EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

Enhancing the security of LTE networks against jamming attacks

Roger Piqueras Jover[1*], Joshua Lackey[1] and Arvind Raghavan[2]

Abstract

The long-term evolution (LTE) is the newly adopted technology to offer enhanced capacity and coverage for current mobility networks, which experience a constant traffic increase and skyrocketing bandwidth demands. This new cellular communication system, built upon a redesigned physical layer and based on an orthogonal frequency division multiple access (OFDMA) modulation, features robust performance in challenging multipath environments and substantially improves the performance of the wireless channel in terms of bits per second per Hertz (bps/Hz). Nevertheless, as all wireless systems, LTE is vulnerable to radio jamming attacks. Such threats have security implications especially in the case of next-generation emergency response communication systems based on LTE technologies. This proof of concept paper overviews a series of new effective attacks (smart jamming) that extend the range and effectiveness of basic radio jamming. Based on these new threats, a series of new potential security research directions are introduced, aiming to enhance the resiliency of LTE networks against such attacks. A spread-spectrum modulation of the main downlink broadcast channels is combined with a scrambling of the radio resource allocation of the uplink control channels and an advanced system information message encryption scheme. Despite the challenging implementation on commercial networks, which would require inclusion of these solutions in future releases of the LTE standard, the security solutions could strongly enhance the security of LTE-based national emergency response communication systems.

Keywords: LTE; Jamming; Security; OFDMA

1 Introduction

As mobile phones steadily become more powerful and bandwidth demands skyrocket, cellular operators are rapidly deploying broadband data services and infrastructure to enhance capacity. The long-term evolution (LTE) is the recently deployed standard technology for communication networks, offering higher data speeds and improved bandwidth. This new cellular communication system is the natural evolution of 3rd Generation Partnership Project (3GPP)-based access networks, enhancing the Universal Mobile Telecommunications System (UMTS).

LTE provides capacity to user equipments (UEs) by means of a centralized assignment of radio resources. A newly enhanced physical (PHY) layer is implemented based on orthogonal frequency division multiple access (OFDMA) and substantially improves the performance of the former wideband code division multiple access (W-CDMA) [1]. The new modulation scheme provides a large capacity and throughput, potentially reaching a raw bit rate of 300 Mbps in the downlink with advanced multiple input multiple output (MIMO) configurations [1].

Due to its spectrum efficiency and great capacity, LTE is planned to be adopted as the basis for the next-generation emergency response communication system, the Nationwide Interoperable Public Safety Broadband Network [2]. In this context, the characteristics of such LTE-based public safety networks are already under consideration in the industry [3]. Note that, specially in the case of this application, the security requirements of LTE communication networks are of paramount importance.

Despite the tremendous capacity and system enhancements implemented by LTE, cellular networks are known to be, as any kind of wireless network, vulnerable to radio jamming. Although it is a simple and well-known attack, radio jamming is the most common way to launch

*Correspondence: roger.jover@att.com
[1] AT&T Security Research Center, New York, NY 10007, USA
Full list of author information is available at the end of the article

a localized denial of service (DoS) attack against a cellular network [4]. The impact of such attacks is very local and mainly constrained by the transmitted power of the jamming device. The attacker is only able to deny the service locally to UEs located in its vicinity. However, more sophisticated attacks have been discovered as a potentially more effective way to jam LTE networks [5,6]. These smart jamming attacks aim to saturate specifically the main downlink broadcast channel of LTE networks in order to launch a local DoS attack that requires less power, making it stealthier. Further complex attacks, such as low-power smart jamming, identify the actual physical resource blocks (PRBs) assigned to essential uplink control channels by capturing the unprotected broadcast messages sent from the base station (eNodeB). The interception of such unencrypted network configuration data allows the attacker to selectively saturate uplink control channels in order to extend the range of the attack to an entire cell or sector. Note that network configuration contained in the broadcast channel can also be leveraged to deploy an effective rogue base station and other kinds of attacks.

