76] Randy Smith Cristian Estan Somesh Jha. Xfa: Faster signature matching with extended automata.

[77] Algorithms to accelerate multiple regular expressions matching for deep.

[78] Michela Becchi and Patrick Crowley. An improved algorithm to accelerate regular expression evaluatio, September 2076.

[79] Advanced algorithms for fast and scalable deep packet inspection.

[80] Snort. Available at: `http://www.snort.org/`.

[81] Barracuda networks. Available at: `http://www.barracudanetworks.com/ns/products/web-filter-features.php`.

[82] Bro intrustion detection system. Available at: `http://www.bro-ids.org/`.

[83] Next generation intrusion detection and prevention engine. Available at: `http://www.openinfosecfoundation.org/index.php/download-suricata/`.

[84] Clearmymail. Available at: http://www.consumersearch.com/spam-filters/clearmymail.

[85] Cloudmark desktop. Available at: http://www.consumersearch.com/spam-filters/cloudmark-desktop.

[86] Spamfighter. Available at: http://www.consumersearch.com/spam-filters/spamfighter.

[87] R.Stonei. Centertrack: an IP overlay network for tracking DoS floods. In *In Proc of the 9th conf. on USENIX Security Symposium*, volume 9, pages 15–15, 2000.

[88] Open Group. Secure mobile architecture vision and architecture. Available at: https://www2.opengroup.org/ogsys/protected/publications/viewDocument.html?publicationid=11306&documentid=10638.

[89] Opnet LTE Specialized Model. Available at: http://www.opnet.com/LTE/.

[90] AppBrain. Number of available android applications. Available at: http://www.appbrain.com/stats/number-of-android-apps.

[91] Threat Post. SMS Trojan Found in Several Android Apps. available at: http://threatpost.com/en_us/blogs/sms-trojan-found-several-android-ap ps-051211?utm_source=Newsletter_051311\&utm_medium=Email+Marketing\&utm_cam.

[92] Hassen Saidi Phillip Porras and Vinod Yegneswaran. An analysis of the ikee.b (duh) iphone botnet. Available at: http://mtc.sri.com/iphone/.