A First Look on the Effects and Mitigation of VoIP SPIT Flooding in 4G Mobile Networks

Elias Bou-Harb
CIISE, Concordia University
Montreal, Quebec, Canada
e_bouh@encs.concordia.ca

Mourad Debbabi
CIISE, Concordia University
Montreal, Quebec, Canada
debbabi@ciise.concordia.ca

Chadi Assi
CIISE, Concordia University
Montreal, Quebec, Canada
assi@ciise.concordia.ca

***Abstract*—The fourth generation of mobile networks is considered a technology-opportunistic and user-centric system. Part of its new architecture, 4G 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 to mitigate such attacks is based on a centralized security architecture. This centralized approach nonetheless, requires large processing resources to handle large amount of traffic, which may result in a significant over dimensioning problem in the centralized nodes causing this approach to fail from achieving its security task.**

In this paper, we primarily contribute by presenting a first look on the DoS effects of VoIP SPIT flooding on 4G mobile networks. We further contribute by proposing a distributed architecture on the mobile network infrastructure that is secure, efficient and cost-effective.

I. Introduction

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. Part of its new architecture, 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 ubiquitous IP access from any network to and from 4G networks in addition to providing various critical advantages. 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. Voice over IP (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 [1] and the Real Time Protocol (RTP) [2]. 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 [3]. However, in a recent report [4], Cisco Systems predicted that VoIP abuse will grow significantly in the very near future. A specific misdemeanor against VoIP is coined SPAM Over Internet Telephony (SPIT) [5]. SPIT refers to unsolicited calls intended for advertising, social engineering and more severely bandwidth and processing utilization. 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 [6], where they quantified that approximately 250 GB of SPIT traffic per month could be generated from only one SPIT bot [7], making SPIT an attack vector of very real significance and hence, interesting to study especially on 4G mobile networks. 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 quality of service (QoS) of mobile users and ultimately denies the service on 4G networks.

A. Defining DoS for VoIP SPIT Flooding

In this paper, we present a first look on the DoS effects of VoIP SPIT flooding on 4G mobile networks. Our intention is to shed the light on the fact that such 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 network infrastructure. Moreover, for clarification purposes, we explain in the following when exactly will a DoS occur in the attack scenario. When using VoIP, there are three critical metrics that determine the QoS:

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

The International Telecommunication Standardization Union (ITU) recommends the following limits for voice one-way latency [8]:

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

On the other hand, the ITU-R advocates that the average one-way jitter and the packet loss rate should be targeted at less than 30 ms [9] and 1% [10] respectively. In this paper, 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 and the VoIP packet loss rate surpass the mentioned

978-1-4577-2053-6/12/$31.00 ©2012 IEEE

thresholds, then a severe and unacceptable degradation in VoIP QoS will occur, prohibiting or denying the service on 4G networks. Additionally, we will use those metrics to show relative service improvements, under the attack, after implementing our proposed distributed architecture. The rest of the paper is organized as follows. Section II overviews a brief background while Section III explains the 4G architectural infrastructure. VoIP SPIT flooding mitigating methods and secure mobile architectures are discussed in Sections IV & V. Furthermore, Section VI reveals the algorithms' profiling discussion and results, portrays our topological simulation scenario and illustrates the attack and countermeasure simulation results. Finally, Section VII summarizes our contributions and concludes this work.

II. Background

To the best of our knowledge, 'VoIP SPIT flooding' attacks and mitigation architectures in the context of '4G mobile networks' have not been studied before. However in the past few years, various papers discussed attacks against VoIP. Sisalem et al. [11] 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. In another closely related work, Luo et al. [12] 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 [13] examined how the vulnerabilities of SIP can be exploited to compromise the reliability and trustworthiness of the billing of SIP-based VoIP systems. In another interesting study, Zhang et al. [14] 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 attacks on VoIP by exploiting DNS and VoIP implementation vulnerabilities. Detection methods for such attacks and others on VoIP were also discussed in the literature. In [15], the author proposed a method to detect DoS attacks that involve flooding SIP entities with illegitimate SIP messages. Furthermore, Sengar et al. [16] presented an online statistical detection mechanism, called vFDS, to detect DoS attacks in the context of VoIP. Additionally, the authors of [17] 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.

