SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2013; **6**:1478–1489
Published online 6 February 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.413

SPECIAL ISSUE PAPER

A secure, efficient, and cost-effective distributed architecture for spam mitigation on LTE 4G mobile networks

Elias Bou-Harb[1]*, Makan Pourzandi[2], Mourad Debbabi[1] and Chadi Assi[1]

[1] CIISE, Concordia University, Montreal, Quebec, Canada
[2] Ericsson Research, Montreal, Quebec, Canada

ABSTRACT

The 4G of mobile networks will be a technology-opportunistic and user-centric system, combining the economical and technological advantages of various transmission technologies. As a part of its new architecture, LTE networks will implement an evolved packet core. Although this will provide various critical advantages, it will, on the other hand, expose telecom networks to serious IP-based attacks. One often adopted solution to mitigate such attacks is based on a centralized security architecture. However, this approach requires large processing and memory resources to handle huge amounts of traffic, which, in turn, causes a significant over dimensioning problem in the centralized nodes. Hence, it may cause this approach to fail from achieving its security task. In this paper, we focus on a SPAM flooding attack, namely SMTP SPAM, and demonstrate, through simulations and discussion, its DoS impact on the Long Term Evolution (LTE) network and subsequent effects on the mobile network operator. Our main contribution involves proposing a distributed architecture on the LTE network that is secure and that mitigates attacks efficiently by solving the over dimensioning problem. It is also cost-effective by utilizing 'off-the-shelf' low-cost hardware in the distributed nodes. Through additional simulation and analysis, we demonstrate the feasibility and effectiveness of our approach. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS

LTE Networks; security architectures; SPAM mitigation

***Correspondence**

Elias Bou-Harb, CIISE, Concordia University, 1515 Ste-Catherine Street West, EV7.640, Montreal, Quebec, Canada.
E-mail: e_bouh@encs.concordia.ca

1. INTRODUCTION

Although 3G technologies deliver significantly higher bit rates than 2G technologies, there is still an ever increasing demand for wireless broadband, lower latency, and increased throughput. Figure 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 growing pool of underserved consumers who can only be satisfied with next generation networks. The solution is the 3GPP Long Term Evolution (LTE) project [2], dubbed as the next generation network beyond 3G. The fourth generation of mobile networks will be a technology-opportunistic and user-centric system that combines the economical and technological advantages of various transmission technologies to provide a ubiquitous, context-aware adaptive service.

As a part of its new architecture, 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 the LTE, in addition to providing various critical advantages including multimegabit 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; because, theoretically, any security attack that is feasible on an IP network will also be viable on the LTE network.

A highly relied on application service is the Simple Message Transfer Protocol (SMTP) [3]. 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

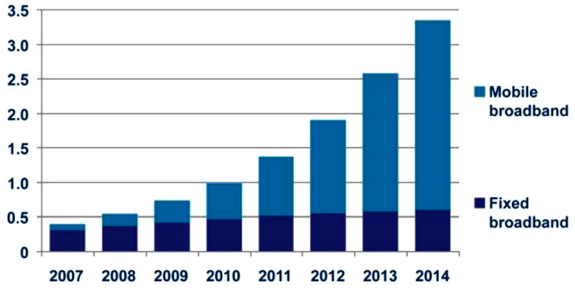


Figure 1. Broadband growth 2007–2014 [1].

exploited malicious clients' user equipments (UEs), 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 (i) cause a DoS to the SMTP server by overloading it with unsolicited emails and, hence, preventing it from processing legitimate email requests in a timely manner; and (ii) more critically, it 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 [4], for misusing the mobile infrastructure for Spamming purposes.

1.1. Defining DoS for SMTP SPAM

In this paper, we focus on a SPAM flooding attack in order to reveal its DoS impact on the LTE network and subsequent effects on the mobile network operator. Our intention is to shed light on the fact that LTE networks are vulnerable to IP-based attacks, which forces mobile network operators to preventively react and become liable in order to preserve their business and reputation. Hence, a security architectural solution is required and, for those, reasons may be proposed on the LTE network infrastructure. Moreover, for clarification purposes, we explain in the following when exactly a DoS will occur in the attack scenario.

1.1.1. SMTP SPAM DoS.

Generally, overloading SMTP servers do 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. 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. Thus, 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. This threshold is based on our Opnet benchmark results that we had performed on three different SMTP servers. The least performing server was a single core Windows 2000 server; the others were four and eight core machines running with the UBUNTU server 9.04.

1.2. Problem statement

Motivated by the fact that SMTP SPAM flooding is an alarming attack 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 impact of such attacks, their effects on the network and on the operator, and preventive architectures on LTE networks. Particularly, there is a need to answer questions, which include the following: Can 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 its subsequent effects? Furthermore, what are the adopted approaches in mitigating the effect of these attacks? Additionally, how can we propose a security architecture that mediates the effect of such attacks yet is efficient and cost-effective?

