Future Internet **2013**, *5*, 474-489; doi:10.3390/fi5040474

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Practical Attacks on Mobile Cellular Networks and Possible Countermeasures

Murat Oğul and Selçuk Baktır *

Department of Computer Engineering, Bahçeşehir University, Çırağan Caddesi, No: 4, Beşiktaş 34353, İstanbul, Turkey; E-Mail: murat.ogul@stu.bahcesehir.edu.tr

* Author to whom correspondence should be addressed; E-Mail: selcuk.baktir@bahcesehir.edu.tr; Tel.: +90-212-381-5676; Fax: +90-212-381-0550.

Received: 29 July 2013; in revised form: 11 September 2013 / Accepted: 11 September 2013 / Published: 30 September 2013

Abstract: Due to widespread adoption of mobile communications devices and increasingly high throughput capacity of cellular networks, Third-Generation (3G) and Long Term Evolution (LTE) are becoming ever more popular. Millions of smart phones with 3G capabilities are sold every year and used for mostly browsing the Internet. Hence, mobile operators have been heavily investing in their packet switched networks to meet customer demand and stay ahead in the market. The widespread use of broadband mobile Internet bring along also some IP based threats such as the Denial of Service (DoS) attacks, botnets and malwares. In this paper, we performed DoS and flooding attacks on 3G mobile networks and measured their effect on the most critical elements of a network such as the Radio Network Controller (RNC) and the Serving GPRS Support Node (SGSN) devices. We carried out our experiments on a real mobile network, not just a simulation environment, and hence our findings depict a realistic picture of the vulnerabilities existent in 3G mobile networks. We propose alternative solutions to avoid these vulnerabilities and mitigate the issues raised.

Keywords: mobile networks; 3G; security; DoS; denial of service attack; paging

---

1. Introduction

Mobile communication is becoming commonplace and playing an irreplaceable role in our lives. It is facilitating not only voice communication but also high speed data communication. Millions of

smart phones with 3G capabilities are sold every year and mostly used for browsing the Internet, banking applications and messaging, resulting in the expectations for the data revenue of mobile cellular network operators to exceed their voice revenue [1]. Especially, with the availability of the high data throughput in 3G, Long Term Evolution (LTE) and LTE-Advanced [2] mobile networks, many subscribers communicate more data than voice. The trend is that data communication, compared to voice communication, is dominating the mobile market. It is expected that mobile revenue will double by 2016, but traffic will increase tenfold due to increasing demand for mobile data communication [3]. As a result, in mobile cellular networks, data communication revenue is forecasted to exceed voice communication revenue [4]. Therefore, mobile operators capitalize on their data services and, in addition to being mobile voice carriers, mobile core networks tend to be used as Internet Service Providers (ISP). The investments made by mobile carriers on their IP based infrastructures and services are motivated mostly by their subscribers' increasing demand for mobile data communication. The acceptance of mobile networks as a venue for Internet access brings along new IP based threats on mobile core networks [5].

Previous studies investigated several vulnerabilities in mobile 3G networks. Ricciato [6] discussed some attacks on 3G networks and showed how unwanted traffic results in resource wastage. He also discussed four different attack models specific for cellular networks and evaluated their results for a more robust network design perspective [7]. Serror *et al.* [8] investigated attacks on the paging channel and presented their findings through simulations. Bavosa [9] made valuable contributions to the field by discussing the vulnerabilities on cellular networks in detail and proposing countermeasures. Wu *et al.* [10] studied the randomization method to prevent DoS attacks on 3G cellular networks, again using simulations. Several DoS attacks on 3G networks were realized [11–13]. In this work, we particularly focus on measuring the effect of DoS and flooding attacks, which exploit paging [14] vulnerabilities, and realize our experiments in a real production mobile cellular network. Furthermore, we propose solutions to mitigate the existent vulnerabilities.

The rest of the paper is organized as follows. Section 2 discusses the basic architecture of a 3G network and Section 3 analyzes possible threats in 3G as well as LTE networks. In Section 4, we conducted some attacks exploiting paging vulnerabilities on 3G networks and observed their negative effects. Section 5 discusses some countermeasures against the security threats mentioned. Finally, Section 6 is the conclusion.

2. Mobile Cellular Network Basics

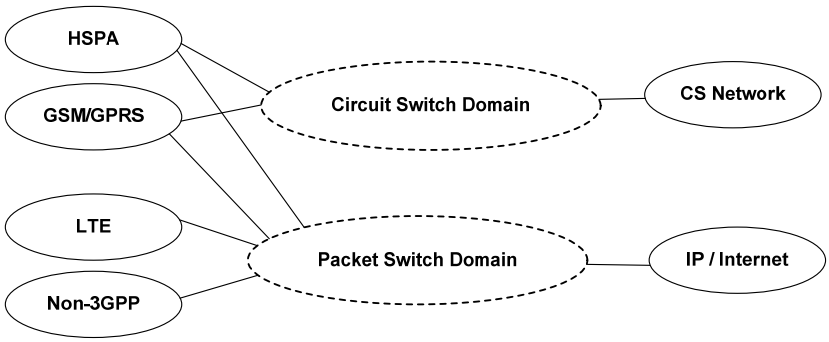
Mobile Cellular Networks are made up of two main components, namely circuit switched (CS) and packet switched (PS) networks [15]. The CS network is used mostly for voice traffic while the PS network is used for data traffic. In other words, a CS network could be called as a Radio Network and a PS network as a Packet Network, as shown in Figure 1 below.

GGSN (Gateway GPRS Support Node) assigns the IP and Domain Name System (DNS) addresses to User Equipment (UE) such as mobile phones, smartphones, GPRS devices, *etc.* When the UE connects to the network, the GGSN handles packet data protocol (PDP) contexts [16] and also performs packet forwarding between the Packet Network (PN) and the Internet. Serving GPRS Support Nodes (SGSN) are placed in the most critical location in cellular networks. They have direct

connection to almost all elements in a cellular network and have responsibilities in managing data channels, such as the PS domain originated paging channels and providing Call Data Register (CDR) information to billing systems. The Radio Network Controller (RNC) is mostly responsible for managing radio resources. User Equipment firstly communicates with NodeB via the air interface. The NodeB performs tasks similar to those performed by a base station in a 2G network. In addition, all the UEs use different timeslots and signaling channels for voice and data communication.

