Botnets in 4G Cellular Networks: Platforms to Launch DDoS Attacks Against the Air Interface

Preprint (accepted version)

Presented in 2013 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), 19-21 August 2013, Montréal, Canada , DOI: 10.1109/MoWNet.2013.6613793

Botnets in 4G Cellular Networks: Platforms to Launch DDoS Attacks Against the Air Interface

Masood Khosroshahy, Dongyu Qiu, and Mustafa K. Mehmet Ali
Electrical and Computer Engineering Department
Concordia University
Montreal, Canada
E-mails: m.kh@ieee.org, {dongyu, mustafa}@ece.concordia.ca

***Abstract*—Botnets are overlay networks built by cybercriminals from hacked smartphones and computers. In this paper, we report a vulnerability of the air interface of 4G cellular networks, the Long Term Evolution (LTE), to Distributed Denial-of-Service (DDoS) attacks launched from botnets. The attack scenario constitutes of a botmaster instructing the botnet nodes to start sending or downloading dummy data in order to overwhelm the air interface, thereby denying service for voice users. Through simulation using a capable LTE simulator, we determine the number of botnet nodes needed per cell that can effectively render the cellular network unusable. Specifically, we show that a botnet that has spread to only 3% of subscribers is capable of lowering the voice quality from 4.3 to 2.8 in Mean Opinion Score (MOS) scale of 1 to 5 for scheduling strategies designed for real-time flows. On the other hand, a botnet that has managed to spread to 6% of subscribers can cause a MOS value of 1, i.e., a complete outage. The threat identified and the reported results could inspire the implementation of new mechanisms to ensure the security and availability of vital telecommunication services.**

***Keywords*—Cellular radio, Long Term Evolution, Communication system security, Computer viruses, Botnets.**

I. Introduction

Long Term Evolution (LTE) is the main air interface technology for the 4G cellular networks. Voice over LTE is being, or scheduled to be, offered using the packet-switched technologies, rather than using the traditional circuit-switched ones [1]. Further, IP Multimedia Subsystem (IMS) is scheduled to be deployed in the core network with the LTE being the primary cellular access technology. Such a paradigm shift in offering vital telecommunication services has many technological benefits, but it also presents a host of other new challenges, the most important of which, in our view, is the maintenance of security and availability of service in the face of Internet-world security threats such as botnets.

In this section, we first describe what botnets are and what kind of threat they pose. Next, the iKee.B botnet is introduced which was a botnet designed for cellular networks. Some hypothetical cellular botnet designs are explored afterwards which are few examples showing the growing interest of researchers in exploring and understanding potential cellular botnets. We then examine a study which quantified the threat of botnets in 2G/3G cellular networks by focusing on attacking a core network element. We finish this section by explaining the contribution of this paper, i.e., identification and evaluation of botnet threat against the air interface in 4G networks. In Section II, we describe the simulation scenario that we have used in order to quantify the threat against the 4G air interface; the section ends with the simulation results giving some indication regarding the needed botnet size in order to seriously impact the service availability. The paper concludes in Section III with some final thoughts as well as potential future work.

A. Botnet Threat in Cellular Networks

Botnets, i.e., network of (ro)bots, are overlay networks built from compromised devices by cybercriminals known as botmasters. The botmasters use many methods to infect these Internet-connected devices, including e-mail attachments, worm scans, and vulnerable network services. Once the device is compromised, the malware residing in the device connects to a central Command & Control (C&C) server or joins a Peer-to-Peer (P2P) network, i.e., the botnet. Once connected to the botnet, the compromised device can receive the commands of the botmaster; such commands provide instructions to upload personal data and to engage in Distributed Denial-of-Service (DDoS) attacks, among other illicit activities. The threat of botnets and DDoS attacks due to the all-IP,

non-circuit switched architecture, has been reported to be the greatest concern of telecom operators [2]. As botnets have shown to be the platform of choice to launch DDoS attacks in the Internet [3], the aforementioned concern of the operators is very well placed.