In this paper, we answer those questions by revealing that SMTP SPAM flooding attacks will indeed trigger a DoS, benefiting from LTE's evolved packet core. We disclose, through performing large scale simulations, that SMTP SPAM flooding through the exploited UEs targeting the mobile network operator's SMTP server, will cause a momentous performance bottleneck on the server and 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 the 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 profiling on various hardware, we estimate the cost of those algorithms in terms of processing/detection delay. Having achieved that, we discuss and compare two mediating approaches based on two different mobile security architectures on the LTE infrastructure. Through measurement, simulation, and analysis, we compare the conventional centralized architecture with our proposed distributed architecture. As a result, we demonstrate that the distributed approach is secure because it mitigates the effect of those attacks, more efficient because it solves the over dimensioning problem caused by the centralized approach, and cost-effective because it utilizes 'off-the-shelf' low-cost hardware in the distributed nodes.

The rest of the paper is organized as follows. Section 2 gives an overview of the related work; whereas, Section 3 demonstrates and explains the LTE architectural infrastructure. SPAM detection methods and mitigating mobile architectures are discussed in Sections 4 and 5. Furthermore, Section 6 reveals the algorithms' profiling discussion and results, which portrays our topological simulation scenario and illustrates the attack and counter-measure simulation results. Finally, Section 7 summarizes our contributions and concludes this work.

2. RELATED WORK

DoS attacks and mitigation methods have been discussed thoroughly in many contexts. A plethora of papers have focused on DNS systems including [5,6]; whereas, other research has focused on Web services [7]. Furthermore, SMTP services were pinpointed in [8,9]. Additionally, DoS attacks targeted search engines [10], VoIP servers [11,12], and, not surprisingly, e-commerce services [13].

The notion of exploiting a system and utilizing it to launch a DoS attack was tackled in [14], 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 it 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 [15], Defrawy *et al*. stated that BitTorrent's enormous traffic can be converted into a firepower used 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*. [16] introduced a signaling attack that seeks to overload the control plane of 3G mobile networks by 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*. [17] characterized a DoS attack that used 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 consisted of, as few as, 11 750 phones can cause a reduction of throughput of more than 90% to area code-sized regions supported by most of the currently deployed systems. Moreover, Enck *et al*. [18] 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 with the use of a regular cable modem. Another interesting study was conducted by Zhao *et al*. [19], where they presented a DoS attack against IMS. They stated that when the presence service, which is a core service of IMS, is congested, a malicious attack can cause chained automatic reaction of the system, thus, blocking all the services of IMS.

Although some basic form of malware targeting mobile devices has surfaced in the past, including Cabir [20], Mabir [21], and Skulls [22], advanced malicious applications exploiting today's full-featured powerful UEs are yet to be reported. However, with the adoption of LTE, vulnerabilities in mobile operating systems, unsafe applications and software, and the evolution of various types of botnets, their consequences and impacts must be investigated.

3. LTE ARCHITECTURE

In this section, we present the LTE network architecture and describe its elements and corresponding functionalities. Figure 2 illustrates a simplified view of the overall LTE architecture which is marked by the elimination of the circuit-switched domain and a simplified access network [23].

The LTE system is comprised of two networks: the E-UTRAN and the Evolved Packet Core (EPC) [25]. The result is a system characterized by its simplicity, a nonhierarchical 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. eNBs interface with user equipments 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 LTE is called the EPC and is depicted in Figure 3.

It is a flat all-IP system 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 and controls establishment of evolved packet system (EPS) bearers in the selected gateways. The Serving Gateway (S-GW) acts as the mobility anchor for the user plane during inter-eNB handovers. It also manages and stores UE contexts such as parameters of the IP bearer service and the network internal routing information, in addition to routing data packets between the Packet Data Network Gateway (P-GW) and the E-UTRAN. The P-GW provides connectivity to external packet data networks by being the point of exit and entry of traffic. Also, it 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

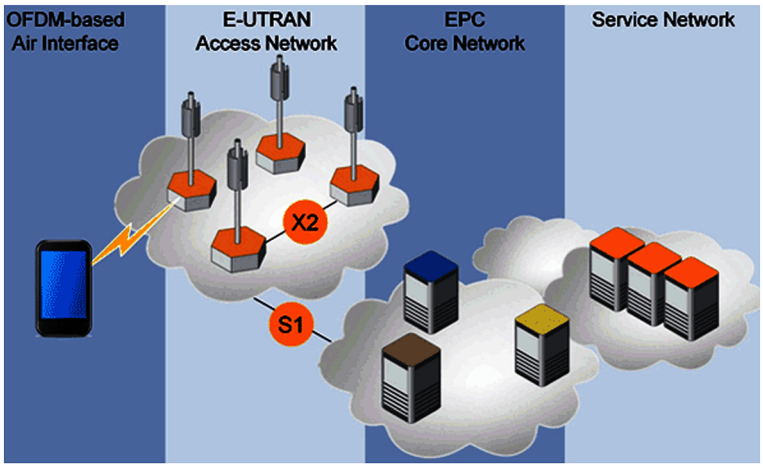


Figure 2. LTE architecture [24].