III. 4G Architecture

In this section we present the 4G network architecture and describe its elements and corresponding functionalities. The 4G system is comprised of two networks: the E-UTRAN and the Evolved Packet Core (EPC) [18]. 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 and advanced antenna techniques. E-NBs interface with user equipments (UEs) and perform numerous functions including radio resource management, admission control, scheduling, ciphering/deciphering and compression/decompression of user and control plane data. The packet domain of 4G networks is called the EPC. It is a flat all-IP system designed to provide much higher packet data rates and significantly lower-latency. It consists of six nodes [19]; 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 (S-GW) 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 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. Finally, the evolved Packet Data Gateway (ePDG) is used for interworking with un-trusted non-3GPP IP access systems.

IV. VoIP SPIT Flooding Mitigation Methods

There are three general forms of VoIP SPIT flooding mitigation methods [20],[21]. In this section, we will attempt to state generic methods which could be utilized to mitigate the negative effects of the flooding attack and therefore, we do not claim in any manner that these are the methods to mitigate SPIT (e.g., based on SIP vulnerabilities).

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.
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.
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 [22].

In this paper, we implement packet inspection based on a pattern detection approach and show through simulations, that it will be effective in mediating the effects of the VoIP SPIT flooding attack; as we discussed in Sections I-A, the VoIP SPIT flooding attack will cause a severe degradation in QoS that ultimately denies VoIP on 4G networks. Thus, stopping the SPIT flooding stream will mitigate the negative QoS effects of the attack. It is important to note that this method is not SIP-based and hence it will not detect SPIT calls before the intended target or the callee answers. Indeed, this is not our intention in this work and it does not constitute our primarily contribution. This method, will, after the callee answers the SPIT call and within few seconds, detect the SPIT in the RTP stream and consequently drop the call which as a result, stops the flooding stream. Furthermore, and even though this method may not be user friendly, we validate in Section VI-D that it will preserve, under the attack, the VoIP service on 4G networks.

Pattern detection is widely deployed in various forms of intrusion detection systems (IDSs) [23], [24], [25]. Therefore, our aim will be to profile specific detection algorithms employed by those IDSs on various hardware in order to model/assess their cost in terms of detection/packet processing delay on 4G specific infrastructure nodes. Having simulated and achieved that, we will be in a position to propose our secure, efficient and cost-effective mediating distributed mobile architecture.

V. Secure Mobile Architectures

Although there exist various mobile network architectures for mitigation methods deployment, in this paper we present, compare and analyze two major design trends; the conventional de facto centralized architectural approach and our proposed distributed architectural approach. In a 4G 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 Fig. 1. This approach can be considered

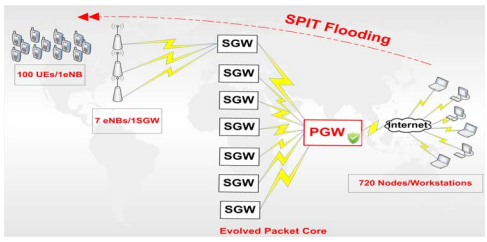

Fig. 1. Centralized Security Architecture

the de facto in current real world implementations since the 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 4G 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. Fig. 2 depicts this approach. The rationale behind this scheme states that if we re-allocate

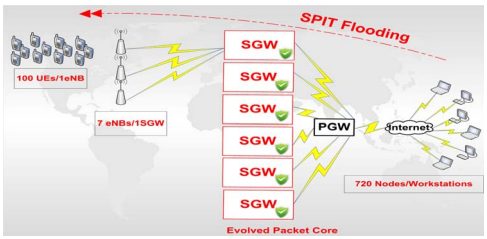

Fig. 2. Distributed Security Architecture

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 (by 4-8 times) 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 VoIP SPIT flooding attack while in addition preserve the efficiency on the 4G 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.