B. Meet iKee.B Botnet

Botnets, however, are already operating in cellular networks and the threat is not a hypothetical one. An example of a cellular botnet is iKee.B which was released in November 2009 and targeted iPhone users in several countries in Europe and Australia; the incident and the client code have been examined in [4]. It is reported that iKee.B was the successor to iKee.A; the latter was released shortly beforehand in Australia and managed to infect an estimated 21,000 iPhone users within a week. iKee.B was spotted in Europe, however, and was the more capable version of the malware, possessing many of the important features of modern-day botnets: ability to self-propagate, carrying of malicious payload, and the functionality to connect to the C&C server to receive updates and commands from the botmaster.

C. Studies on Hypothetical Cellular Botnets

Recognizing the threat of botnets in cellular networks, many researchers have recently started to examine how botnets can be constructed in such networks: In [5], it has been shown how the Session Initiation Protocol (SIP), which is used in IMS for service delivery, can be abused to conceal botnet traffic which would prevent the detection of a botnet in 4G cellular networks. An example of in-the-lab cellular botnet is the implementation and evaluation of an iPhone-based mobile botnet [6]. In this work, authors report having tested a P2P-based and an SMS-based C&C mechanisms for the botnet and conclude that a hybrid approach of SMS- and HTTP-based C&C mechanism is the most threatening structure due to the difficulties in detection that it presents. Finally, a simulation study to evaluate the performance of a hypothetical botnet which utilizes SMS messages for the C&C of the botnet and has a Kademlia-based P2P structure is reported in [7]. Similar to the research that has been done for several years now for botnets operating in the wired Internet world, these studies provide ideas on how to develop mitigation strategies for botnets operating in the wireless/cellular networks.

D. Botnet-launched DDoS Attacks in 2G/3G Networks

Regarding the threat of botnets in 2G/3G cellular networks, the work done in [8] is perhaps the most detailed, with convincing and worrying results. In the study, a DDoS attack on the Home Location Register (HLR) has been tested. A DDoS attack that can successfully overload the HLR would make the network unusable for the clients. In order to carry out the attack, they have chosen to test various signaling requests sent by handsets; these requests must be processed by the HLR. After several tests, they have determined that, in 2G/3G networks, "Insert/Delete Call Forwarding" is the most demanding request that can be sent by the handsets that needs to be processed by the HLR. The DDoS attack then constitutes of handsets simultaneously sending such requests to the HLR. To determine whether or not the generated traffic overloads the HLR, a several-computer testbed has been built using a traffic generating and benchmarking suite. The result of the tests is the number of botnet nodes needed by the botmaster in each HLR service area in order to overload the HLR. Depending on the traffic condition and the capacity of the HLR system, the numbers range from 11,750 to 141,000 botnet nodes (infected phones). With the assumption of one million users serviced by each HLR, the paper concludes, the needed infection rate would be between 1.2% and 14.1%.

E. Our Contribution: Presentation and Evaluation of DDoS Attacks Against the Air Interface of 4G Cellular Networks

The contribution of this paper is the introduction and evaluation of the threat of attacking the air interface which always has limited capacity due to the limited frequency spectrum available for such networks. 4G cellular networks, with their packet-switched mechanism and support of rich multimedia applications, are particularly vulnerable to such DDoS attacks that can be launched at will from a botnet operating in the cellular network. We therefore consider the air interface as the *main target* of the DDoS attack; the attack scenario would be as follows: when the botmasters create a botnet using smartphones, they can either activate all botnet nodes using a command or pre-program the nodes to wake up at a certain time. At the moment of attack, all botnet nodes can either start downloading a large file (a YouTube video, for example) to create congestion on the downlink or send dummy data to an arbitrary destination to create congestion on the uplink. The effect of the congestion is that most clients would no longer be able to effectively use the

cellular network which is the same effect predicted in [8] caused through overloading an HLR in 2G/3G networks. In the next section, we determine the needed botnet nodes per cell through a simulation study done using a highly capable open-source LTE simulator. The knowledge about existence of such a threat and how it might impact the availability of service, especially in emergency situations where the system already operates at capacity, is important and may lead to the designing of countermeasures by the operators.