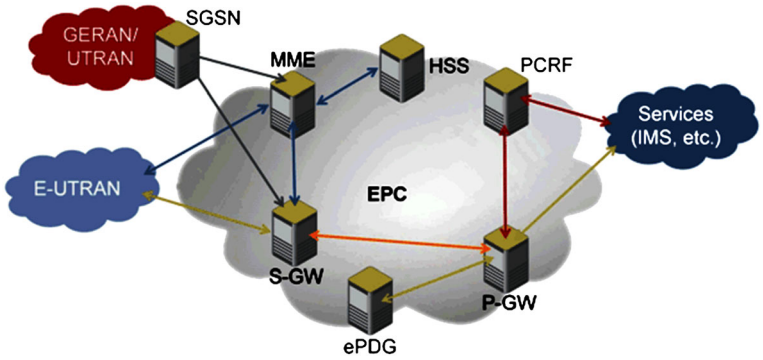


Figure 3. LTE EPC [24].

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 for passing these rules to the P-GW for enforcement. Finally, the evolved Packet Data Gateway (ePDG) is used for interworking with untrusted non-3GPP IP access systems.

4. SPAM DETECTION METHODS

There are three main forms of SPAM DoS detection methods discussed throughout the literature:

(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 that indicate a common attack. Pattern detection can be subdivided 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 $P = P[0]P[1]\cdots P[m\text{-}1]$ of length m in a large text $T = T[0]T[1]\cdots T[n\text{-}1]$ 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.

(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 that 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 in real networks, as traffic flows can be highly variable but 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 more than usual number of emails coming from a limited number of clients.

(3) Third party detection: These are systems that 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 [26].

In this paper, we implement a pattern detection approach, and we assert that it will be effective in mediating the effect of the SMTP SPAM flooding attack. This type of detection is widely deployed in various forms of IDSs. Therefore, our aim will be to profile specific detection algorithms employed by those IDSs on various hardware in order to assess their cost in terms of detection/packet processing delay. Consequently, we intend to simulate their effect when implemented on different nodes on the LTE network. Having achieved that, we will be in a position to propose our secure, efficient, and cost-effective mediating distributed mobile architecture.

5. MITIGATING MOBILE ARCHITECTURES

Although there exists various mobile network architectures for filtering prevention methods deployment, in this paper, we present, compare, and analyze two major design trends: the conventional centralized architectural approach, and the 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 prevention mechanisms on LTE 4G mobile networks. In this work, we aspire to show that the proposed distributed approach is:

(1) secure through mitigating the effect of the SMTP SPAM flooding attack;
(2) efficient through solving the over dimensioning problem caused by the conventional centralized architectural approach;
(3) cost-effective compared with the centralized approach through utilizing less commercial performant, less expensive off-the-shelf hardware in the distributed nodes rather than utilizing immensely specialized performant, expensive hardware in the centralized node.

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

This approach can be considered the *de facto* method in the current real world implementations. This is because 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, detection 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

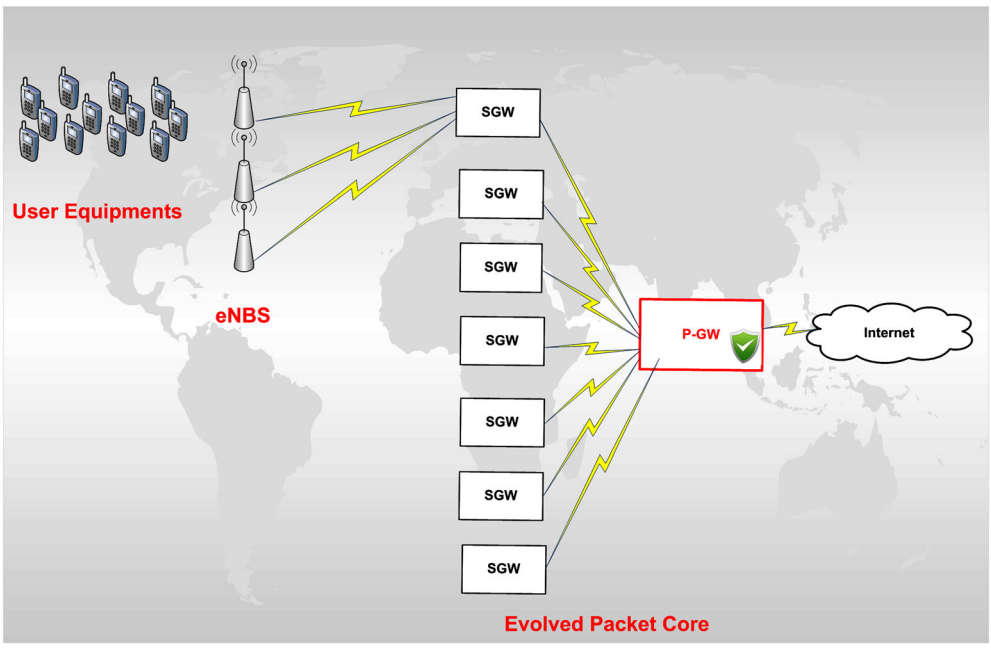


Figure 4. Centralized security architecture.