In Cellular Networks, different kind of protocols, such as the GPRS Tunneling Protocol (GTP) tunnels, the User Datagram Protocol (UDP) and the IP, are used between devices. Mostly, the IP protocol is used but other upper layer protocols are also used on different layers of the OSI model [17].

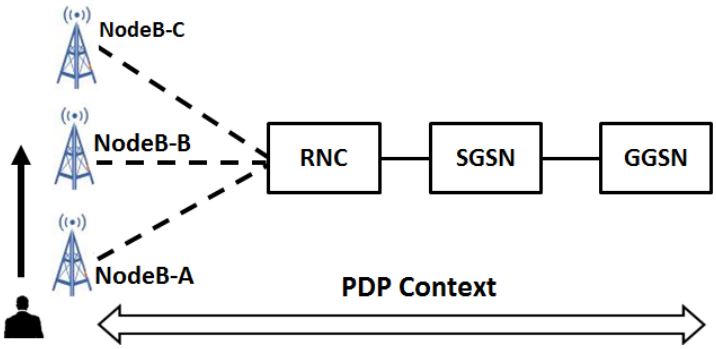
Figure 1. Mobile Cellular Network.



2.1. 3G Mobility Management for Data Communication

In mobile networks, the mobile end point may change its location and hence the systems serving this mobile end point may change. For instance, as seen in Figure 2, when a mobile user connects to a mobile PS network and moves from one point to another without closing the connection, the serving system for the end point, such as the Node B, can change from NodeB-A to NodeB-B. In Global System for Mobile (GSM) networks, knowing the end point location is one of the most critical issues for the network devices of an operator. Therefore, in order to give better service, the mobile operator must know the exact location of the mobile end point.

Figure 2. Serving NodeB changes.



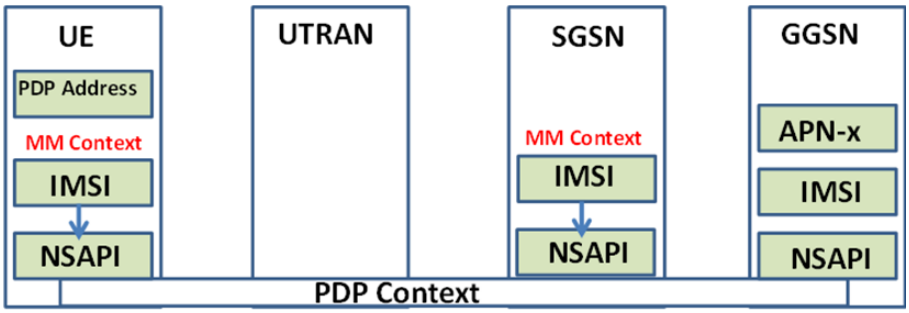
Packet Mobility Management (PMM) context is used to track a mobile end point's location and its serving systems such as the NodeB, the RNC and the SGSN. In the PS domain, the SGSN and the mobile end point perform this task by managing PMM contexts. However, GGSN is not directly

related to location tracking and does not need to know the mobile end point's PMM context. A PMM context may be different on a mobile end point and on a SGSN.

Mobility Management (MM) is necessary for tracking the physical location of the UE and serving devices such as NodeB. After the establishment of the connection between the UE and cellular network equipments, all PS user data (from or to the UE) is first sent to the GGSN. This means the UE connects to a mobile network and uses the NodeB, the RNC and the SGSN for different session establishments. However, end to end IP level communication takes place between the UE and GGSN. Later, the GGSN forwards the UE's data towards its destination according to per host specific routing on the GGSN.

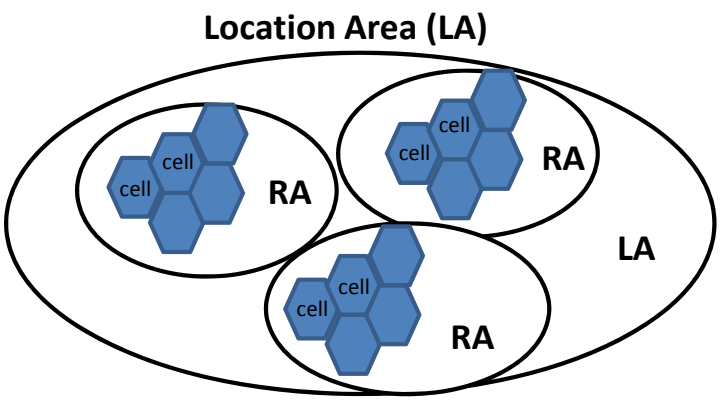
The connection between the UE and the GGSN is referred to as an active PDP context. Each PDP context has its own IP address that is assigned by a GGSN. As needed, each UE can have up to 16 activated PDP contexts and each of them is uniquely identified by a combination of the subscriber's International Mobile Subscriber Identity (IMSI) and a Network Service Access Point Identifier (NSAPI) [18]. In order to route the UE data correctly, a PDP context should exist from the UE to the GGSN, as shown in Figure 3. A PDP context is necessary only for data communication and not voice.

Figure 3. End to End packet data protocol (PDP) Context.



MM is referred to as PMM (Packet Mobility Management) on GPRS 3G networks. In order to track a UE's location easily, mobile networks use a hierarchy of areas, such as Location Area (LA) and Routing Area (RA). Cells form an RA and RAs form an LA, as shown in Figure 4.

Figure 4. Mobile network hierarchy.



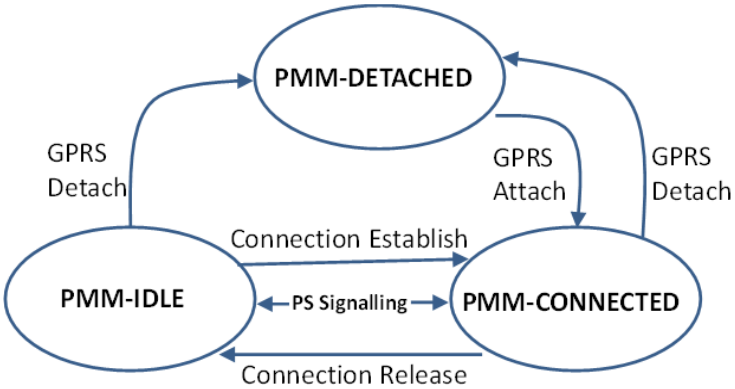
An LA is a set of base stations that are grouped together to optimize signaling. An RNC manages radio channel allocation and handover for all cells in the same LA. Many nodeBs in the Universal

Mobile Telecommunications System (UMTS) share a single RNC in UMTS. The size of an LA is an issue since an LA too big or too small could be a problem from the optimization point of view. The size of an LA may also affect paging on the RNC [19].