II. Impact of Botnets: A Simulation Study

A. Simulation Scenario

In order to do performance evaluations of the LTE air interface, one of the best options is to use the LTE-Sim simulator [9]. As a feature-rich simulator, LTE-Sim has everything we need to assess the congestion caused by the DDoS attack on the air interface: it has an implementation of the physical layer, radio resource schedulers, applications (Voice over IP [VoIP], video, etc.), and a full protocol stack. In our scenario, VoIP uses a G.729 voice codec and the voice flow alternates between On and Off periods to model the natural silences in human conversation [9]. The duration of On periods is exponentially distributed with a mean value of 3 secs. On the other hand, the Off periods have a truncated exponential distribution with an average of 3 secs and an upper limit of 6.9 secs. During the Off period, the sending rate is zero, as a voice activity detector is assumed to be present. During the On period, the source sends with the rate of 8 Kbps (20 bytes every 20 msec.). Finally, the video flow uses realistic video trace files of type H.264 Foreman sequence with a bit rate of 242 Kbps [9].

The whole evaluation of the botnet-launched DDoS attack takes place when the system operates at or near capacity, as we are concerned with times when the system is already under pressure to service many users due to an emergency; the assumption is that the cellular system has already been planned and deployed to be able to deal with a hypothetical emergency situation. When operating at capacity, the botnet attack is launched and we observe the effect of such an attack and determine the needed botnet nodes per cell in order to effectively deny service to users.

The simulated scenario is depicted in Fig. 1. We consider that there is a botnet built by a botmaster that can be activated to launch a DDoS attack against the air interface. The total botnet size is equal to the number of botnet nodes per cell times the number of cells. In each simulation run, there are a number of botnet nodes that are configured to download video simultaneously and there are other normal nodes (users) in the simulation that would be using VoIP in the meantime. We then examine the relationship between the number of botnet nodes and the level of degradation of service quality for the VoIP users.

In this work, due to simulator limitations, we only examine the case that all calls can pass through any call admission control module that might be present. It is noteworthy that even the presence of any such module does not diminish the threat posed by botnets, as the module cannot differentiate between any VoIP/video calls initiated by the botnet and the legitimate VoIP calls. The botnet therefore still manages to decrease the available capacity of service considerably.

As we are examining an extreme case in terms of number of User Equipments (UEs) and the fact that LTE-Sim is a particularly detailed simulator, each simulation run of 100 seconds takes 24 hours to complete in a powerful PC. In order to reduce the time needed for each run to 24 hours, however, we had to simulate a rather small network size of one cluster of 3 cells, with each cell having 5 MHz allocated downlink bandwidth. The cell radius is 1 km and users move around with a pedestrian speed of 3 km/h according to the Random Walk mobility model [10]; the UEs may hand over to the eNodeB of the neighboring cell due to changing power reception levels. As will be shown later on, with the aforementioned configuration for the cellular network, each cell/eNodeB has a capacity of servicing 100 VoIP users simultaneously; above this threshold, the quality of service starts to drop below industry standards. While examining the botnet-launched DDoS attack when the system operates at this maximum capacity, we also compare the performance of the main three downlink schedulers: (1) Proportional Fair (PF); (2) Modified Largest Weighted Delay First (MLWDF); and (3) Exponential Proportional Fair (EXP/PF). The details of these schedulers are beyond the scope of this paper and it suffices to mention that MLWDF and EXP/PF are designed to deal with real-time flows, while PF treats every flow the same. One key difference would therefore be that MLWDF and EXP/PF erase packets belonging to real-time flows from the queue if those packets cannot be sent within a reasonable delay; this is done to avoid wasting bandwidth.