Security Comm. Networks 2013; **6**:1478–1489 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

candidate. The S-GW, similar to the P-GW, covers all ingress and egress traffic from and to the Internet. However, the S-GW traffic is, in some order of magnitude, less than the P-GW traffic; 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. Figure 5 depicts this approach.

The rationale behind this scheme states that if we re-allocate the filtering 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, we will still be able to achieve the security task of mediating the effect of the SMTP SPAM flooding attack, at the same time preserve the efficiency on the LTE network by solving the over dimensioning problem in the P-GW caused by the centralized approach. Moreover, because 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.

6. SCENARIO: SMTP SPAM FLOODING

6.1. Profiling for SPAM detection

As we have stated in Section 4, we intend to measure specific pattern detection 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. Having achieved that, we will be in a position to simulate their effect when implemented on the LTE network for the purpose of SPAM detection.

To accomplish that task, Snort [27], which is an open source network intrusion prevention and detection system that combines 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 nondeterministic finite automata regular expression (NFA RegEx) detection algorithm. In fact, these generic algorithms are widely adopted in various forms of IDSs such as Bro [28] and Suricata [29]. However, we have selected Snort because it is very well established and well supported in addition to providing us with a very scientific and sophisticated profiling engine.

The 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 [30]. Note that the length of the shift is the maximum shift between the occurrence heuristic and the match heuristic. Additionally, these heuristics are preprocessed in $O(m+|\Sigma|)$ time and space, where m is the pattern length and Σ is the alphabet. Furthermore, the searching phase of the BM algorithm requires $O(n \times m)$, time in the worse case, where n is the text length. Finally, the expected performance of the BM algorithm is sublinear, requiring about $\frac{n}{m}$ character comparisons on average [31].

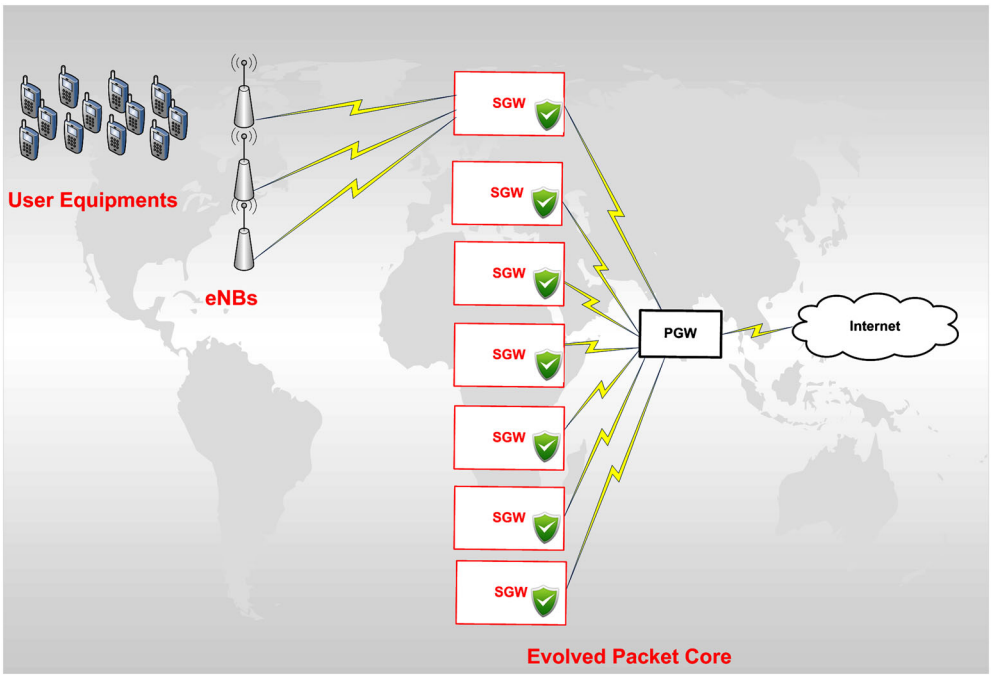


Figure 5. Distributed security architecture.

On the other hand, the NFA RegEx algorithm is excessively utilized because it is known to be space efficient. A nondeterministic 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 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.

A graphical representation of an NFA is called a transition graph. 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 spells 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 $O(|Nd \times |x|)$, where $|N|$ is the number of states in automata and $|x|$ is the input string length. Additionally, N has, at most, twice as many states as $|r|$; thus, the space complexity is $O(|r|)$, where $|r|$ is the size of the regular expression.

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) (Canonical Group Limited, Millbank Tower, Millbank, London, United Kingdom) with PCRE version 7.8. The first machine was a dual core with 4 GB of memory. This machine models the S-GW in terms of processing power in our simulations. The second was a dual quad core (8 core) machine with 160 GB of memory, 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 profiling statistics similar to Figure 6.

To acquire 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 these rules independently by using 10 data samples ranging from 2 KB to 1024 KB; for each sample, we ran the profiling procedure 10 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 BM and 43% utilize NFA RegEx. Moreover, for practical reasons, we assumed that only 20% of the rules will actually be employed to inspect the traffic. Acting upon the above assumptions, the results are summarized in Table I. According to our profiling results, the overhead of inspecting SMTP packets that used both algorithms would be 99.3 ms on the dual core machine (the S-GW) and 15.08 ms on the dual quad core machine (the P-GW).