An RA is used in the PS domain by UEs that are attached to GPRS and have active PDP contexts. A change from an RA to another RA is done in same way as it is done during a change from one LA to another LA. The only difference is that an LA is controlled by an RNC whereas an RA is controlled by an SGSN.

In a PS network, a UE can be in one of the three different PMM states: PMM-Detached, PMM-Idle and PMM-Connected, as shown in Figure 5.

Figure 5. A User equipment (UE)'s packet mobility management (PMM) state transition.



PMM-Idle State: Once a UE is attached to a GPRS network, in addition to IP assignment, end-to-end resources are dedicated for the virtual channel between the UE and the GGSN, and also a timeout timer is started to track the UE activity. If the UE is idle for longer than a certain amount of time, the related systems such the GGSN and the SGSN will release their dedicated resources. After this release, although the UE is still known by an SGSN, a significant signaling overhead is required to reinitiate the data transfer. Connection re-establishment can be initiated by either the UE or the SGSN. The SGSN triggered connection re-establishment occurs only if an SGSN receives data destined for a certain UE, from a GGSN. In order to realize this, the SGSN uses the paging procedure. In that case, the UE's location is known by the SGSN with an accuracy of an RA but not a cell. It is important to note that if there is a PDP context active, the given UE's cell is already known, so a paging message is no longer required. So, the UE and the SGSN have valid PMM contexts. The UE and SGSN should enter the PMM-CONNECTED state when the PS signaling connection is established between the UE and the SGSN.

PMM-Detached state: This state means that the UE is switched off, outside the service area or not attached to a PS network, *i.e.*, the UE and SGSN contexts don't have any location and routing information for the UE, and hence the UE is not reachable by an SGSN. In this state, there is no active PDP context and assigned IP address to the UE. A GPRS attach procedure should be performed in order to transfer to the PMM-Connected state. If any traffic destined to the UE comes to the GGSN, it will be discarded and no paging procedure will be needed.

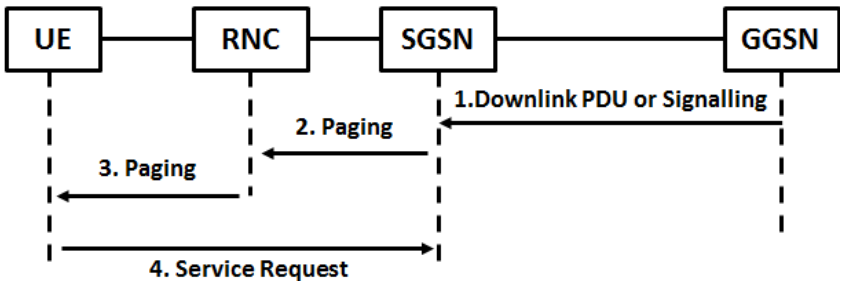
PMM-Connected State: In this state, the UE's location is known in the SGSN with an accuracy of a serving RNC. Also, the serving RNC tracks the UE with an accuracy of a serving cell. Therefore, if

any traffic destined to the UE comes to the GGSN, it will be forwarded to the UE through a PDP context and no paging procedure will be needed.

2.2. Paging

Paging can be triggered by a request from a PS or CS network. Paging triggered by a CS network is not in our concern. On a PS network triggered paging, the paging procedure is used only for a UE in the PMM-idle state. Packets that are destined to a UE may come to the GGSN from the Internet or 3G packet networks, such as from another 3G subscriber. If a PDP context exists, packets will be sent to the SGSN via a GTP tunnel. For these packets to reach to the UE, the SGSN should know about the target UE's cell information, *i.e.*, the cell that is serving the UE. Therefore, if the SGSN does not have the cell information of the destined UE, it will initiate a paging procedure by sending some packets to the RNC. As mentioned before, this means that paging is realized only if the UE is in the PMM-idle state when packets are sent to it. Figure 6 illustrates the signal flow activity for the PS triggered paging.

Figure 6. Packet switched (PS) triggered paging procedure.



The paging procedure from the GGSN to the UE, given in Figure 6, is described in detail below.

1. The GGSN sends a packet, destined for the UE in PPM-idle state, to the SGSN;
2. Upon getting packets from the GGSN, the SGSN sends a Paging Request message that includes the IMSI number, RA, *etc.*, to the RNC belonging to the RA where the UE is located;
3. The RNC passes the paging requests to the UE;
4. Upon getting the paging request message, the UE's state changes from PMM-idle to PMM-connected. Also, the UE sends paging request packets back to the SGSN.

After completing the paging procedure, the SGSN knows about the cell, RA and all the other location information of the destination UE. This means that any packet destined from the GGSN to the UE in PMM-idle state can be delivered to the UE.

While a paging procedure is taking place, mostly the RNC's and SGSN's loads rise. This can be exploited by some DoS or Distributed Denial of Service (DDoS) type of attacks, which is the major focus of this study.

3. Threats on Cellular Networks

Unlike wired networks, mobile cellular networks have a complex structure with many components and protocols resulting in vulnerabilities and threats [20]. However, it is possible to take the necessary precautions and thus mitigate the risks of these threats to an acceptable level. Mobile operators should

take the required actions to mitigate the security risks to their subscribers and also to their core networks. It is up to an operator to possibly charge for these security actions.

As discussed in the previous section, in mobile cellular networks, paging effects are important security issues. Paging attacks could be most damaging on the border of a mobile operator's network. One border of cellular networks is where Internet access starts and another one is where subscribers attach to a 3G network. Mobile operators can take most of the countermeasures on these border points.

Thanks to the release of the 3G and LTE technologies, mobile GSM operators have overtaken ISP roles. Some argue that, like traditional ISPs, mobile operators have no obligation to protect their customers, while others argue they should protect their subscribers, as well as their core network infrastructure, against security threats [21]. Although traditional wired network ISPs and mobile network operators both act as ISPs, their core network infrastructure or underlying networks are very different. The security requirement on the border of the Internet and on the subscriber border is higher for mobile operators than for traditional wired ISPs. This is due to the existence of more fragile components and protocols used in mobile networks. In our study, we've focused on these border points. In an actual production mobile network environment, we have investigated the effect of DoS kind of attacks from the Internet against 3G users. We discuss these attacks and possible countermeasures in the next section.