Although radio jamming attacks have a rather local range, they become highly relevant in the current cybersecurity scenario. Reports of very targeted and extremely sophisticated 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 goal of stealing intellectual property or other valuable digital assets [8]. The advent of APTs has substantially changed the set of assumptions in the current threat scenario. When it comes to very well-planned and funded cyber attacks, the scale of the threat is not important anymore. Instead, achieving a very specific and localized goal for economic benefit or military advantage is the key element. In this context, scenarios such as a local DoS attack against the cell service around, for example, a large corporation's headquarters or the New York Stock Exchange becomes very relevant. DoS is also often a tool used to knock a phone off a secure network and force it down to an insecure radio access network (RAN) to pursue further attacks and data exfiltrations [9].

The goal of this proof of concept paper is to raise awareness on the traditionally overlooked threat of radio jamming and to propose a combination of potential research directions and LTE RAN enhancements against sophisticated jamming attacks. This theoretical enhanced security architecture relies on a boost of the jamming resiliency of the main downlink broadcast channels and the encryption of the data broadcasted in it. The potential results would be twofold. On one hand, an attacker would not be able to easily jam the downlink broadcast channels and, therefore, deny the service to UEs in its vicinity. On the other hand, no network configuration information could be intercepted and decoded, preventing an attacker to gain knowledge on each cell's specific configuration, which could be leveraged in security attacks. Finally, a proactive smart jamming multi-antenna cancelation technique is presented.

Some of the proposed security solutions involve substantial changes at the PHY layer of LTE networks which could be very challenging to implement on a commercial network and would require collaboration within the industry. Nevertheless, such security architecture could substantially increase the reliability and resiliency against security attacks of the Nationwide Interoperable Public Safety Broadband Network [2]. Anti-jamming enhancements could be included to the list of requirements for LTE-based public safety networks that are not in the scope of current releases of the LTE standard, such as direct communication and group communication [3].

The remainder of the paper is organized as follows. Section 2 briefly overviews the cell selection procedure in LTE networks, the main downlink broadcast channels, and the feasibility of eavesdropping unprotected broadcasted network configuration messages. Three attacks against LTE networks are described in Section 3. The proposed research directions and theoretical architecture to mitigate radio jamming attacks is introduced in Section 4. Finally, related work is reviewed in Section 5, and the concluding remarks are presented in Section 6.

2 Initial access to LTE networks

This section overviews the basic procedures necessary for a phone to synchronize with and connect to an LTE network. Any UE willing to access the network must first perform a cell selection procedure. After this procedure, the UE decodes the physical broadcast channel (PBCH) to extract the basic system information that allows the other channels in the cell to be configured and operated. The messages carried on this channels are unencrypted and can be eavesdropped by a passive radio sniffer. Once at this point, the UE can initiate an actual connection with the network by means of a random access procedure and establish a radio access bearer (RAB) in order to send and receive user traffic. The whole process is portrayed in Figure 1.

2.1 Cell search procedure

The cell search procedure consists of a series of synchronization steps that allow the UE to determine time and frequency parameters required to detect and demodulate downlink signals as well as to transmit uplink signals with the right timing. The three major steps in this procedure are symbol timing acquisition, carrier frequency synchronization, and sampling clock synchronization. To achieve full synchronization, the UE detects and decodes the

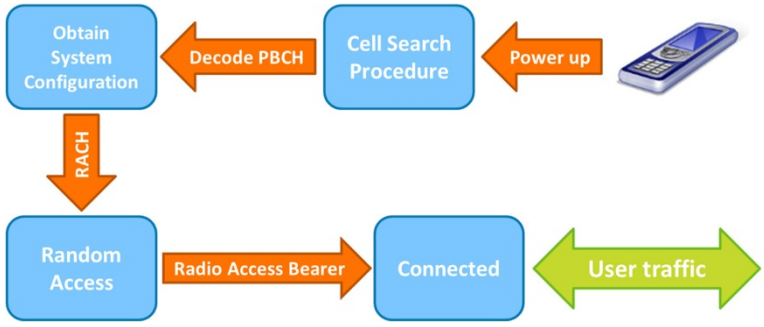

Figure 1 LTE initial access.

primary synchronization signal (PSS) and the secondary synchronization signal (SSS), which are fully described in [10]. The mapping of the PSS and SSS in the central subcarriers of the LTE frame as well as the main functions of these synchronization signals is shown in Figure 2.