The previous outcome will be employed to simulate and analyze the effect of the detection algorithms when implemented on the LTE network. This will be the foundation of our proposed mediating security architectures and, ultimately, our proposed distributed approach.

6.2. Simulation setup

For our simulations, we have utilized Opnet Modeler version 16.0 (OPNET Technologies Inc,. Woodmont Avenue Bethesda)with the LTE-specialized model [32] on a WINDOWS 7 machine running a quad core 2.5GHZ CPU with 4 GB of memory. The simulated architecture, illustrated in Figure 7, consists of the mobile network operator's SMTP Server, 1 P-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 in depicting a realistic LTE network deployment in a large city. Additionally, the links configuration [†]is given in Table II.

6.3. Scenario rationale

With the increase in the flourishing of multivendor 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 AppBrain [33], 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 [34]. Moreover, in 2009, a major mobile botnet was identified by the name 'Ikee.B', [35] which targeted UEs running on Apple's mobile operating system. Hence, specifically in this scenario, we demonstrate the feasibility of maliciously exploiting UEs from within the LTE network, flooding the operator'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, it, 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, reliability, and reputation, as well as making the operator liable to facing serious legal issues

[†] Our intention in selecting this broad bandwidth links configuration is to eliminate any possible delay that can be caused by the links

```
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 6. Rule profiling snapshot.

Table I. SMTP SPAM profiling results.

Algorithm/	Boyer–Moore/ NFA RegEx/		Total time/
Machine Type	SMTP Packet (ms)	SMTP Packet (ms)	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 II. Links configuration.

Link	Type	Bandwidth
UE-eNodeB	Wireless	10 Mbps
eNodeB-EPC	Ethernet-1000BX	1 Gbps
EPC-Internet	PPP-Sonet-OC48	2.37 Gbps

(e.g., under the Canadian House Government Bill C-28 Act) for misusing the mobile infrastructure for spamming purposes.

6.4. SMTP SPAM flooding impact

In this section, we aim to manipulate the traffic parameters of the scenario in Figure 7 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 1.1.1. Furthermore, we will be able to show the subsequent impacts of the attack on the mobile network operator.

6.4.1. Normal network traffic.

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 [36]. Therefore, modeling these distributions on the LTE network will provide us with a baseline that highly replicates a normal network functionality scenario. We simulated this scheme for 20 min in accordance with the proposed scenario of Figure 7 and the simulation parameters of Section 6.2. Specifically, we configured the UEs to initiate the various traffic services and communicate with the operator's SMTP server and their corresponding Internet servers.

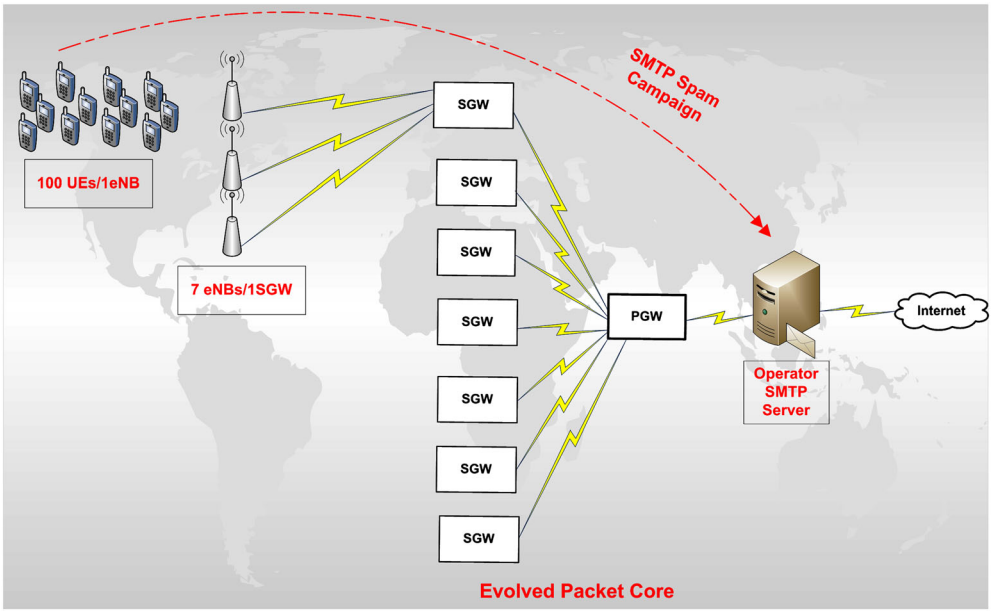


Figure 7. LTE SMTP SPAM topology.

6.4.2. SMTP SPAM flooding attack.

To model the SMTP SPAM flooding attack against the mobile network operator's SMTP server, we presume that the UEs have been exploited and aim to flood the server with SPAM email. In accordance with the topology of Figure 7, we setup and executed this attack scenario for 20 min.

Figures 8 and 9, 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 when 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 15^{th} 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 s to complete causing a drastic bottleneck. Relating this to our DoS definition and discussion from Section 1.1.1, we assert that this attack successfully caused a DoS targeting the operator's SMTP Server.