VI. Scenario: VoIP SPIT Flooding

A. Profiling for SPIT Flooding Mitigation

As we have stated in Section IV, our ultimate goal is to identify how much time an algorithm will require to inspect a packet when implemented on specific 4G nodes (S-GWs & P-GWs). Having achieved that, we will be in a position to simulate their effect when implemented on the mobile network for the purpose of SPIT flooding mediation. To accomplish that task, Snort [23] (specifically, its profiling engine) an open source network intrusion prevention and detection system, 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 IDSs such as Bro [24] and Suricata [25]. However, we have selected Snort since it is very well established and supported in addition to providing us with a very scientific and sophisticated profiling engine. 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 SPIT in VoIP data packets. The procedure was executed on two Linux machines

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 I
SPIT PROFILING RESULTS

operating an Ubuntu 9.10, Snort Version 2.8.5.3 (Build 124) with PCRE version 7.8. The first was a dual core machine which will model the S-GW in terms of processing power in our simulations. The second was a dual quad core (8 core) machine which will model the 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 the profiling statistics. Additionally, assuming

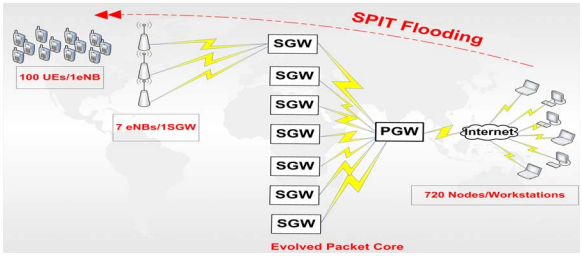

Fig. 3. 4G Simulated Topology

the fact that we are using the G.711 as the voice codec, 160 Bytes are used as the voice payload size [26]. As a result and acting upon the above assumptions, the results are summarized in Table I. According to our profiling results, the overhead of analyzing VoIP packets using both BM and NFA 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).

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 II
LINKS CONFIGURATION

B. Simulation Setup

For our simulations, we have utilized Opnet Modeler version 16.0 with the LTE specialized model [27] on a Windows 7 machine, running a quad core 2.5GHZ CPU with 4GB of memory. The simulated architecture (Fig. 3) consists of 720 Internet connected nodes [1], 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 [2] is given in Table II.

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

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

C. VoIP SPIT Flooding Impact

In this section, we aim at manipulating the traffic parameters of the scenario of Fig. 3 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 a VoIP SPIT flooding attack. Having accomplished that, we will be capable to compare both scenarios, specifically the three VoIP metrics, and thus analyze the impact of the attack on the QoS and availability of the VoIP application service on 4G mobile networks.

1) Normal Network Load: According to [3], 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 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 Fig. 3 and the simulation parameters of Section VI-B. Specifically, we configured the workstations to initiate the various traffic services and communicate with the UEs in a random manner.

2) Network Load Under VoIP SPIT Flooding Attack: To model the network under the VoIP SPIT flooding attack, we presume that the workstations have been exploited by malicious bots/malware and aim to flood the mobile network, more specifically, the UEs with VoIP SPIT. Under the same parameters defined in Section VI-B, we setup and ran the simulation for 30 minutes. Figures 4, 5 and 6 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. This is demonstrated when the average end-to-end delay for voice packets ranges from 69 ms to 75 ms (Fig. 4), the average one-way jitter is below 30 ms (Fig. 5) and the VoIP packet loss rate is almost negligible (Fig. 6). On the other hand and under the VoIP SPIT flooding attack, the results disclose the severe impact of the attack on the QoS and availability of the VoIP service on the 4G network. This is revealed in Fig. 4 when the average end-to-end delay for voice packets surpasses the 400 ms threshold just after 5 minutes of attack simulation time. Moreover, the average one-way jitter peaks at 460 ms (Fig. 5) and the VoIP packet loss rate is around 33% (Fig. 6). These indicators strongly imply the DoS effects of the VoIP SPIT flooding attack on 4G mobile networks.

Therefore, in order for mobile network operators to mediate all the effects of the attack and preserve the VoIP service on 4G networks, a mitigating security architecture must be