The PSS enables the UE to acquire the time slot boundary independently from the cyclic prefix configuration of the cell, which at this point is unknown to the UE. Based on the downlink frame structure, the PSS is transmitted twice per radio frame. This enables the UE to get time synchronized on a 5-ms basis, which simplifies the required inter-frequency and inter-RAT measurements. The PSS is transmitted occupying the six central PRBs of the LTE frequency configuration [11]. With 12 subcarriers per PRB, this results in 1.08 MHz of bandwidth (BW). This way, independently of the BW configuration of the cell, the UE is able to decode it.

The next step is to obtain the radio frame timing and the group identity of the cell, which is found in the SSS. In the time domain, the SSS is transmitted in the preceding symbol to the PSS. The SSS also has a 5-ms periodicity and occupies 62 of the 72 central subcarriers so it can be decoded without knowledge of the system BW configuration.

Decoding this signal, the device determines the unique identity of the cell. At this point, the terminal can get fully synchronized with the eNodeB because the reference signals are transmitted in well-defined resource elements and the current synchronization allows locating them. A reference symbol from the generated reference signal pattern is transmitted on every sixth subcarrier. In the time domain, every fourth OFDM symbol holds a reference symbol. This results on four reference symbols per PRB.

2.2 LTE physical broadcast channel

The LTE PBCH is crucial for the successful operation of the LTE radio interface. Therefore, its transmission has to be optimized so it can be reliably decoded by cell edge users with low latency and low impact on battery life.

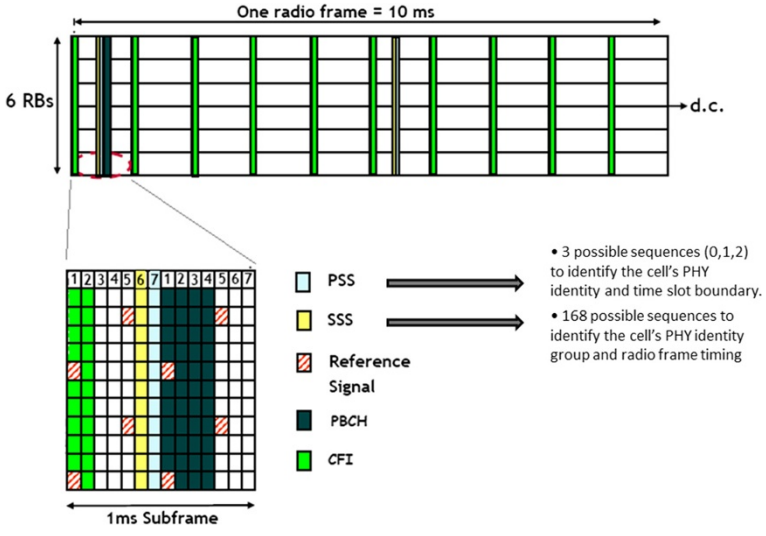

Figure 2 Primary and secondary synchronization signals mapping and main functions.

This is achieved by means of low system overhead (the effective data rate is of just 350 bps) and transmission with the lowest modulation and coding scheme (MCS) in order to minimize the bit error rate (BER) for a given signal-to-noise ratio (SNR) [1].

The main LTE system information is transmitted over the PBCH within the master information block (MIB). This message contains the most frequently transmitted parameters, essential for an initial access to the cell, such as the system BW, the physical hybrid ARQ indicator channel (PHICH) structure and the most significant eight bits of the system frame number (SFN).

The remainder of the system configuration is encoded in the system information blocks (SIBs), which are modulated on the physical downlink shared channel (PDSCH). These messages can be mapped on the PDSCH based on their broadcast id, the system information RAN temporary identifier (SI-RNTI), which is fixed in the specifications and therefore known *a priori* to all UEs and potential attackers. The SIB-1 message contains transport parameters necessary to connect to the cell as well as scheduling information, and the SIB-2 message contains information on all common and shared channels. Subsequent SIB messages define multiple parameters, such as the power thresholds for cell re-selection and the list of neighboring cells.

