International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 32, Issue 01) and (Publishing Month: July 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN: 2319-6564
www.ijesonline.com

Enhancing the Security of LTE Networks against Jamming Attacks

Ali Babikher Bakheet and Dr. Hala Alddaw
Faculty of Engineering, AL-Neelain University, Khartoum, Sudan

Publishing Date: July 18, 2016

Abstract

The long-term advancement (LTE) is the new mobile communication system, built after a redesigned physical part and predicated on an orthogonal regularity division multiple gain access to (OFDMA) modulation, features solid performance in challenging multipath surroundings and substantially boosts the performance of the cellular channel in conditions of pieces per second per Hertz (bps/Hz). Nevertheless, as all cordless systems, LTE is susceptible to radio jamming episodes. Such dangers have security implications especially regarding next-generation disaster response communication systems predicated on LTE technology. This proof concept paper overviews some new effective attacks (smart jamming) that extend the number and effectiveness of basic radio jamming. Predicated on these new hazards, some new potential security research guidelines are introduced, looking to improve the resiliency of LTE systems against such problems. A spread-spectrum modulation of the key downlink broadcast stations is coupled with a scrambling of the air tool allocation of the uplink control stations and a sophisticated system information subject matter encryption scheme.

Keywords: *LTE, Jamming, Security, OFDMA.*

1. Introduction

The long-term advancement (LTE) is the lately deployed standard technology for communication sites, offering higher data rates of speed and upgraded bandwidth. This new mobile communication system is the natural advancement of 3rd Technology Partnership Task (3GPP)-based access sites, improving the Common Mobile Telecommunications System (UMTS).

LTE provides capacity to customer equipments (UEs) through a centralized project of radio resources. A recently increased physical (PHY) covering is implemented predicated on orthogonal frequency section multiple gain access to (OFDMA) and greatly increases the performance of the past wideband code department multiple gain access to (WCDMA) [1]. The new modulation scheme provides a huge capacity and throughput, potentially attaining a raw tad rate of 300 Mbps in the downlink with advanced multiple type multiple end result (MIMO) configurations [1].Because of its variety efficiency and great capacity, LTE is designed to be implemented as the foundation for the next-generation disaster response communication system, the Nationwide Interoperable Community Security Broadband Network [2].Within this context, the characteristics of such LTE-based general public safeness sites already are under concern on the market [3]. Note that, especially regarding this application, the security requirements of LTE communication networks are of paramount importance. Regardless of the marvelous system and capacity improvements integrated by LTE, cellular systems are regarded as, as any sort of wireless network, susceptible to radio jamming. Though it is a well-known and simple assault, radio jamming is the most frequent way to kick off a localized denial of service (DoS) episode against a mobile network [4]. The impact of such disorders is very local and mainly constrained by the sent electric power of the jamming device. The attacker is merely able to deny the service to UEs positioned in its vicinity locally. However, more complex attacks have been learned as a more effective way to jam LTE networks [5 potentially,6].These smart jamming problems try to saturate specifically the key downlink broadcast route of LTE sites to be able to launch an area DoS attack that will require less power, so that it is stealthier. Complex attacks further, such as low-power smart jamming, identify the bodily source of information blocks (PRBs) allocated to essential uplink control stations by taking the unprotected broadcast emails sent from the bottom train station (eNodeB). The interception of such unencrypted network construction data allows the attacker to selectively saturate uplink control programs in order to increase the number of the assault to a whole cell or sector. Remember that network configuration within the broadcast channel can be leveraged to deploy a powerful rogue base train station and other varieties of attacks. Although radio jamming episodes have a fairly local range, they become highly relevant in today's cyber security circumstance. Reports of much targeted and extremely superior attacks have emerged over the last 2 years [7]. These attacks, popularly known as advanced persistent threats (APTs), span over months or even years and target large corporations and government institutions with the purpose of stealing intellectual property or other valuable digital assets [8]. A number of the proposed security alternatives involve large changes at the PHY level of LTE sites that could be very challenging to use over a commercial network and would require cooperation within the industry. Nevertheless, such security structures could substantially raise the stability and resiliency against security problems of the Nationwide Interoperable People Protection Broadband Network [2]. Anti-jamming improvements could be included to the set of requirements for LTE-based general population safety networks that aren't in the opportunity of current produces of the LTE standard, such as immediate group and communication communication [3].