4. Measuring the Effect of the DoS Attack on 3G Networks

We think paging is a big threat in mobile cellular networks. So, we performed some attacks by exploiting vulnerabilities in GSM network components due to paging, and examined the effect of these attacks. A network or company is as strong as its weakest point in terms of security. Therefore, a network should be assessed as a whole when a security solution is put in place. All pieces of a network should be evaluated carefully in terms of security. We performed DoS and flooding attacks in a production mobile cellular network that supports 120,000 concurrent users and investigated their effect on core network equipment such as the RNC and SGSN. We suggest some countermeasures, taking our findings into consideration.

As discussed earlier, some mobile cellular operators think that no security solution is necessary on the Internet border of their network that serves their subscribers during Internet access. So, they typically construct their networks as shown in Figure 7. In this setting, any packet coming from the Internet, destined to a subscriber of the mobile operator, could reach its target.

A subscriber accesses core network devices for authentication and authorization, after passing through the air interface and the transport network of the mobile operator. An IP address is assigned to a subscriber by a GGSN if it is successfully authenticated and authorized. The first point on the mobile cellular network where a subscriber can do IP-based communication is the GGSN. The GGSN acts as a remote access server. A subscriber's data traffic is carried via tunnels until the GGSN. For example, the subscriber traffic from the GGSN to the SGSN is carried by GTP tunnels. Briefly, behind the GGSN, the subscriber data traffic is tunneled and carried to the subscriber as shown in Figure 8. Therefore, when any customer tries to learn the traffic path by using trace applications (e.g., tracert for Windows or traceroute for Linux and Unix), they notice that they can see just the GGSN's IP address, and the devices after the GGSN only if the operator allows. Direct access to core network equipment is

not allowed by nature of mobile cellular networks. Even then, we think that the traffic from a subscriber to the Internet, and from the Internet to a subscriber, could affect core network devices dramatically. It is a serious threat and a countermeasure needs to be taken. The most practical way to decrease the risks here to an acceptable level, without monetary investment, is to enable the IP filter feature of the used Internet router without a firewall feature. With this feature, a router examines the source and/or destination IP address fields, and possibly also the TCP/UDP port numbers, in a packet's IP header. By controlling the TCP/UDP port number in the IP header, it might achieve more detailed filtering. On the other hand, Access Control Lists (ACLs) consist of IP/TCP/UDP based filtering entries, and they are typically used to indicate the allowed/blocked IP addresses whose traffic is allowed/blocked. This simple countermeasure will protect the core network devices and also the UEs. However, the basic ACLs on the router supports only basic IP/TCP/UDP restriction and does not provide session state tracking or stateful inspection [22] for all the used protocols such as TCP and UDP. Without a stateful firewall feature set, a router can only support TCP SYN attack protection. However, all other attacks with TCP flags, such as ACK, RST/ACK, FIN, FIN/ACK, *etc.*, which are set to 1, can pass through a router's ACLs without being blocked. Therefore, a router recognizes any packet coming from the Internet with its SYN bit set to 1. If the packet is not given the access right on the ACL, it will be dropped. Thus, a router can block only the unwanted packets with their TCP SYN bit set to 1. And all other TCP or UDP packets will be allowed in order not to block the response to legal customer initiated traffic. In our study, we call this kind of an ACL as TCP ACL. Hence, by using this kind of a solution, we protect customers and mobile core network infrastructure against only TCP SYN based attacks. Although our routers provide only TCP SYN based attack protection, we notice that the number of paging on RNC decreases after the TCP based Access Control List (ACL) is applied. To ensure the positive effect, we temporarily disabled TCP based ACL on our Internet router and observed the paging activity and resource usage of our core network devices. After we applied TCP based ACL on our Internet routers again, the paging activity and CPU usage was influenced positively as shown with the graphs in Figures 9 and 10. In these graphs, the horizontal axis shows time and date, and the vertical axis shows the CPU usage. These graphs have a sampling period of 1875 s. As seen in these graphs, the CPU usage on the RNC and SGSN decrease by approximately 25%, compared to the values when the ACL is not applied.

Figure 7. Network designed without a security solution.

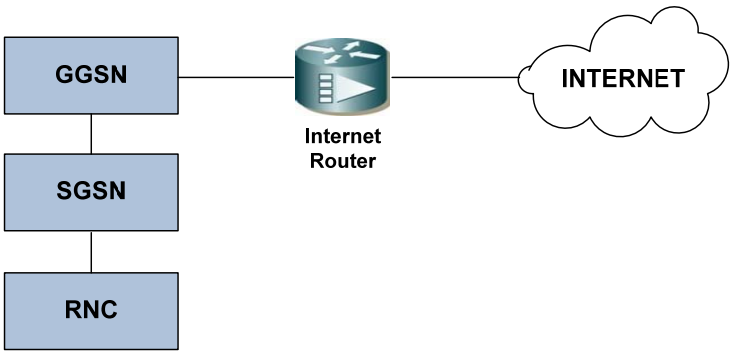


Figure 8. Mobile device's intrusion prevention (IP) connectivity.

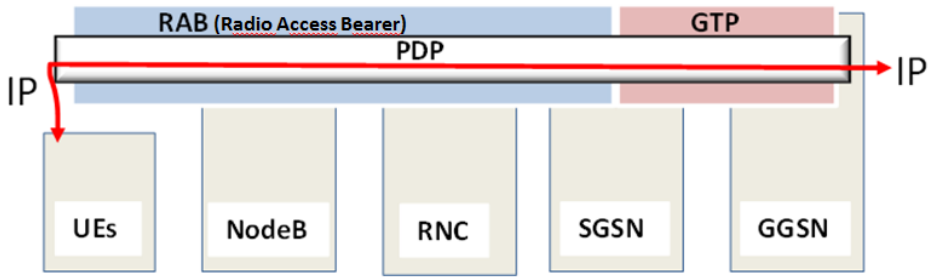


Figure 9. Serving GPRS support node (SGSN) CPU usage with/without TCP access control list (ACL).