2.3 MIB and SIB message eavesdropping

The MIB and SIB messages are broadcasted on PRBs known *a priori* and transmitted with no encryption. Therefore, a passive sniffer is able to decode them. This simplifies the initial access procedure for the UEs but could be potentially leveraged by an attacker to craft sophisticated jamming attacks, optimize the configuration of a rogue base station or tune other types of sophisticated attacks. Figure 3a,b presents our lab system configuration eavesdropped with a commercial of-the-shelf LTE wireless traffic sniffer. Note that details such as the system BW, the cell identity, and the MCC and the mobile network code (MNC) of the eNodeB are broadcasted in the clear. These values have been faded out on purpose in the figures.

Similarly, using the same commercial traffic sniffer, the subsequent SIB messages can be intercepted. For example, the SIB-2 messages contains the PRB mapping of other control channels, such as the uplink (UL) resources reserved for the UE random access procedure on the random access channel (RACH).

Note that a commercial traffic sniffer is not necessary to obtain this information. A skilled programmer could design a PBCH traffic sniffer implemented on a cheap software-defined radio (SDR) platform such as the universal software radio peripheral (USRP) [12], which is commonly used as radio transceiver in GSM (Global System of Mobile Communications) open source projects [13].

Figure 3 MIB (a) and SIB-1 (b) LTE messages eavesdropped with a commercial traffic sniffer.

3 Attacks against cellular networks

Radio jamming is the deliberate transmission of radio signals to disrupt communications by decreasing the SNR of the received signal. This attack essentially consists of blasting a high-power constant signal over the entire target band of the system under attack [4,14].

This attack is broadly known as a simple and common way to attack a wireless network and has been widely studied in the literature in the context of wireless local area networks (WLAN) [4], sensor networks [15], and cellular networks [14]. Despite the attack's simplicity, often, the only solution is to locate and neutralize the attacker, specially in the situation where the entire band of the system is being jammed. The very large amount of transmitted power, though, results in a reduced stealthiness so more

elaborated schemes to jam cellular networks are being proposed in the literature.

It has been shown that a standard barrage jamming attack is the optimal jamming strategy when the attacker has no knowledge of the target signal [16]. This section overviews specific derivations of radio jamming attacks against cellular networks based on the knowledge of the target LTE signal that an attacker can obtain from publicly available documents and standards. A popular new threat vector that can be exploited as a result of such attacks is also described.

3.1 Downlink smart jamming

Downlink smart jamming consists of generating malicious radio signals in order to interfere with the reception of essential downlink control channels. A recent report introduces the potential theoretical results of jamming the PBCH of LTE networks [5]. The authors of the original study expanded the details of this study in a recent paper [6]. This attack, which could be applied to both 2G and 3G networks as well, targets this channel because, as described in Section 2.1, its assigned PRBs are known *a priori* and always mapped to the central 72 subcarriers of the OFDMA signal. Given that this channel is required to configure and operate the other channels in the cell, 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 fairly high-power interfering signal to deny the service to noncell edge users. Note that, in order to outpower the legitimate signal, the attacker is bounded by the large transmitted power at the eNodeB and the potentially low transmitted power of the jamming device.

More sophisticated versions of this attack have been proposed, targeting the downlink pilot signals used by the UE to estimate the channel for signal equalization [17]. However, Release 10 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) [18]. As a consequence of the inter-cell interference coordination (ICIC) efforts of Release 10, the downlink (DL) pilot signals might experience an enhancement in their resiliency against jamming.

3.2 Uplink (low-power) smart jamming

Low-power smart jamming takes a step further by targeting essential uplink control channels. Note that, as depicted in Figure 4, the range of an uplink smart jamming attack is less local and covers the entire cell or sector. This is because the attacker jams UL control channels, preventing the eNodeB from receiving essential UL signaling messages required for the correct operation of the cell. By overwhelming reception at the eNodeB by means of a jamming signal, the attacker is effectively preventing the base station to communicate with every UE in the cell, thus extending the range of the attack to the entire cell.