2. Initial Access to LTE Networks

This section overviews the essential procedures essential for a cellphone to synchronize with and hook up with an LTE network, any UE eager to gain access to the network must execute a cell selection treatment first. Following this procedure, the UE decodes the physical broadcast channel (PBCH) to extract the essential system information which allows the other channels in the cell to be configured and operated. The announcements continued this programs are unencrypted and can be eavesdropped with a unaggressive radio sniffer. Once as of this true point, the UE can start an actual reference to the network through a random gain access to procedure and set up a radio gain access to bearer (RAB) to be able to send and acquire user traffic. The complete process is portrayed in Physique 1.

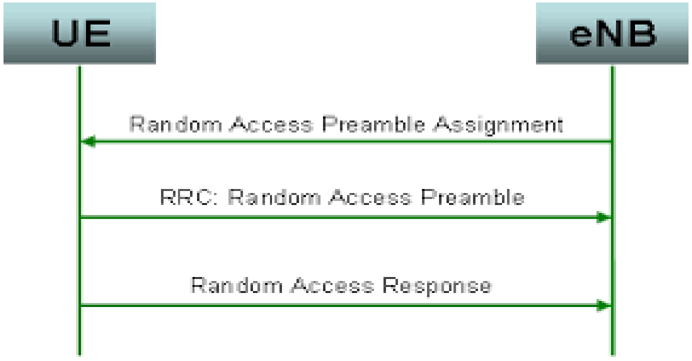
UE
eNB
Random Access Preamble Assignment
RRC: Random Access Preamble
Random Access Response

Figure 1: LTE Initial Access

3. Attacks against Cellular Networks

Radio jamming is the deliberate transmitting of radio impulses to disrupt marketing communications by lowering the SNR of the received transmission. This assault essentially contains blasting a high-power regular signal over the complete target strap of the machine under strike [4,9].

This invasion is broadly known as a straightforward and common way to assault a radio network and has been extensively examined in the books in the framework of wireless geographic area sites (WLAN) [4], sensor systems [10], and mobile networks [9]. Regardless of the attack's convenience, often, really the only solution is to find and neutralize the attacker, specially in the situation where the complete band of the operational system is being jammed. The very massive amount transmitted power, though, leads to lower life expectancy stealthiness so more elaborated schemes to jam cellular networks are being proposed in the literature.

It's been shown a standard barrage jamming strike is the perfect jamming strategy when the attacker does not have any knowledge of the mark sign [11]. This section overviews specific derivations of radio jamming disorders against cellular systems based on the data of the prospective LTE signal an attacker can buy from publicly available documents and expectations. A popular new threat vector that can be exploited as a total result of such attacks is also described.

3.1 Downlink Smart Jamming

Downlink smart jamming contains making malicious radio signals as a way to interfere with the reception of essential downlink control channels. A recent report introduces the potential theoretical results of playing the PBCH of LTE networks [5]. The authors of the first research expanded the details on this study in a recent paper [6]. This kind of attack, which could be applied to both 2G and 3G networks as well, targets this port because, as described in Section 2. 1, the assigned PRBs are known a priori and always mapped to the central 72 subcarriers of the OFDMA signal. Given that this channel is necessary to change and operate the other channels in the cellular, this jamming attack is characterized by a low duty cycle and a fairly low bandwidth.

The range of the jammer in this case is still rather small, with a very localized impact. The transmission and modulation characteristics of the PBCH still require a quite high-power interfering signal to deny the service to non cell edge users. Be aware that, in order to out power the genuine signal, the attacker is bounded by the large transmitted power at the eNodeB and the probably low transmitted benefits of the jamming device. Extra superior versions of this attack have been recommended, targeting the downlink preliminary signals employed by the UE to estimate the port for signal equalization [12].

However, Release 12 of the LTE standard covers the concepts of heterogeneous networks (HetNets), with strong enhancements in the pilot signals to avoid strong interference between the pilots sent by different overlaying cells (macrocells and pico/femto/metrocells) [13]. Because a consequence of the inter-cell interference coordination (ICIC) efforts of Release twelve, the downlink (DL) initial signals might experience an enhancement in their resiliency against jamming.