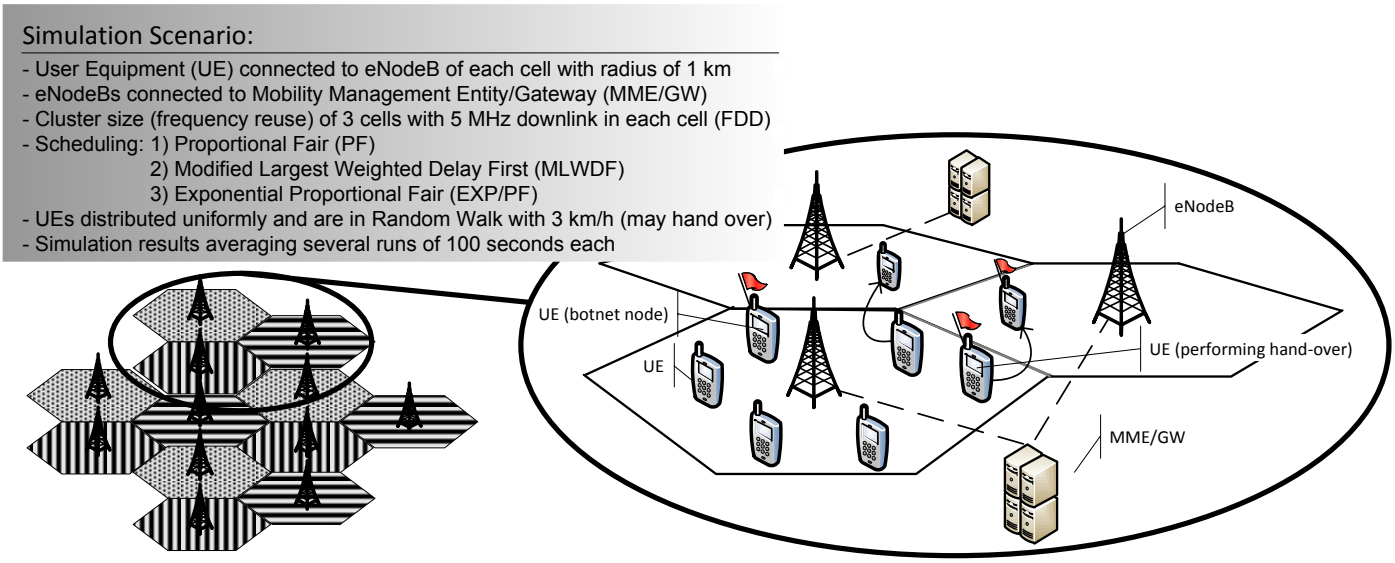


Fig. 1: Simulation Scenario: User Equipments (UEs) carrying VoIP sessions as well as botnet nodes starting dummy video sessions both moving around