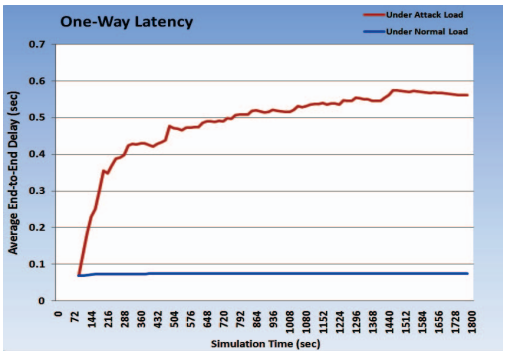

Fig. 4. Avg. End-to-End Delay for Voice Packets Normal Load Vs Attack Load

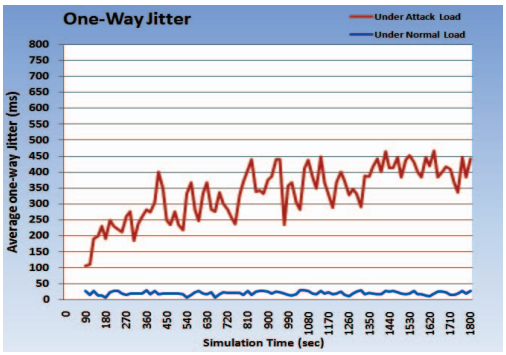

Fig. 5. Avg. One-Way Jitter - Normal Load Vs Attack Load

implemented and validated.

D. Simulation Results of SPIT Flooding Security Architectures

1) Centralized Architecture: In this scheme that is based on the conventional de facto centralized network security architecture, we propose to add both mitigating algorithms (BM & NFA RegEX) in the Packet Data Network Gateway as discussed in Section V and depicted in Fig. 1. We achieve this by adding the detection/packet filtering delay that we acquired from the profiling results of Section VI-A to the P-GW as packet processing delay.

2) Distributed Architecture: This scheme proposes a distributed architecture as discussed in Section V and depicted in Fig. 2. Hence, we distributed the mitigating algorithms on the S-GWs, utilizing the profiling results of Section VI-A. Note that our profiling results take into consideration the processing power of S-GWs & the P-GW and thus represent a realistic approach to their filtering power. To demonstrate relative service improvements, we setup, implemented and simulated both security architectures under the VoIP SPIT flooding attack for 20 minutes. It is creditable to note, that since we are implementing the same algorithms in both mitigating architectures and for the purpose of comparing them, 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

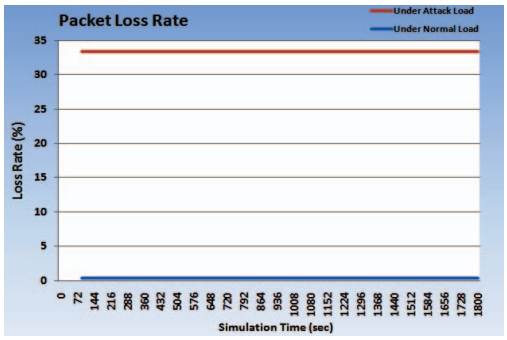

Fig. 6. VoIP Packet Loss Rate - Normal Load Vs Attack Load

are generating huge number of VoIP SPIT sessions, the P-GW will struggle to process and filter all the sessions. This fact is depicted in Fig. 7 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 demonstrated when the one-way latency metric exceeds the 400 ms threshold (Fig. 8), the average one-way jitter metric ranges from 80 ms to 140 ms (Fig. 9) and the VoIP packet loss rate metric is around 19% (Fig. 10). On the

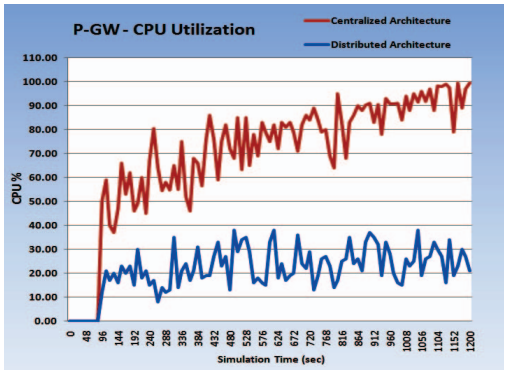

Fig. 7. P-GW: CPU Utilization in Both Security Architectures

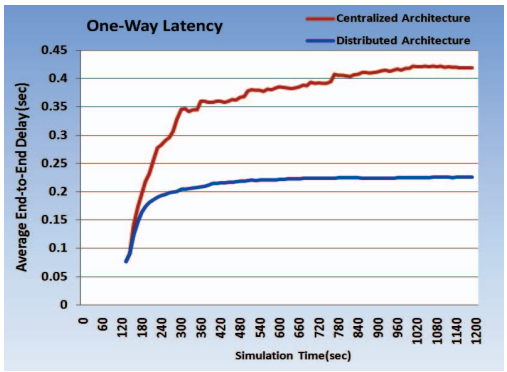

Fig. 8. Avg. End-to-End Delay for Voice Packets In Both Security Architectures

other hand, and comparing with the centralized architecture, our proposed distributed architectural approach, under the attack, is secure yet efficient. According to the simulation