3.2 Uplink (Low-Power) Smart Jamming

Low-power smart jamming requires a step further by concentrating on essential uplink control stations. Remember that, as depicted in Figure 4, the range of an uplink smart jamming attack is less local and covers the complete sector or cell. It is because the attacker jams UL control channels, stopping the eNodeB from acquiring essential UL signaling messages necessary for the correct procedure of the cell. By frustrating reception at the eNodeB through a jamming indication, the attacker is effectively stopping the base train station to talk to every UE in the cell, extending the range of the attack to the complete cell thus.

In addition, the attacker is not bounded by the high electricity of downlink indicators sent by the eNodeB (often in the number of 48 dBm), but by the utmost power, the best UE can transfer, which is set at 23 dBm in the entire circumstance of LTE [14]. In this full case, an attacker seated near the eNodeB transmitting at the same ability level as any legitimate smartphone may potentially jam the uplink control announcements of all UEs within confirmed cell or sector. Furthermore, the attacker might use an extremely directive antenna directed on the eNodeB and considerably enhance the efficiency of the strike.
This sort of assault has been recently confirmed in the framework of GSM systems concentrating on the uplink RACH [15].

The first meaning exchange upon this route allows the UE to synchronize in the uplink and, after the preliminary access method, radio resources can be assigned to the UE.

To be able to target a particular LTE uplink control route, the attacker would have to know the real PRBs designated to it at the PHY part. This PRB project can be acquired from available paperwork publicly. Nevertheless, as it will be shown in Subsection 4.4, if the actual location of the signals in the time-frequency LTE frame was randomized or scrambled, such radio resource assignment information could be extracted from the SIB unprotected messages carried by the PBCH and PDSCH.

In the context of a complex and highly targeted attack, one should remember that the MNC and MCC of any eNodeB are also encoded in the SIB-1 meaning. Eavesdropping of the information allows an attacker, for example, to selectively target a jamming charge against base stations from a particular cellular network operator.

Remember that uplink smart jamming, while being much far better than basic jamming or downlink smart jamming, is a far more complex attack. To be able to jam the PRBs designated to selectively, for example, the RACH route, an attacker should be synchronized in time and frequency with the LTE signal perfectly. Moreover, the attacker can capture and decode the MIB and SIB messages to be able to extract the actual RACH PRB allocation information. Therefore, an experienced attacker and average development focus on, for example, software-defined radio would be needed.

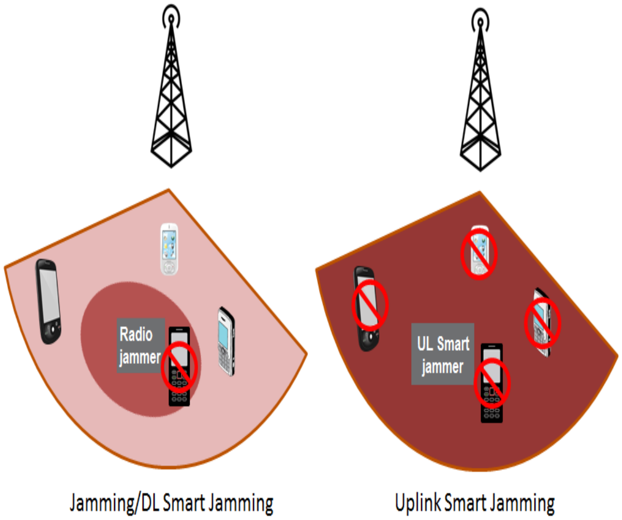

Figure 2: Impact Range of Radio Jamming Vs UL Smart Jamming

4. LTE Security Solutions against Jamming Attacks

Among the goals of the proof of strategy newspaper is to propose research guidelines to improve the resilience of LTE against smart jamming hazards. We add a couple of security research guidelines at the PHY covering of LTE sites, aiming to improve the resiliency of data marketing communications against jamming. The envisioned security system would protect communication systems by mitigating the air jamming attacks mentioned in Section 4. These alternatives would also decrease the system construction information an attacker may easily eavesdrop to be able to leverage a jamming demand or the deployment of any rogue base train station.