Moreover, the attacker is not bounded by the high power of downlink signals transmitted by the eNodeB (often in the range of 48 dBm), but by the maximum power, a legitimate UE can transmit, which is fixed at 23 dBm in the case of LTE [19]. In this case, an attacker sitting in the vicinity of the eNodeB transmitting at the same power level as any legitimate smartphone could potentially jam the uplink control messages of all the UEs within a given cell or sector. Furthermore, the attacker could use a very directive antenna pointed towards the eNodeB and substantially enhance the effectiveness of the attack.

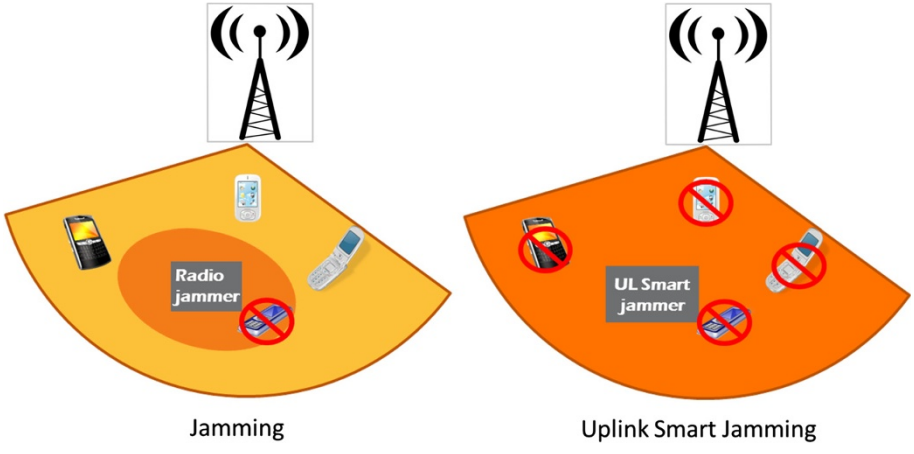

Figure 4 Impact range of radio jamming vs UL smart jamming.

This type of attack has been previously demonstrated in the context of GSM networks targeting the uplink RACH [20].

The first message exchange on this channel allows the UE to synchronize in the uplink and, after the initial access procedure, radio resources can be allocated to the UE.

In order to target a specific LTE uplink control channel, the attacker would need to know the actual PRBs assigned to it at the PHY layer. This PRB assignment can be obtained from publicly available documentation. Nevertheless, as it will be presented in Subsection 4.4, if the actual location of this signals in the time-frequency LTE frame was randomized or scrambled, such radio resource assignment information could still be obtained from the SIB unprotected messages carried by the PBCH and PDSCH.

In the context of a sophisticated and highly targeted attack, one should note that the MCC and MNC of an eNodeB are also encoded in the SIB-1 message. Eavesdropping of this information would allow an attacker, for example, to selectively target a jamming charge against base stations from a specific cellular network operator.

Note that uplink smart jamming, while being much more effective than basic jamming or downlink smart jamming, is a more complex attack. In order to selectively jam the PRBs assigned to, for example, the RACH channel, an attacker should be perfectly synchronized in time and frequency with the LTE signal. Moreover, the attacker should be able to capture and decode the MIB and SIB messages in order to extract the actual RACH PRB allocation information. Therefore, a skilled attacker and moderate development work on, for example, software-defined radio would be required.

3.2.1 LTE link budget

To illustrate the gain in transmitted power and, therefore, range of uplink smart jamming, we compute the link budget for a typical 10 MHz LTE system in both the uplink and downlink. The main parameters of this LTE configuration are described in Table 1. Such calculations can be done with multiple open access tools available online such as [21].