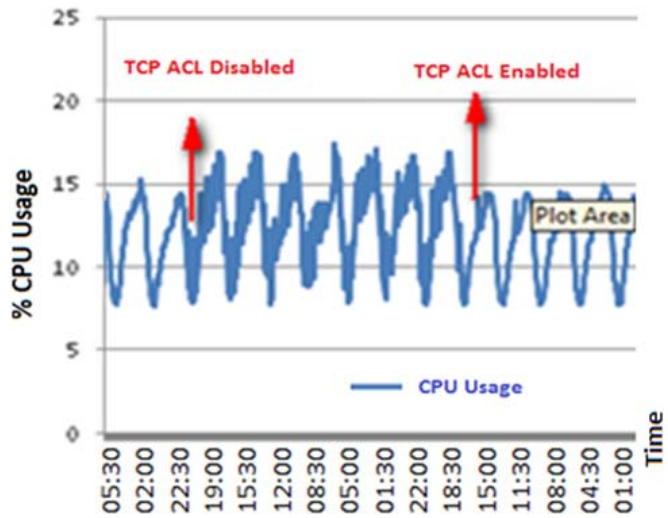
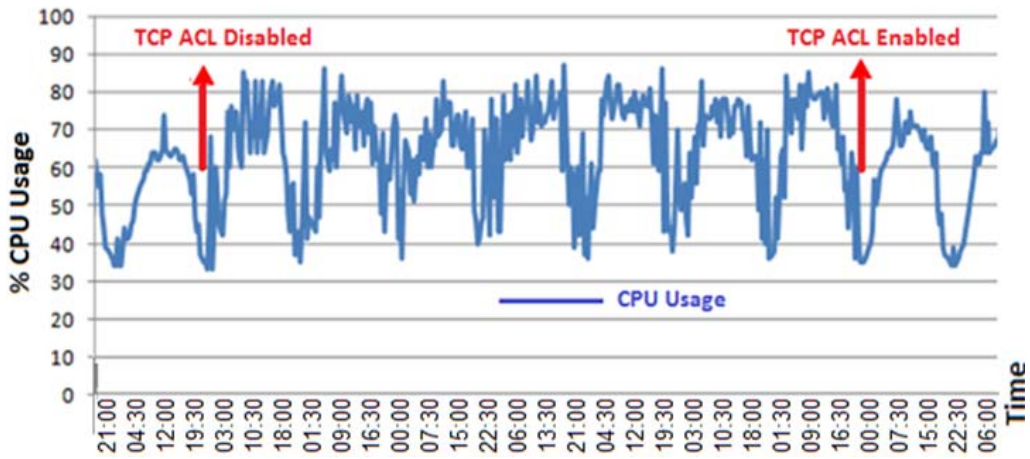


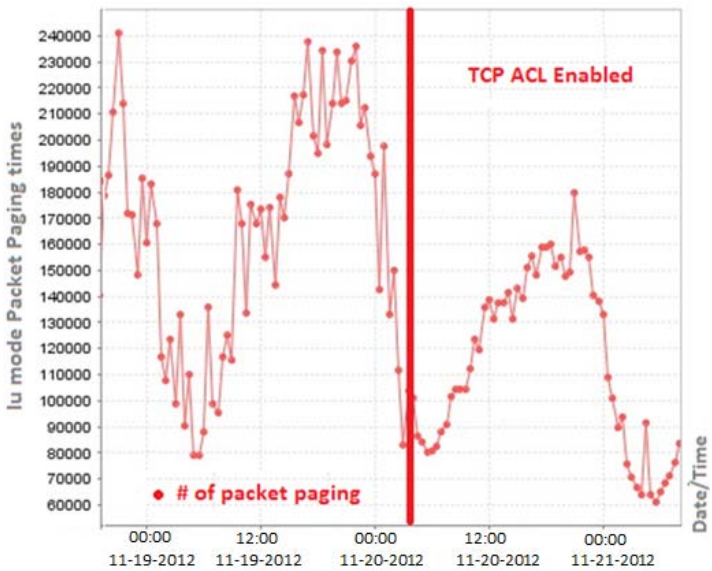
Figure 10. RNC CPU usage with/without TCP ACL.



These results do not mean that we are under a TCP SYN based attack all the time but there is some TCP based traffic from the Internet to our 3G subscribers' subnet. Therefore, the CPU usage is decreasing after applying the TCP based ACL that blocks the unnecessary traffic from the Internet.

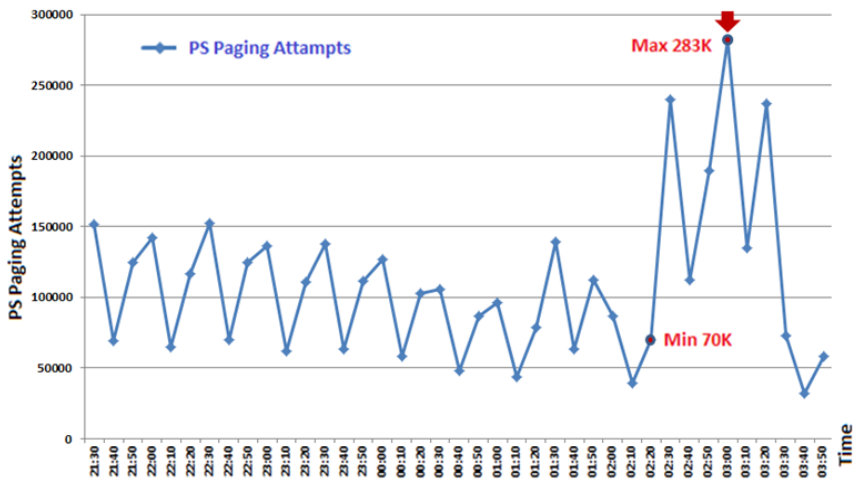
Paging activity on the RNC also decreased from 240,000 to 160,000, *i.e.*, by approximately 33%, after applying the ACL on the Internet router, as shown in Figure 11 where the vertical and horizontal axes show the number of paging activity and date/time, respectively.

Figure 11. Number of paging activity on an radio network controller (RNC) with/without applying an ACL.