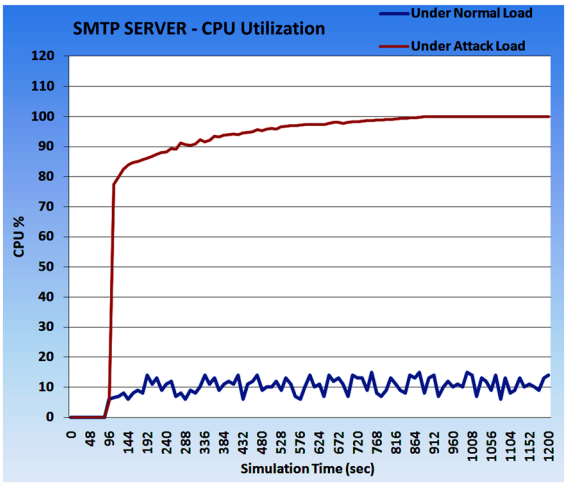


Figure 8. SMTP server: CPU utilization in both scenarios.

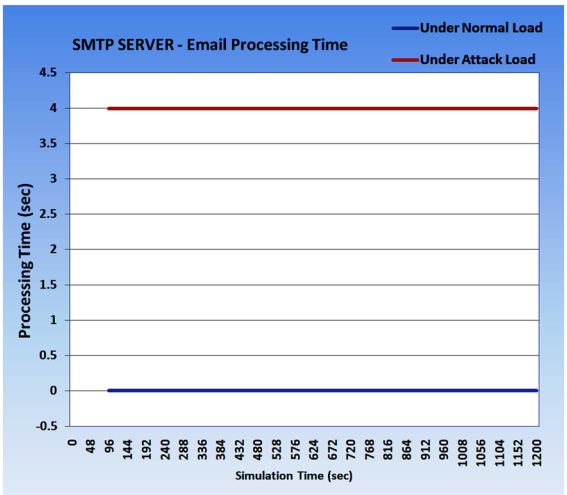


Figure 9. SMTP server: email processing time/email in both scenarios.

It is extremely noteworthy to mention that this SPAM flooding will force 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 because its infrastructure was misused. Therefore, to mediate all those effects, a security architecture must be implemented.

6.5. Simulation results: SMTP SPAM flooding security architectures

6.5.1. Centralized architecture.

In this scheme, which is based on the conventional centralized network security architecture, we propose to add both detection algorithms (BM and NFA RegEX) in the P-GW, as discussed in Section 5 and depicted in Figure 4. We achieve this by adding the detection/packet filtering delay that we acquired from the profiling results of Section 6.1 to the P-GW as a 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.

6.5.2. Distributed architecture.

This scheme proposes a distributed architecture, as discussed in Section 5 and depicted in Figure 5. Hence, we distributed our detection algorithms to the S-GWs, utilizing the profiling results from Section 6.1 and implementing them as a 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. Moreover, for future work, we plan to work on collaborative schemes between LTE nodes for the purpose of SPAM 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.

We setup, implemented, and simulated both security architectures under the SMTP SPAM flooding attack for 20 min following the same simulation parameters of Section 6.2. It's is worthy to note that, because 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.

The centralized architecture may be secure; however under the attack, it will cause an over dimensioning problem in the P-GW. Because the exploited UEs are

generating a huge number of SMTP SPAM sessions, the P-GW will struggle to process and filter all the sessions. This fact is depicted in Figure 10 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 it will affect the functionality of the LTE network.

On the other hand, under the SMTP SPAM flooding attack, the results of our proposed distributed architecture on the SMTP Server's performance are illustrated in Figures 11(a) and 11(b). 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 11(a)) still permitting the server to process emails in a timely manner, as depicted in Figure 11(b). In addition, this distributed architecture solved the over dimensioning problem caused by the centralized architecture, as demonstrated in Figure 10. 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.

As a result, we affirm that this proposed scheme, which is based on a distributed mobile network security architecture, will not only achieve the security task of mediating the direct and indirect effects of the attack but will also preserve and provide efficiency to the LTE network, in addition to being cost-effective for the reason mentioned in Section 5.

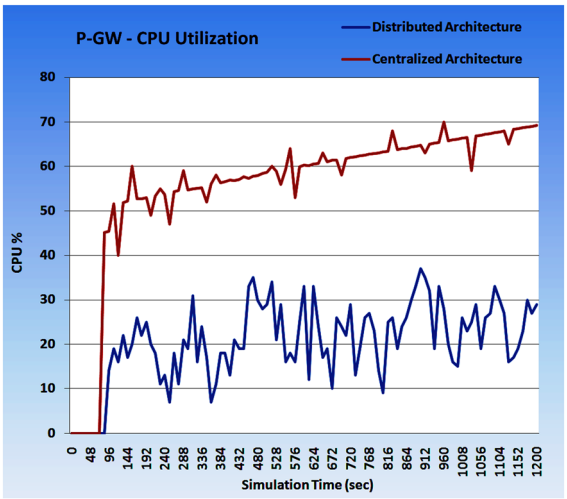
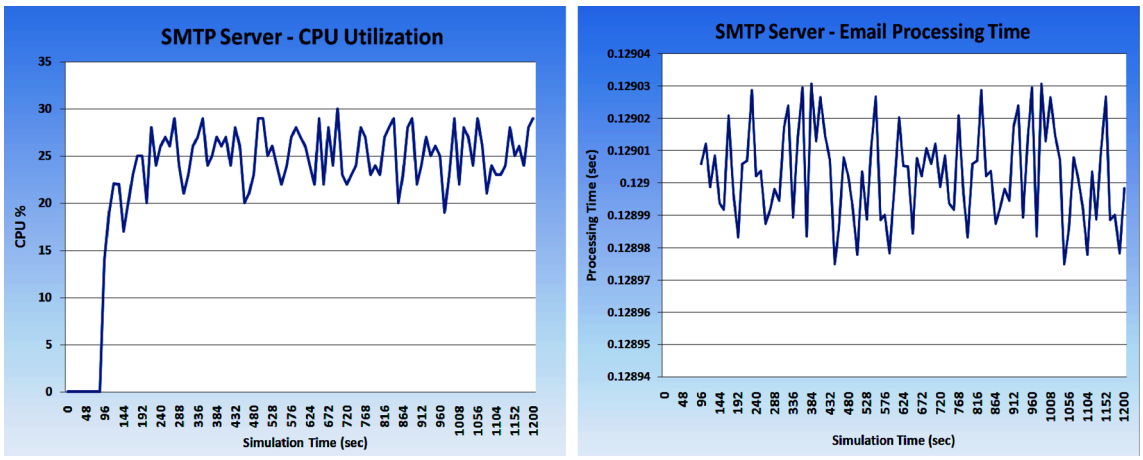


Figure 10. P-GW: CPU utilization in both architectures.

7. CONCLUSION AND FUTURE WORK