Given an eNodeB transmitting at the standard power (48 dBm), the received power at a UE located at the edge of a cell is of −100.80 dBm for the largest possible cell with radius 0.4 Km (i.e., −100.80 dBm is the receiver sensitivity in the DL). Although the maximum size of the cell is limited by the UL link, for the sake of comparison, we compute the received power at the eNodeB from a UE located at the cell edge, 0.4 km away from the UL receiver. This link budget results in −132.26 dBm received at the eNodeB. This difference of 31.46 dB between the received power in the UL and DL indicates that the power the eNodeB receives from a UE at the cell edge is 1,000 times lower than the power that the same UE at the cell edge receives from the eNodeB in the dowlink. This gives a clear indication on the much lower jamming signal power requirements for an UL smart jamming strategy.

Table 1 LTE link budget parameters from a standard 10 MHz deployment

System parameters	Values
System BW	10 MHz
Subchannel reuse	One-three
Carrier frequency	2.5 GHz
#TX antennas	2
#RX antennas	2
Path loss model	Cost 231
BS antenna height	30 m
UE antenna height	1.5 m
MCS	QPSK 1/2
SNR_{min} for MCS	8.5 dB [22]
Thermal noise density	-174 dBm/Hz
Log-normal fading margin	6 dB
Downlink	
eNodeB max power	43 dBm
Multi-antenna gain	3 dB
TX antenna gain	17 dBi
Noise figure	4 dB
Uplink	
UE max power	23 dBm
Multi-antenna gain	0 dBm
TX antenna gain	-1 dBm
Noise figure	9 dB

3.2.2 Attack complexity

Based on the characteristics of UL smart jamming, the attacker would require full synchronization in time and frequency with the LTE signal to be able to, for example, selectively jam the RACH. This raises the complexity of the attack as compared to DL smart jamming. Nevertheless, there are numerous of-the-shelf and open access tools that could be leveraged in this context.

The USRP is commonly used for GSM-related projects, but there are certain ongoing open source projects that could be used to write software radio applications that synchronize with an LTE signal. One example is the openLTE project [23]. Leveraging these tools, a skilled attacker could potentially implement an advanced jammer at a very low cost. Moreover, there are other off-the-shelf applications and tools that allow a user to synchronize with an LTE signal such as specialized LTE sniffing hardware and commercial software-based LTE base stations.

3.3 Rogue base station attacks

Rogue base station attacks have been proposed in the literature as a means to, for example, steal credentials or invade the privacy of mobile users [9,24]. These attacks are based on the deployment of a GSM rogue base station combined with jamming the UMTS and/or LTE network in order to force as many UEs as possible to camp on the fake GSM cell. Many security features of GSM have been defeated over the last few years [25]. Given that the authentication algorithm is not symmetric, the network is not required to authenticate, so the UE believes it is connected to a real base station.

An efficient technique to maximize the potential number of devices camping on the fake cell is by advertising the id of the rogue base station based on the list of neighboring cells broadcasted by legitimate base stations. Note that such information can be extracted from the unprotected downlink broadcast MIB and SIB messages. From the data sniffed from such broadcast messages, one can efficiently tune the transmitted power of the rogue cell as well such that the UEs will handoff to the rogue base station.

Note that both techniques leveraged to optimize a rogue base station attack (jamming of the LTE network and obtaining information from the unencrypted MIB and SIB messages) leverage the vulnerabilities introduced in Section 2.

4 LTE security solutions against jamming attacks

One of the goals of this proof of concept paper is to propose research directions to enhance the resilience of LTE against smart jamming threats. We introduce a set of security research directions at the PHY layer of LTE networks, aiming to enhance the resiliency of data communications against jamming. The envisioned security system would protect communication systems by mitigating the radio jamming attacks discussed in Section 3. These solutions would also minimize the system configuration information that an attacker can easily eavesdrop in order to leverage a jamming charge or the deployment of a rogue base station.

The proposed theoretical security system is based on an enhancement of the resiliency against radio jamming of the PBCH by means of a spread spectrum transmission. This can be combined with scrambling of the PRB allocation of UL control channels and a distributed encryption scheme for downlink control broadcast messages. On one hand, the system protects its most vulnerable resources, downlink control channels, which are the target of DoS attacks [6]. On the other hand, MIB and SIB messages are protected so an attacker cannot learn any information on the PRB allocation for the other control channels, which are now randomly allocated in time and frequency. Only with the information encoded and encrypted in the MIB and SIB messages an attacker would be able to aim to the UL control channels with a jamming charge. Full application of such security solutions render a jamming attack to be only as effective as basic barrage jamming. Note that in jamming mitigation studies, the goal is precisely to force any sophisticated jamming attack to be just as efficient as standard jamming [17].