These results made us also think about the risks that could occur due to UDP based attacks. Therefore, using UDP packets, we performed some attacks against our 3G network. By using some free open source tools, we sent UDP packets of size 60 bytes at a rate of 60,000 to 100,000 packets per second from the Internet to our 3G network. We performed our attacks at midnight between 02:30 and 03:00 a.m. to minimize the adverse effects to the customers. During these attacks, the number of paging and amount of CPU usage on our core network devices dramatically increased as shown in Figure 12. As seen in the figure, the RNC's PS paging attempt count was 70,000 just before attack and during the attack it reached 283,000. Hence, the number of pagings increased by approximately 304% due to our attack.

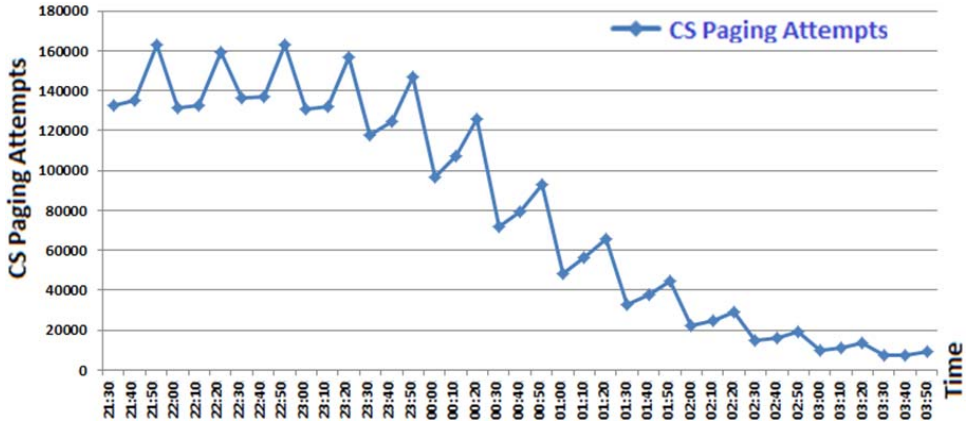
Figure 12. RNC PS paging attempts during the user datagram protocol (UDP) based attacks (sampling period is 30 min).



PS paging activity dramatically increased on the RNC and SGSN when we sent bulk data traffic to the subnets of the 3G subscribers. However, CS paging [23] is not affected during that time. Both the PS and CS paging activity decreased after midnight due to the decreasing number of phone calls. Figure 13

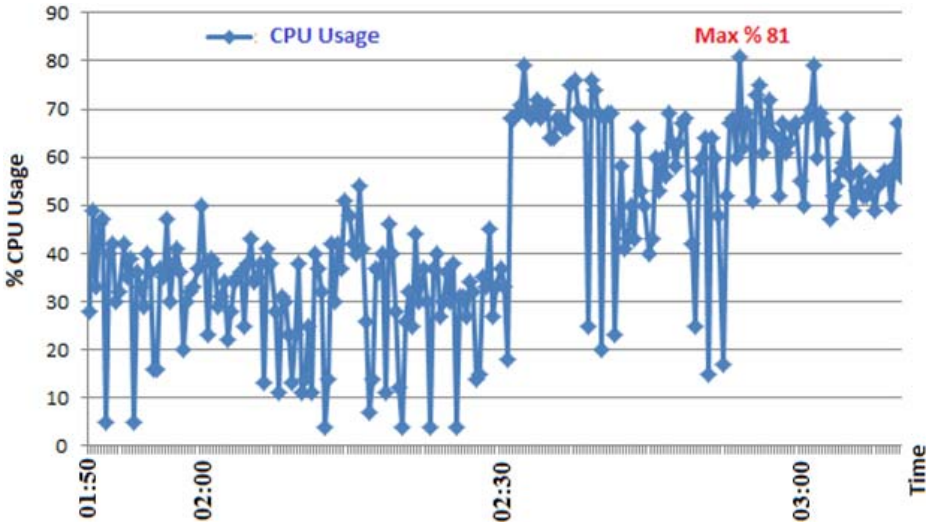
shows how the same RNC's CS paging activity changes during the same time interval. This shows that the PS paging and the CS paging are used for different purposes. The CS and PS paging activities are triggered by the MSC and GGSN, respectively. In other words, PS paging is data-oriented and CS paging is voice-oriented. They use different signaling channels until the RNC. However, they use the same control channel from the RNC to NodeB. Therefore, all voice and data transmission can be effected if it is overloaded by an attacker who exploits PS paging.

Figure 13. Circuit switched (CS) paging attempts on the RNC during the UDP based attack.



During our attacks, we observed that the CPU usage of an RNC increased. In Figure 14, the RNC CPU usage during the UDP attack is given with a sampling period of 1875 s.

Figure 14. RNCs CPU usage during the UDP based attack.



In this work, we first examined the effect of unwanted data traffic on cellular network devices such as the RNC and SGSN. We realized that blocking unnecessary TCP traffic from the Internet to 3G subscribers' IP subnets decreases not only the resource usage on cellular network devices but also the number of paging attempts on the RNC. However, we did not apply the UDP based access restriction on our Internet router due to the router's limited filtering capability. In order to see the effects of UDP based DoS/DDoS or flooding attacks from the Internet, we performed a UDP based attack at midnight because of the smallest data and voice load on cellular network at that time. The CPU usage and

number of PS paging attempts of the RNC was dramatically affected, although the attack was not sophisticated and it was not performed during peak hours. All these results show that mobile cellular networks are more vulnerable against unwanted bulk traffic caused by DoS/DDoS or flooding attacks.

As we discussed before, the RNC is one of the most critical device in a mobile network. It is related to both data and voice services. Hence, both voice and data subscribers will be affected if the RNC is out of service due to a CPU overload caused by high traffic resulting from attacks or malicious software [24] such as viruses [25], worms, *etc.*

5. Countermeasures against 3/4G Security Threats

The mobile communication industry has been getting a rise during the last three years. Hence, the security issues in mobile communications have become increasingly more important in 2013 [26]. Therefore, not only mobile operators but also mobile device users should be careful when using services over a mobile network. We focused especially on the mobile operators' security vulnerabilities when they don't protect their customers and networks against cyber threats. So, we will mention only the countermeasures that could be taken on the mobile operator's side. Security countermeasures against the security threats on the 3G border and core network devices could be summarized as follows:

1. Stateful IP packet filtering could be applied on the Internet border of the mobile network. This task could be achieved by an Internet router with firewall feature with both TCP and UDP stateful packet filtering functionality. A second option is to use a firewall device between the GGSN and the Internet router. The packet filtering device must be stateful for TCP and UDP, and drop all unnecessary traffic from the Internet to the mobile operator or to the customers. The drawback of the stateful firewall solution is the limitations in a firewall's session state table;
2. Carrier-grade Network Address Translation (NAT [27], CGN [28]) is used both to mitigate IPv4 exhaustion and to block unnecessary traffic from the Internet. But when a CGN is used, it is not possible to allow the traffic from the Internet to the subscribers, which is a drawback in using the CGN;
3. Configuration should be done against IP address spoofing [29] on the IP packet filter device or the Internet router;
4. The flooding and the DoS/DDoS type of attacks are the most dangerous and effective ways to destroy target devices. They could be performed individually or organized, e.g., using a botnet [30,31]. A high number of connection requests could put most stateful firewalls out of service due to limitations in their state tables. Therefore, a DoS/DDoS protection service or product should be used against attacks coming from the Internet. Generally, it is recommended that DDoS protection is placed in the ISP's side [32];
5. Mobile to mobile traffic could cause spreading of worms and viruses. This can be dangerous for both mobile devices and mobile operators, especially when worms/viruses act in an organized manner forming a botnet. Therefore, mobile to mobile traffic should be filtered by the GGSN or an IP filtering device;
6. Malware [33] or botnet members can generate flooding traffic to their victims such as mobile devices or operators, causing service interruptions on core network devices. Hence, rate

limiting [34] should be applied to mobile user traffic on the GGSN or an IP packet filtering device should be used to avoid this threat;

7. Directed broadcast [35] traffic must be denied on the GGSN to protect against DDoS attacks;
8. RA and LA scope optimization should be done according to the best practices to decrease paging effects;
9. Parameter optimization on RNC and SGSN should be done according to the best practices to decrease the PS paging effect;
10. Mobile operators could locate the GTP aware firewall products between the SGSN and the GGSN to block attacks coming through the GTP protocol;
11. The PS and the CS paging control channels should be isolated to prevent the CS paging from being overloaded by the PS paging channel under attack. Hence, at least voice communication service would not be affected in the case of an attack against the PS paging channel.

A pictorial summary of all the countermeasures to be taken on the mobile operator's side can be seen in Figure 15. The advantages and disadvantages of using the above mentioned countermeasures are listed in the Table 1.

Figure 15. Application points for possible countermeasures on an ISP and a mobile operator's network.

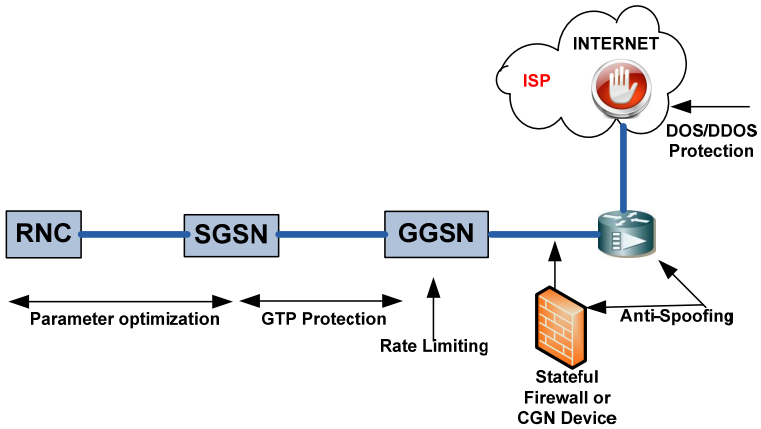


Table 1. Advantages and disadvantages of possible countermeasures against DoS and DDoS attacks on 3G mobile networks.

Protections	PROS	CONS
DDoS Protection on ISP	Effective DDoS protection	Extra cost
Stateful Firewall	Effective and flexible IP filtering	Session state table limitations, Point of failure
CGN	Blocking unwanted traffic from the Internet	NAT table limitations, Lack of IP filtering, Point of failure
GTP Firewall	GTP attack protection	Extra cost, Point of failure
Parameter Optimization	No-cost and protection	N/A
User Isolation	Preventing organized internal attacks	Unforeseen UE-to-UE communication
Rete Limiting	Decreases the effect of attacks	N/A

Security solutions could be applied most easily and efficiently on the border of the Internet. We have shown that cellular mobile networks should be effectively protected by using firewalls, Intrusion Prevention Devices (IPS) and/or DoS/DDoS protection products on the border of the Internet. In addition to these solutions, DoS/DDoS protection on the ISP side is very important, due to the limitations in the session tables of stateful firewalls. DDoS protection service on the ISP side is expected to filter all flooding and DDoS attacks before they overload an Internet connection link and fill up the session table of a stateful firewall. Another security solution is to isolate the customer traffic in order to prevent spreading of malicious software which may otherwise result in subscriber dissatisfaction due to additional usage charges and also harm core network equipment.

6. Conclusions

In the IP world, most effective and easy to realize attacks are DoS and DDoS attacks. Especially, mobile cellular networks could be affected by these attacks unless necessary countermeasures are taken. We observed these threats on mobile networks and took some precautions to mitigate them. We realized some DoS attacks on a production mobile cellular network and measured their destructive effects on core network devices. Our study shows that security solutions can be applied most easily and effectively on the Internet border of mobile cellular networks and user access devices, before any unwanted traffic ever arrives at the core network. In addition to this, all devices throughout the mobile network should be hardened in terms of security against attacks. Furthermore, DDoS protection service located on the ISP side is becoming necessary for all telecom and enterprise companies.

As future work, we plan to change the Location Area Code (LAC) and Routing Area Code (RAC) parameters on the RNC, and observe resource usage and paging effects on an RNC under attack. Furthermore, by using the CGN and a stateful firewall as a border filtering device, the robustness of a mobile cellular network can be improved.

Acknowledgments

This work is supported in part by the grant EU FP7 Marie Curie IRG 256544.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. CBS Interactive Web Page. Japan First Country Where Data Revenues Exceed Voice. Available online: http://www.zdnet.com/japan-first-country-where-data-revenues-exceed-voice-7000011817 (accessed on 28 July 2013).
2. Ghosh, A.; Ratasuk, R.; Mondal, B.; Mangalvedhe, N.; Thomas, T. LTE-advanced: Next-generation wireless broadband technology. *IEEE Wirel. Commun.* **2010**, *17*, 10–22.
3. Technology Marketing Corporation Web Page. Mobile Revenue will Double by 2016, but Traffic will Increase Tenfold. Available online: http://www.tmcnet.com/topics/articles/2012/05/16/290655-mobile-revenue-will-double-2016-but-traffic-will.htm (accessed on 28 July 2013).