B. Determining the Cell Capacity

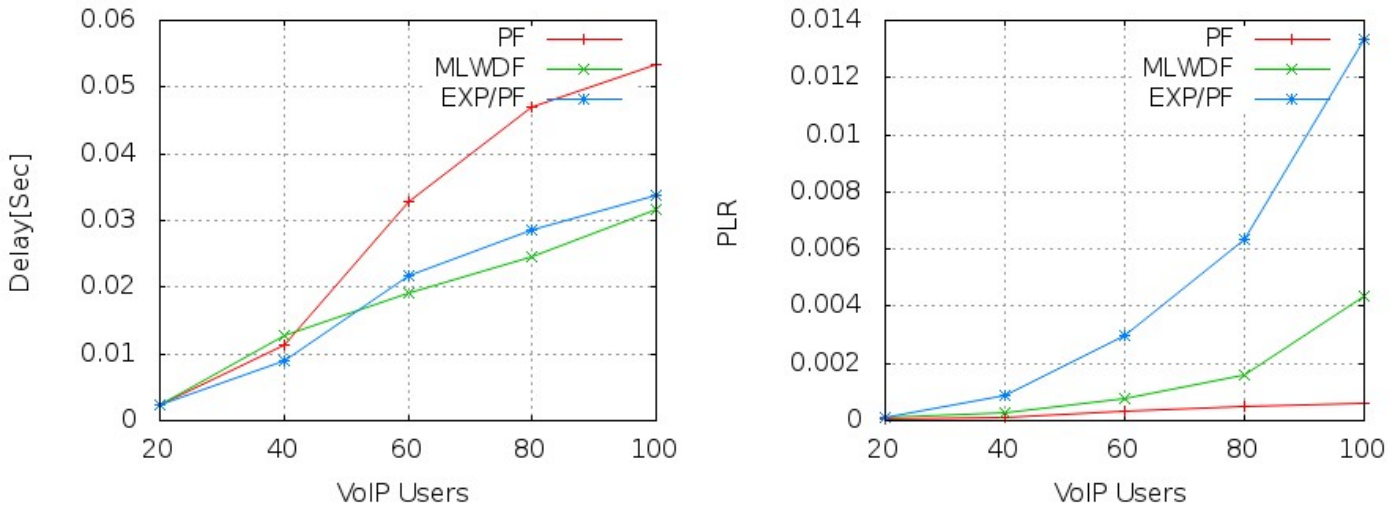
We first determine the cell capacity in the set up cellular network by increasing the number of VoIP users and monitoring each VoIP user's delay and packet loss ratio (PLR); see Fig. 2. In each sub-figure, results are reported for all the downlink schedulers. Considering the VoIP quality metrics, we see that the cell capacity is around 100 simultaneous VoIP users; these metrics will be elaborated on shortly.

We now need to determine the average number of subscribers that are present in a cell which has the capacity of serving 100 simultaneous VoIP users. For this, we turn to reports on user behavior regarding average monthly phone conversations. According to [11], a typical mobile phone user talks 761.5 minutes on average per month; the daily average would therefore be about 25 minutes. Assuming that most phone conversations happen in the period from 8 a.m. to 10 p.m. (i.e., a 14-hour slot in each 24 hours), we have: $25\ \textit{mins.}/(14 \times 60\ \textit{mins.}) \approx 3\%$. We can then state that each subscriber is actively using the system resources (i.e., it becomes one of the 100 simultaneous VoIP users) about 3% of the time each day[1]. Therefore, we can now consider that the maximum number of simultaneous VoIP users is about 3% of the average number of subscribers that are present in each cell. As our set up network had the capacity of serving 100 simultaneous VoIP users, then the average number of subscribers at this capacity would be about 3,300. This 1-to-33 relationship between the number of simultaneously-active users and the average number of subscribers has also been considered to be a reasonable estimate in real-world LTE deployments by [12].

[1]Note that assuming a complete 24-hour slot, instead of the 14-hour slot, will lead to a percentage lower than 3%; hence, the needed percentage of botnet spread among subscribers of each cell to cause an outage, as will be determined later one, will be even lower.

C. VoIP Quality Metrics

Before proceeding further, we briefly introduce key VoIP quality metrics, as these will be needed in order to understand the observed degradation of service. Mean Opinion Score (MOS) is a subjective measurement of voice quality described in ITU recommendation P.800. MOS value for a voice communication ranges from 1 (impossible to communicate) to 5 (very satisfied). The two main VoIP quality metrics affecting MOS are packet loss and delay. Mouth-to-ear (one-way) delay is usually considered acceptable as long as it is below 150 msec. We, however, measure the packet delays only on the air interface which must be significantly less than 150 msec in order to satisfy the mouth-to-ear threshold. On the other hand, as we use the common G.729 voice codec in the simulator, we refer to results reported in [13] to point out that packet loss for this codec (with replacing the lost packet by the repetition method) leads to MOS going



(a) Delay

(b) PLR

Fig. 2: Determining cell capacity; increasing number of VoIP users until Delay and Packet Loss Ratio (PLR) reach maximum acceptable levels.

down from 4.3 (with 1% packet loss) to 2.8 (with 20% packet loss); the decrease is near linear and no results are reported for above 20% loss, as this would be completely unacceptable. Nonetheless, as MOS has degraded in a linear fashion from 1% packet loss to 20% packet loss, we can expect that at 50% packet loss, we will have a MOS value of 1 (impossible to communicate).