Note that the full implementation of the proposed techniques would not be trivial, as it will be discussed throughout this section. For example, the scrambling of the PRB allocation of UL control channels will challenge the SC-FDMA scheduling in the uplink because it could potentially break up the continuity of user allocations. The successful implementation of some of these solutions would be very challenging in commercial networks. Nevertheless, such modifications at the PHY layer could be aimed for the development on the Nationwide Interoperable Public Safety Broadband Network, with a PHY layer based on LTE [2,3]. Such next-generation communication systems for emergency response present strict security requirements and should be protected against potential jamming attacks.

4.1 Spread-spectrum jamming resiliency

By means of jamming the central 1.08 MHz of any LTE signal, an attacker would deny the service to all UEs in its vicinity. Therefore, it is important to enhance the protection of the main broadcast channels at the PHY layer. The goal is to counteract the advantage in bandwidth and transmitted power the jammer has due to this LTE vulnerability [6].

Newly deployed LTE networks implement a completely redesigned modulation scheme that substantially maximizes the performance of the wireless channel in terms of bits per second per Hertz (bps/Hz). However, the implementation of an OFDMA-based PHY layer lacks of the inherent interference resilience features of code division multiple access (CDMA)-based networks. While OFDMA is often the choice because of its robust performance in challenging multipath environments, it is not optimal for scenarios where adversarial entities intentionally attempt to jam communications, such as in tactical scenarios [17].

The strong interference resiliency of CDMA-based networks is well known [26,27]. The application of a scrambling signal with a high chip rate to the transmitted signal spreads the spectrum to levels that, in some cases, can be masked by the thermal noise at the receiver. Upon reception of the signal, application of the same code, orthogonal with the code used in other base stations or UEs, allows to recover the original signal. Due to the nature of the transmitted signal in UMTS, based on W-CDMA, an interfering signal needs to be transmitted at a very high power in order to jam the communication. This is due to the fact that the process of despreading the signal spectrum at the receiver causes, assuming an

interfering signal uncorrelated with the scrambling signal, an inherent reduction of the interference power by $\log_{10}(G)$ decibels (dBs), being G the spreading factor or processing gain of the W-CDMA signal [26].

Considering the characteristics of broadcast channels, one could envision an alternative transmission scheme where the main downlink broadcast channels are protected by a spread spectrum-based method. Although downgrading from OFDMA could potentially decrease the available throughput for broadcast messages, such control channels are known for having very low overhead and a low throughput of, in the case of the PBCH, just 350 bps [1].

4.1.1 System description

The proposed security solution applies a spread spectrum-based modulation to the downlink control channels in order to extend their spectrum 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 portion of the LTE signal.

This solution by itself would prevent a downlink jamming attack to be launched with a simple radio transmitter or jammer, which substantially increases the attack complexity and cost. To perform such attack, full synchronization in time and frequency would be required in order to apply the same CDMA spreading code to the jamming signal. In the case that an attacker does incur this cost, a further enhancement to this solution is described in Subsection 4.3.

Assuming a scrambling or spreading sequence with a rate of $R_b \cdot G$, with R_b being the rate of the PBCH messages, a jammer would theoretically require an extra $\log_{10}(G)$ dBs of transmitted power in order to achieve the same result. With the transmitted power kept constant, the BW of the jamming signal would be reduced by a factor of up to G times. With both power and BW kept constant, the range of the attack would be reduced.

4.1.2 Limitations and potential implementation

The main limitation of the solution is that the UE requires a finer synchronization with the DL signal. In addition to that, the effectiveness of the defense is directly proportional to the spreading factor of the broadcast signal. 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 an effective throughput of just 350 bps, there is potentially room for improvement.