4. Itwire Web Page. Asia Pacific Mobile Data Revenues Tipped to Exceed Voice in 2016. Available online: http://www.itwire.com/your-it-news/mobility/49878-asia-pacific-mobile-data-revenues-tipped-to-exceed-voice-in-2016 (accessed on 28 July 2013).
5. Nagy, M.; Kotosová, M. An IP Based Security Threat in Mobile Networks. In Proceedings of the 35th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2012.
6. Ricciato, F. Unwanted traffic in 3G networks. *ACM SIGCOMM Comput. Commun. Rev.* **2006**, *36*, 53–56.
7. Ricciato, F.; Coluccia, A.; D'Alconzo, A. A review of DoS attack models for 3G cellular networks from a system-design perspective. *Comput. Commun.* **2010**, *33*, 551–558.
8. Serror, J.; Zang, H.; Bolot, J.C. Impact of Paging Channel Overloads or Attacks on a Cellular Network. In Proceedings of the ACM Workshop on Wireless Security (WiSe 06), Los Angeles, CA, USA, 29 September 2006.
9. Whitehouse, O.; Murphy, G. *Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks*; White Paper; Juniper Networks: Sunnyvale, CA, USA, 2004.
10. Wu, Z.; Zhou, X.; Yang, F. Defending against DoS Attacks on 3G Cellular Networks via Randomization Method. In Proceedings of the 2010 International Conference on Educational and Information Technology (ICEIT 2010), Chongqing, China, 17–19 September 2010.
11. Lee, P.P.C.; Bu, T.; Woo, T. On the Detection of Signaling DoS Attacks on 3G Wireless Networks. In Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), Anchorage, AK, USA, 6–12 May 2007.
12. Zhao, B.; Chi, C.; Gao, W.; Zhu, S.; Cao, G. A Chain Reaction DoS Attack on 3G Networks: Analysis and Defenses. In Proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM 2009), Rio de Janeiro, Brazil, 19–25 April 2009.
13. Cheng, C.M.; Kung, H.T.; Tan, K.S. Use of Spectral Analysis in Defense against DoS Attacks. In Proceedings of the Global Telecommunications Conference 2002, Taipei, Taiwan, 17–21 November 2002.
14. The European Telecommunications Standards Institute (ETSI). *Technical Specification: 3GPP TS 25.331*; version 8.1.0; ETSI: Valbonne, France, 2008. Available online: http://www.etsi.org/deliver/etsi_ts/125300_125399/125331/08.01.00_60/ts_125331v080100p.pdf (accessed on 28 July 2013).
15. Eng, K.Y.; Ali, A.M.; Baradello, C.; Turner, J.; Vlack, D.; Walters, S.M. Packet Switching *vs.* Circuit Switching in Future Integrated Services Digital Networks. In Proceedings of the 7th IEEE International Conference on Computer Communications, New Orleans, LA, USA 27–31 March 1988.
16. Killalea, T. *Recommended Internet Service Provider Security Services and Procedures*; BCP 46 and RFC 3013; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2000.
17. Lyman, C.A. Computer communication standarts. *ACM SIGCOMM Comput. Commun. Rev.* **1984**, *14*, 46–52.
18. Ericsson Inc. GPRS System Survey. In *Student Book*; LZT 123 5347 R4A; Ericsson: Stockholm, Sweden, 2005.

19. Ozugur, T. Multiobjective Hierarchical Location and Routing Area Optimization in GPRS and UMTS Networks. In Proceedings of the 2002 IEEE International Conference on Communications (ICC 2002), New York, NY, USA, 28 April–2 May 2002.
20. Leavitt, N. Mobile phones: The next frontier for hackers? *Computer* **2005**, *38*, 20–23.
21. Becher, M.; Freiling, F.C.; Hoffmann, J.; Holz, T. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 22–25 May 2011.
22. Newman, D. *Benchmarking Terminology for Firewall Performance*; RFC 2647; Internet Engineering Task Force (IETF): Fremont, CA, USA, 1999.
23. The 3rd Generation Partnership Project (3GPP) Technical Specification Group. *Technical Specification*; 23.060 V6.11.0; 3GPP: Valbonne, France, 2005.
24. Leavitt, N. Malicious code moves to mobile devices. *IEEE Comput.* **2000**, *33*, 16–19.
25. Dagon, D. Mobile phones as computing devices: The viruses are coming! *IEEE Pervasive Comput.* **2004**, *3*, 11–15.
26. Mobile Marketer Web Page. Top Mobile Security Threats for 2013. Available online: http://www.mobilemarketer.com/cms/news/strategy/14518.html (accessed on 28 July 2013).
27. Egevang, K.; Francis, P. *The IP Network Address Translator (NAT)*; RFC 1631; Internet Engineering Task Force (IETF): Fremont, CA, USA, 1994.
28. Jiang, S.; Carpenter, B. *An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition*; RFC 6264; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2011.
29. Ferguson, P.; Senie, D. *Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing. BCP 38 and RFC 2827*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2000.
30. Tyagi, A.K.; Aghila G. A wide scale survey on botnet. *Int. J. Comput. Appl.* **2011**, *34*, 9–22.
31. Sharma, R.K.; Chandel, G.S. Botnet detection and resolution challenges: A survey paper. *Int. J. Comput. Inf. Technol. Bioinforma.* **2009**, *1*, 10–15.
32. Douligeris, C.; Mitrokotsa, A. DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Comput. Netw.* **2004**, *44*, 643–666.
33. Lawton, G. Is it finally time to worry about mobile malware? *IEEE Comput.* **2008**, *41*, 12–14.
34. Morrow, C.; Jones, G. Filtering and Rate Limiting Capabilities for IP Network Infrastructure. Available online: https://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09 (accessed on 28 July 2013).
35. The European Telecommunications Standards Institute (ETSI). *Technical Specification*; 3GPP TS 29.060 V9.3.0 (2010-06); ETSI: Valbonne, France. Available online: http://www.etsi.org/deliver/etsi_ts/129000_129099/129060/09.03.00_60/ts_129060v090300p.pdf (accessed on 28 July 2013).