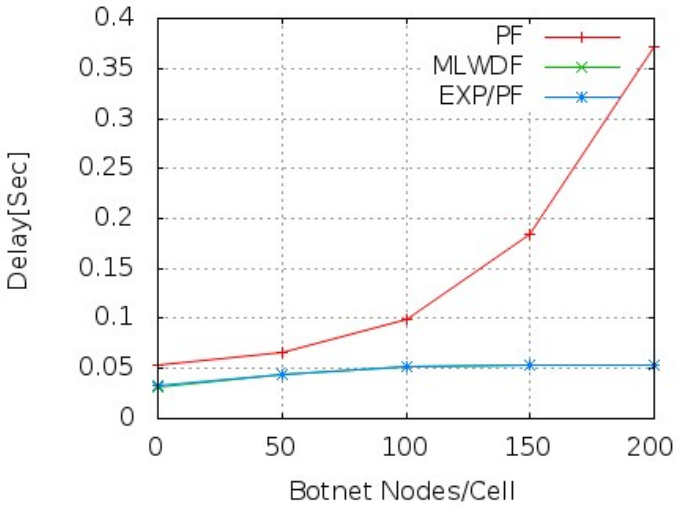
D. Determining the Effect of Botnet-launched DDoS Attack

At the maximum capacity, i.e., while 100 VoIP users are being served, we now start adding an increasing number of botnet nodes which download video while the VoIP users continue their sessions. The effect of botnet nodes on the VoIP quality of those 100 users is reported in Fig. 3. It can be seen that while the PF scheduler keeps the PLR near acceptable levels, the delay becomes increasingly large which hinders a proper phone conversation. Note that the shown delays are only the air interface delays which must be a small fraction of the acceptable mouth-to-ear delay of 150 msec. On the other hand, MLWDF and EXP/PF schedulers are designed for real-time flows and as such, drop many packets due to large delays to save bandwidth, as those delayed packets are no longer useful. These two schedulers hence show an acceptable level of delay, however, the PLR reaches 20% with 100 botnet nodes and reaches 50% with 200 botnet nodes. Note that 100 botnet nodes and 200 botnet nodes represent a 3% infection rate and a 6% infection rate, respectively, among the subscribers in each cell.