The proposed theoretical security system is dependent on an augmentation of the resiliency against radio jamming of the PBCH through a spread variety transmission. This is coupled with scrambling of the PRB allocation of UL control programs and a allocated encryption design for downlink control transmit messages. Similarly, the functional system shields its most susceptible resources, downlink control stations, which will be the concentrate on of DoS disorders [6]. Alternatively, MIB and SIB information are covered so an attacker cannot learn any information on the PRB allocation for the other control stations that happen to be arbitrarily allocated with time and consistency now. Only with the info encoded and encrypted in the MIB and SIB messages an attacker can try to the UL control channels with a jamming charge. Full software of such security alternatives render a jamming episode to be only as effectual as basic barrage jamming. Remember that in jamming mitigation studies, the target is accurately to power any superior jamming invasion to be equally as productive as standard jamming [12].

Note that the entire execution of the suggested techniques wouldn't normally be trivial, as it will be mentioned throughout this section. For instance, the scrambling of the PRB allocation of UL control channels will challenge the SC-FDMA scheduling in the uplink since it could potentially split up the continuity of user allocations. The successful execution of many of these alternatives would be very challenging in commercial systems. Nevertheless, such adjustments at the PHY coating could be directed for the development on the Nationwide Interoperable Consumer Safe practices Broadband Network, with a PHY covering predicated on LTE [2,3]. Such next-generation communication systems for disaster response present tight security requirements and really should be guarded against potential jamming episodes.

4.1 Spread-Spectrum Jamming Resiliency

By using jamming the central you) 08 MHz of any LTE signal, an attacker would deny the in order to all UEs in its neighbourhood. Therefore, it is important to enhance the safeguard of the key broadcast programs at the PHY part. The goal is to counteract the advantage in bandwidth and transmitted ability the jammer has for this reason LTE vulnerability [6]. Newly deployed LTE systems implement a completely remodeled modulation scheme that considerably maximizes the performance of the wireless channel in conditions of bits every second per Hertz (bps/Hz). Nevertheless , the implementation of an OFDMA-based PHY level lacks of the natural interference resilience features of code division multiple gain access to (CDMA)-based networks. While OFDMA is often the choice because of its powerful performance in challenging multipath environments, it is not necessarily optimal for scenarios where adversarial agencies intentionally make an attempt to jam sales and marketing communications, such as with tactical cases [12]. The strong interference resiliency of CDMA-based networks is well known [17, 18]. The application of a scrambling signal with a high chip rate to the transmitted signal propagates the spectrum to levels that, in some instances, can be masked by the thermal noise at the receiver. Upon response of the signal, app of the same code, orthogonal with the code used in other foundation stations or UEs, allows to recover the original signal. Due to the nature of the sent signal in UMTS, centered on W- CDMA, an interfering signal needs to be transmitted at a very high power in order to jam the communication. This is credited to the fact that the despreading the sign spectrum at the device causes, assuming an interfering signal uncorrelated with the scrambling signal, an built in reduction of the disturbance power by log10(G) sound levels (dBs), being G the spreading factor or control gain of the W-CDMA signal [17].

Looking at the characteristics of transmission channels, one could visualize an alternative transmission system where the key downlink voice broadcasting channels are protected by a spread spectrum-based method. Although downgrading from OFDMA could potentially cure the available throughput for voice broadcasting messages, such control programs are known for having very low overhead and a low throughput of, in the case of the PBCH, just three hundred and fifty bps [1].

4.2 System Description

The proposed security solution can be applied a spread spectrum- structured modulation to the downlink control channels in order to extend their array over the available BW. This could be done by just expanding the BW of the downlink broadcast signals or by applying an actual CDMA-based modulation on this section of the LTE transmission.

This solution alone would prevent a downlink playing attack to be launched with a simple r / c transmitter or jammer, which substantially increases the harm complexity and cost. To perform such attack, full synchronization over time and consistency would need in order to apply the same CDMA spreading code to the jamming signal. In case that an assailant does incur this cost, a further enhancement to this solution is defined in Subsection 4.3.

Assuming a scrambling or spreading sequence with an interest rate of Rb-G, with Rb being the rate of the PBCH messages, a jammer would theoretically require an additional log10(G) dBs of transmitted electricity in order to achieve the same result. With the transmitted power retained constant, the BW of the jamming signal would be reduced with a factor of up to G times. With both power and BW stored constant, the range of the attack would be reduced.