In this paper, we focused on a SPAM flooding attack, namely SMTP SPAM, and revealed through performing large scale simulations its DoS impact on the LTE network and subsequent effects on the mobile operator. We confirmed that IP-based attacks that take advantage of LTE's EPC and originate from within the mobile network, are feasible. Moreover, in an effort to mediate the effect 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 BM and NFA RegEx detection algorithms on S-GWs and P-GWs. Consequently, we discussed various detection methods and secure mobile architectures. Additionally, we simulated, compared, and analyzed the conventional centralized mobile security architecture and our proposed distributed security



(a) SMTP Server CPU Utilization Under Attack Load **(b)** SMTP Server: Email Processing Time/Email Under Attack Load

Figure 11. SMTP Server—performance metrics under the distributed security architecture. (a) SMTP server CPU utilization under attack load, and (b) SMTP server: email processing time/email under attack load.

architecture. We concluded by demonstrating that our proposed architecture is secure, as it mitigates the direct and indirect effects of the SMTP SPAM flooding attack targeting the operator's email server, efficient as it solves the over dimensioning problem caused by the centralized architectural approach, and cost-effective as it utilizes off-the-shelf low-cost hardware in the S-GW nodes. For future work, we plan to work on collaborative preventive approaches against SPAM flooding in LTE networks.

REFERENCES

1. Dahlman P, Parkvall S, Beming D. In *3G Evolution: HSPA and LTE for Mobile Broadband* (Second edition edn). Academic Press: Oxford, UK, 2008.
2. 3GPP-LTE. Available at: http://www.3gpp.org/LTE
3. Protocol SMT. Available at: http://tools.ietf.org/html/rfc5321t
4. Act CHGBC. Available at: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Bill=C28Language=EMo de = 1Parl = 40Ses = 3
5. Wu J, Wang X, Lee X, Yan B. Detecting DDoS attack towards dns server using a neural network classifier. In *Artificial Neural Networks ICANN 2010*, *Lecture Notes in Computer Science*, Vol. **6354**, Diamantaras K, Duch W, Iliadis L (eds)(eds). Vol.Springer: Berlin/Heidelberg, 2010; 118–123URL http://dx.doi.org/10.1007/978/3-642-15825-415, 10.1007/978-3-642-15825-415
6. Sun C, Liu B, Shi L. Efficient and low-cost hardware defense against DNS amplification attacks. *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* 2008: 1–5. doi: 10.1109/GLOCOM.2008.ECP.397
7. Chonka A, Xiang Y, Zhou W, Bonti A. Cloud security defence to protect cloud computing against http-dos and xml-dos attacks. *Journal of Network and Computer Applications* 2010; In Press, Corrected Proof–doi:10.1016/j.jnca.2010.06.004URL http://www.sciencedirect.com/science/article/B6WKB-50CDSTV-1/2/85cd7430c1201abbffd690fadc54aa48
8. Still M, McCreath EC. DDoS protections for SMTP servers. *International Journal of Computer Science and Security (IJCSS)* 2011; abs/0912.1815: 537–550.
9. Kumar R, Jindal A, Pandove K. Article: launching email spoofing attacks. *International Journal of Computer Applications August* 2010; **5**(1):21–22Published By Foundation of Computer Science.
10. Times NY. Yahoo attributes a lengthy service failure to an attack. http://partners.nytimes.com/library/tech/00/02/biztech/articles/08yahoo .html
11. Rafique M, Ali Akbar M, Farooq M. Evaluating DoS attacks against sip-based voIP systems. *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009; 1–6, doi:10.1109/GLOCOM.2009.5426247
12. Zhang H, Gu Z, Liu C, Jie T. Detecting voIP-specific denial-of-service using change-point method. *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, vol. 02, 2009; 1059–1064.
13. ZDnet. Leading web sites under attack. http://news.cnet.com/2100-1017-236683.html
14. Naoumov N, Ross K. Exploiting p2p systems for DDoS attacks. *Proceedings of the 1st International Conference on Scalable Information Systems*, InfoScale '06, ACM: New York, NY, USA, 2006, doi:http://doi.acm.org/10.1145/1146847.1146894. URL http://doi.acm.org/10.1145/1146847.1146894