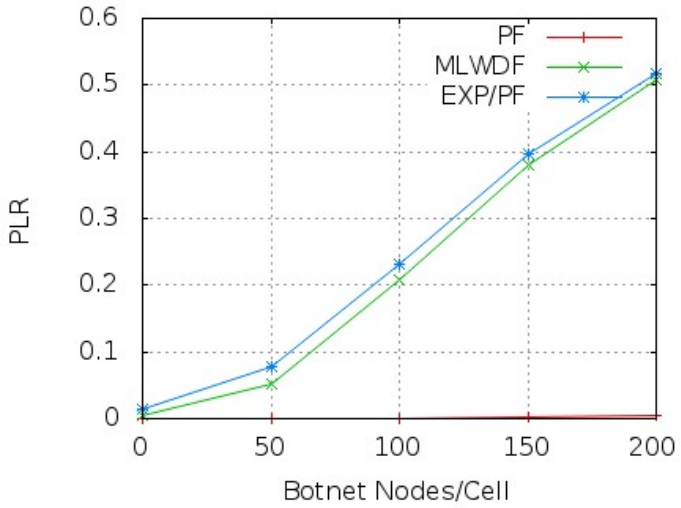
III. Conclusion and Future Work

In this paper, we identified a potentially devastating threat against the LTE/4G cellular networks, i.e., launch of a DDoS attack against the air interface which is simple to implement and does not require inside knowledge about core network elements. Through the simulations, we determined that a botnet that has spread to only 6% of subscribers can effectively cause an outage in cellular services, particularly in peak hours and especially in emergency situations. Contrasting this percentage with up to 14.1% botnet spread needed in 2G/3G networks, reported in [8], 4G/LTE networks seem to be much more vulnerable to botnet-launched DDoS attacks. We hope that the exposed vulnerability and results shown would lead to the implementation of mechanisms to eliminate such a threat.

As future work, we intend to pursue the following two directions: (1) in light of the threat exposed in this paper, we intend to investigate potential mitigation techniques in order to reduce and possibly eliminate the threat of the air interface falling victim to a DDoS attack. One possible mitigation technique would be the enhancement of the call admission control module so that the module



(a) Delay



(b) PLR

Fig. 3: Determining the effect of botnet-launched DDoS attack on 100 VoIP users that share resources with an increasing number of botnet nodes.

is able to screen, detect, and prevent rogue calls; and (2) following the work reported in [8] and described earlier, it is certainly relevant to determine how a botnet could attack a core network element in 4G systems. The equivalent of a Home Location Register (HLR) in 2G/3G networks is the Home Subscriber Server (HSS) of IMS in 4G networks. This research work could be carried out as soon as IMS implementations reach maturity and hardware specifications of HSS are known in order to test HSS's capacity and overload thresholds.

REFERENCES

[1] "Voice and video calling over lte," Ericsson, White paper 284 23-3163 Uen, Feb. 2012. [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/WP-Voice-Video-Calling-LTE.pdf

[2] A. Berger, I. Gojmerac, and O. Jung, "Internet security meets the ip multimedia subsystem: an overview," *Security Comm. Networks*, vol. 3, no. 2-3, pp. 185–206, 2010.

[3] C. Elliott, "Botnets: To what extent are they a threat to information security?" *Information Security Technical Report*, vol. 15, no. 3, pp. 79 – 103, 2010 (computer crime - a 2011 update).

[4] P. A. Porras, H. Saidi, and V. Yegneswaran, "An analysis of the ikee.b iphone botnet," *MobiSec, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer*, vol. 47, pp. 141–152, 2010.

[5] A. Berger and M. Hefeeda, "Exploiting sip for botnet communication," in *Proc. 5th IEEE Workshop Secure Network Protocols*, 2009, pp. 31–36.

[6] C. Mulliner and J.-P. Seifert, "Rise of the ibots: Owning a telco network," in *Proc. 5th International Conference on Malicious and Unwanted Software (MALWARE)*, Oct. 2010, pp. 71 –80.

[7] Y. Zeng, K. G. Shin, and X. Hu, "Design of sms commanded-and-controlled and p2p-structured mobile botnets," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12. NY, USA: ACM, 2012, pp. 137–148.

[8] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in *Proc. 16th ACM conference on Computer and communications security*, ser. CCS. NY, USA: ACM, 2009, pp. 223–234.

[9] G. Piro, L. A. Grieco, G. Boggia, F. Capozzi, and P. Camarda, "Simulating lte cellular systems: An open-source framework," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 498–513, 2011.

[10] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, 2002.

[11] "Mobile usage data : The voice results compiled from one year (april 2009-march 2010) of 60,000 mobile subscribers," The Nielsen Company, Online Report, Aug. 2010. [Online]. Available: http://www.nielsen.com/us/en/newswire/2010/african-americans-women-and-southerners-talk-and-text-the-most-in-the-u-s.html

[12] N. Etminani, (Core Network Lead at Nokia Siemens Networks). Private communication, Nov. 15 2012.

[13] L. Ding and R. Goubran, "Speech quality prediction in voip using the extended e-model," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 7, Dec. 2003, pp. 3974 – 3978.