4.3 Limitations and Potential Implementation

The primary restriction of the perfect solution is is a finer is necessary by the UE synchronization with the DL sign. Moreover, the potency of the protection is proportional to the dispersing factor of the broadcast indication straight. Therefore, either extra BW should be allocated for the PBCH or its PRB allocation should be modified and spread over the available 1.08 MHz. Nevertheless, with a powerful throughput of just 350 bps, you can find room for improvement probably. To become implemented in commercial cellular, this system would require changes in the LTE standards. Additionally, it could not be backwards appropriate for current LTE terminals unless the PBCH and broadcasting text messages were sent both within the central subcarriers and with the get spread around spectrum augmentation. Nevertheless, this solution is possible and may be applied in the framework associated with an anti-jamming security-enhanced LTE-based armed forces or tactical world wide web- work, which would use custom cellular devices and eNodeBs.

5. Related Work

Jamming attacks are the main basic type of threat that wireless communication networks face given the fact that the threat vector exploited is inherent to the actual technology. There is no way to prevent an attacker from broadcasting high-power signals on the frequency band allocated to a commercial mobility network. The goal of this attack is often to prevent users to access communication networks, which catalogues this threat as a DoS attack. Several attacks proposed in the literature use radio jamming as a first step in order to force UEs to an insecure access network [16]. Jamming attacks have been in the scope of network and security research for several years already [11]. As new network standards arise, jamming attacks spread their threat over new technologies such as wireless sensor net- works (WSNs) [10] and WLANs [4]. Mobility networks, the main commercial wireless networks, have also been considered in radio jamming studies [9].In parallel, the potential of this kind of attack has lead to improvements and refinements, resulting in more sophisticated jamming techniques. Over the years, authors have proposed ways to launch DoS attacks against mobility net- works by overloading the system at the paging channel [19] or with a spike in core network signaling messages [20]. Some other sophisticated jamming techniques have been proposed for UMTS networks [21].The author of [15] was the first to implement an actual smart jamming attack against an UL control channel in a GSM network, opening a new simple but very effective attack vector to be leveraged in a radio jamming attack. The same idea has recently been proposed as a potential way to jam LTE networks [6].Despite the prevalence and effectiveness of jamming in the context of wireless networks, there is a clear lack of security strategies to mitigate the impact of such attacks specially in current mobility networks and upcoming LTE-based emergency response broadband systems. Current standardization bodies do not consider any jamming resiliency requirements for the next planned release of the LTE advanced standard. Nevertheless, some work has been done in addressing jamming attacks in WLANs [22] and WSNs [10].

6. Conclusions

Jamming attacks are one of the main types of security attack that mobility networks face. This threat is inherent to the actual wireless technology employed in this type of network, and in its most basic implementation (bar- rage jamming), there is no means to prevent an attacker from broadcasting a high power interfering signal on a commercial frequency band.

Despite that jamming attacks are well known and have been widely studied in the literature, no actual security and mitigation strategies have been proposed to enhance the resiliency against jamming attacks in mobility net- works. This has resulted on a constantly growing list of new proposals for sophisticated DoS attacks against cellular networks based on jamming principles. However, standardization bodies do not include any anti-jamming guidelines or requirements for the upcoming new releases of LTE advanced. Nevertheless, the forecasted application of LTE-based technologies to implement national emergency response networks makes the reliability and security requirements of LTE of paramount importance.

In this proof of concept paper, we overview a series of simple but effective jamming attacks that extend the range of basic jamming while requiring less power. Based on these new threats, classified as smart jamming, we pro- pose a series of potential security research directions that could protect LTE cellular networks, forcing a potential attacker to rely on just basic jamming to attempt a DoS charge. The goal is to raise awareness on this tradition- ally overlooked threat and spark security research work in this area. We are, in parallel, implementing smart jamming in the lab as well as some of the proposed security solutions.

A potential enhancement of the anti-jamming properties of the main DL broadcast channels, importing concepts from spread spectrum modulations, protects the wireless interface from a smart jamming attack aimed to such control channels. In parallel, a randomization of the PRB allocation of UL control channels plus a sophisticated encryption method for DL system configuration messages, backed up by the deployment of a TPM in the UE, prevent an attacker from launching a smart jamming attack against these essential UL channels. Finally, a method that leverages the current availability of antennas at the eNodeB is proposed to filter out an UL smart jamming signal in order to block an UL smart jamming attack The limitations for all these solutions have been discussed as well. Such enhancements, or similar proposals, should be considered in the scope and requirements of the upcoming releases for wireless cellular networks, specially for the Nationwide Interoperable Public Safety Broadband Net- work. Mobility networks, providing mobility services to billions of customers over the world, were never designed with a security perspective. The evolution from GSM to UMTS and finally LTE has addressed encryption and authentication issues, aiming to enhance the overall sys- tem security. The same kind of proactive approach should be taken in order to mitigate potential DoS jamming attacks against mobility networks.