15. El Defrawy K, Gjoka M, Markopoulou A. BotTorrent: misusing bitTorrent to launch DDoS attacks. *Proceedings of the 3 rd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet*, USENIX Association: Berkeley, CA, USA, 2007; 1:1–1:6. URL http://portal.acm.org/citation.cfm?id=1361436.1361437
16. Lee P, Bu T, Woo T. On the detection of signaling DoS attacks on 3G wireless networks. *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007; 1289–1297, doi:10.1109/INFCOM.2007.153
17. Traynor P, Lin M, Ongtang M, *et al*. On cellular botnets: measuring the impact of malicious devices on a cellular network core. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, ACM: New York, NY, USA, 2009; 223–234, doi:http://doi.acm.org/10.1145/1653662.1653690. URL http://doi.acm.org/10.1145/1653662.1653690
18. Enck W, Traynor P, McDaniel P, La Porta T. Exploiting open functionality in SMS-capable cellular networks. *Proceedings of the 12th ACM Conference on Computer and Communications Security*, CCS '05, ACM: New York, NY, USA, 2005; 393–404, doi:http://doi.acm.org/10.1145/1102120.1102171. URL http://doi.acm.org/10.1145/1102120.1102171
19. Zhao B, Chi C, Gao W, Zhu S, Cao G. A chain reaction DoS attack on 3G networks: Analysis and defenses. *INFOCOM 2009, IEEE*, 2009; 2455–2463, doi:10.1109/INFCOM.2009.5062173
20. SecureList. Worm.symbos.cabir.a. Available at: http://www.securelist.com/en/descriptions/old60663
21. Symantec. Symbos.mabir. Available at: http://www.symantec.com/security*,esponse/writeup.jsp*?*docid* = 2005 – 040414 – 1543 – 99.
22. F-Secure. Trojan:symbos/skulls.a. Available at: http://www.f-secure.com/v-descs/skulls.shtml

23. Akyildiz IF, Gutierrez-Estevez DM, Reyes EC. The evolution to 4G cellular systems: LTE-advanced. *Physical Communication* 2010; **3**(4):217–244doi. doi:10.1016/j.phycom.2010.08.001URL http://www.sciencedirect.com/science/article/pii/S18744907100 00303
24. Cobler K. Mobile network evolution and the LTE architecture. Available at: http://www.wirelessweek.com/Articles/2010
25. Parikh J, Basu A. Article: LTE advanced: the 4G mobile broadband technology. *International Journal of Computer Applications* 2011; **13**(5):17–21Published by Foundation of Computer Science.
26. RStonei. Centertrack: an IP overlay network for tracking DoS floods. *In Proc of the 9th conf. on USENIX Security Symposium*, vol. 9, 2000; 15–15.
27. Snort. Available at: http://www.snort.org
28. Bro intrusion detection system. Availble at: http://www.bro-ids.org/
29. Next generation intrusion detection and prevention engine. Availble at: http://www.openinfosecfoundation.org/index.php/download-suricata/
30. Charras C, Lecroq T. In *Handbook of Exact String Matching Algorithms*. King's College Publications: London, UK, 2004.
31. Michailidis MKGPD. In *On-line string matching algorithms: survey and experimental results*. Taylor and Francis: USA, 2001. URL http://www.informaworld.com/10.1080/00207160108805036
32. Model OLS. Available at: http://www.opnet.com/LTE/.
33. AppBrain. Number of available android applications. Available at: http://www.appbrain.com/stats/number-of-android-apps
34. Post T. SMS Trojan found in several android apps. Available at: http://threatpost.com/en$_{u}$s/blogs/sms − trojan − found − several − android − apps − 051211 ? utm$_{s}$ource = Newsletter$_{0}$51311 & utm$_{m}$edium = Email + Marketing & utm$_{c}$am
35. Phillip Porras HS, Yegneswaran V. An analysis of the Ikee.B (duh) Iphone botnet. Available at: http://mtc.sri.com/iphone/
36. Mobile broadband traffic across regions 2009-2017-coda research consultancy ltd. laptops and netbooks 2009.