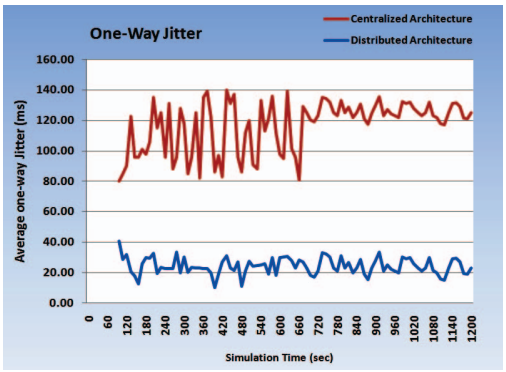

Fig. 9. Avg. One-Way Jitter In Both Security Architectures

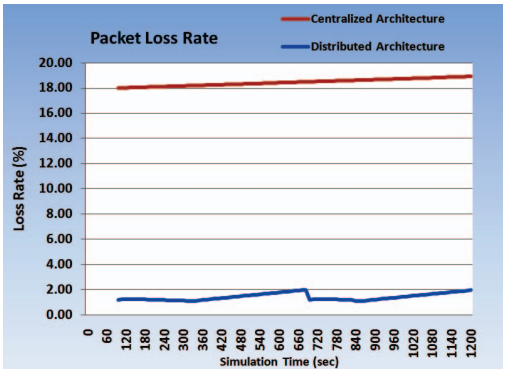

Fig. 10. VoIP Packet Loss Rate In Both Security Architectures

results, this architecture solves the over dimensioning problem in the P-GW as depicted in Fig. 7 and preserves the VoIP service on the 4G network. The latter statement is confirmed and backed up by Figures 8, 9 and 10 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 approximately, by 50%, 66% and 16% comparing with the conventional centralized architecture.

VII. Conclusion

In this paper, we presented a first look on the DoS effects of VoIP SPIT flooding on 4G mobile networks. Moreover, in an effort to mitigate the effects of the attack, we investigated generic detection algorithms employed by various IDSs. By utilizing Snort's profiling engine, we predicted and modeled the cost of the detection/filtering delay of the Boyer-Moore and NFA Regular Expression detection algorithms on 4G's S-GWs and P-GWs. Additionally, we simulated, compared and analyzed the de facto centralized mobile security architecture and our proposed distributed security architecture. We concluded that our proposed architecture is secure by mitigating the effects of the VoIP SPIT flooding attack, efficient by solving the over dimensioning problem caused by the centralized architectural approach and cost-effective by utilizing 'off the shelf' low-cost hardware in the S-GW nodes.

References

[1] J. Rosenberg et.al. SIP: Session Initiation Protocol, 2002.

[2] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. Rtp: A transport protocol for real-time applications, 2003.

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

[4] 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.

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

[6] 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.

[7] Online Cyber Safety. Available at: http://www.bsacybersafety.com/threat/bots.cfm.

[8] 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.

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

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

[11] 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.

[12] 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.

[13] 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*. USENIX Association, 2007.

[14] 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.

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

[16] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia. Fast Detection of Denial-of-Service Attacks on IP Telephony. In *IWQoS 2006,*, pages 199 –208, june 2006.

[17] 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*, volume 02, pages 1059 –1064, feb. 2009.

[18] Ian F. Akyildiz, David M. Gutierrez-Estevez, and Elias Chavarria Reyes. The evolution to 4g cellular systems: Lte-advanced. *Physical Communication*, 3(4):217 – 244, 2010.

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

[20] Vincent M. Quinten, Remco van de Meent, and Aiko Pras. Analysis of techniques for protection against spam over internet telephony. In *IFIP TC6.6*, EUNICE'07, pages 70–77, Berlin, Heidelberg, 2007. Springer-Verlag.

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

[22] 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.

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

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

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

[26] Voice Over IP Per Call Bandwidth Consumption CISCO Systems. Available at:http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml.

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