References

[1] S Sesia, M Baker, I Toufik, LTE, The UMTS Long Term Evolution: From Theory to Practice. (Wiley, New York, 2009)

[2] Nationwide Public Safety Broadband Network.

US Department of Homeland Security: Office of Emergency Communications (2012). http://goo.gl/AoF41. Accessed MAY 2016

[3] T Doumi, M Dolan, S Tatesh, A Casati, G Tsirtsis, K Anchan, D Flore, LTE for public safety networks. IEEE Comm. Mag. 51(2), 106–112 (2013)

[4] W Xu, Y Zhang, T Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in ACMMOBIHOC; Urbana-Champaign (ACM New York, 2005), pp. 46–57

[5] D Talbot, One simple trick could disable a city 4G phone network. (MIT Technology Review, 2012). http://goo.gl/jROMe2.

[6] M Lichtman, JH Reed, TC Clancy, M Norton, Vulnerability of LTE to hostile interference, in Proceedings of the IEEE Global Conference on Signal and Information Processing, GlobalSIP ‘13, Austin, TX (IEEE New York, 2013), pp. 285–288

[7] When advanced persistent threats go mainstream. Emc Corporation: security for business innovation council (2011). http://www.emc.com/collateral/industry-overview/sbic-rpt.pdf.

[8] D Alperovitch, Revealed: operation shady RAT. Threat research, mcafee (2011). http://www.mcafee.com/us/resources/white-papers/wpoperation-shady-rat.pdf.

[9] M Stahlberg, Radio jamming attacks against two popular mobile networks, in Helsinki University of Technology. Seminar on Network Security.Mobile Security, (2000). Accessed MAY 2016

[10] W Xu, K Ma, W Trappe, Y Zhang, Jamming sensor networks: attack and defense strategies. IEEE Netw. 20(3), 41–47 (2006)

[11] T Basar, The Gaussian test channel with an intelligent jammer. IEEE Trans. Inform. Theor. 29, 152–157 (1983)

[12] T Clancy, Efficient OFDM denial: pilot jamming and pilot nulling, in Communications (ICC), 2011 IEEE International Conference on (IEEE New York, 2011), pp. 1–5

[13] P Bhat, S Nagata, L Campoy, I Berberana, T Derham, G Liu, X Shen, P Zong, J Yang, LTE-advanced: an operator perspective. IEEE Comm. Mag.50(2), 104–114 (2012)

[14] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception. 3GPP TS 36.101 vol. fv10.3.0 (2011)

[15] D Spaar, A practical DoS attack to the GSM network, in In DeepSec, (2009). http://tinyurl.com/7vtdoj5.

[16] K Nohl, S Munaut, Wideband GSM sniffing. In 27th Chaos Communication Congress (2010). http://goo.gl/wT5tz.

[17] J Pérez-Romero, O Sallent, Agustí R, MA Diaz-Guerra, Radio Resource Management Strategies in UMTS. (John Wiley & Sons, New York, 2005). http://books.google.com/books?id=581gFV8abl4C.

[18] AJ Viterbi, CDMA: Principles of Spread Spectrum Communication, Volume 129. (Addison-Wesley Boston, MA, 1995)

[19] J Serror J, Impact of paging channel overloads or attacks on a cellular network, in Proceedings of the ACM Workshop on Wireless Security (WiSe) (IEEE New York, 2006), pp. 1289–1297

[20] P Lee, T Bu, T Woo, On the detection of signaling DoS attacks on 3G wireless networks, in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, (2007) [21]. G Kambourakis, C Kolias, S Gritzalis, J Park, DoS attacks exploiting signaling in UMTS and IMS. Comput. Commun. 34(3), 226–235 (2011)

[21] S Khattab, D Mosse, R Melhem, Jamming mitigation in multi-radio wireless networks: reactive or proactive?, in Proceedings of the 4th International Conference on Security and Privacy In Communication Netowrks, SecureComm ‘08 (ACM New York, 2008), pp. 27:1–27:10