In order to be implemented in commercial cellular, this technique would require changes in the LTE standards. Moreover, it would not be backwards compatible with current LTE terminals unless the PBCH and broadcasting messages were transmitted both within the central subcarriers and with the spread spectrum enhancement. Nevertheless, this solution is feasible and could be implemented in the context of an anti-jamming security-enhanced LTE-based military or tactical network, which would use custom wireless devices and eNodeBs.

4.2 LTE, MIB, and SIB message encryption

As introduced in Subsection 2.2, the MIB and SIB messages broadcasted by an eNodeB contain essential network configuration parameters that aid the UE to synchronize and establish a connection with the network. Nevertheless, all these messages are transmitted in the clear with obvious security implications.

Assuming a hypothetical scenario with control broadcast messages encrypted but no specific protection for the PSS and SSS, an attacker could not obtain any configuration information by means of a commercial traffic sniffer. A skilled attacker could still synchronize with the network by means of a SDR platform. Extraction of network configuration information, though, would be impossible, assuming a strong encryption scheme. Therefore, the only way an attacker could obtain the network configuration details would be by using a legitimate wireless device and hijacking it to extract data from the baseband chip, which is unreachable from the user space.

4.2.1 Initial limitations

A simple encryption scheme cannot be applied to the system information messages. If the information in the PBCH was encrypted with a secret key, the mobile terminal must know that key *a priori*. Assuming the case of a mobile terminal being turned on or roaming to a new network, the device must still be able to decode the PBCH to establish a connection. In parallel, key exchange algorithms cannot be executed with the network at this stage because the device is not connected and authenticated yet. Therefore, the key that encodes the MIB and SIBs must be hard-coded in the UE.

Relying on one common key for all users and cells is not possible either. If this key was compromised by any means, the whole system would be useless. Therefore, the system must be able to operate with a large number of different keys or able to generate a large number of keys.

4.2.2 Assumptions

The main assumption for this security architecture is a global collaboration of all mobile operators. Subscriber identity module (SIM)-based authentication schemes allow to provide cellular services to a mobile terminal independently of the network being roamed (assuming, of course, that the user has roaming activated and the phone and network are compatible). Encryption of the MIB and SIB messages would require a similar collaboration among carriers.

It is important to note that, in the case of such encryption scheme being applied exclusively to a national LTE-based emergency response broadband network, such as the Nationwide Interoperable Public Safety Broadband Network, this limitation does not apply.

The proposed solution assumes that the UE is equipped with a trusted hardware (HW) platform which is secure and able to both securely store data and perform cryptographic operations. Note that all UEs are already provisioned with such element, the SIM card. Basing the encryption scheme on the SIM, though, could potentially allow an attacker to capture LTE wireless traffic and decode it afterwards with a legitimate SIM on a standard card reader connected to a personal computer. Therefore, such encryption scheme would only be effective if it was implemented on a protected trusted platform module (TPM) that can be only operated by, for example, the baseband of a cell phone. Note that there are initial plans in the industry to equip UEs with a TPM [28]. In the context of a national emergency response network, equipping mobile devices with a secure TPM is feasible. Finally, a strong private key encryption scheme is assumed.

4.2.3 System description

The proposed solution is depicted in Figure 5. On the network side, either each base station or a node in the EPC stores a set of N secret keys in a secure location. In the case of storing the keys in a centralized way, this secure storage could be the home subscriber server (HSS) or any other newly implemented network node. On the other hand, the TPM (or SIM card) in each mobile phone stores securely the same set of N keys. The value of N can be arbitrarily large.

Note that, in practice, only one secret key K would be required. Based on this initial secret key, each sub-key K_j $j = 1, ..., N$ would be generated as $K_j = H(K|j)$, being H a hash function and '|' the concatenation operation. Assuming a robust hash function, eventual leakage of a sub-key K_j would not provide an attacker any information on the actual secret key K. However, leakage of the main secret key K would relent this method useless.

The operation of the system is described as follows. The eNodeB selects a key K_j with id j. The broadcast MIB and SIB messages are encrypted with the key K_j and transmitted over the air. Along with the encryption of the broadcast message, for example $\text{enc}_{Kj}(\text{MIB})$, the system transmits the id j in plain text. This way, any UE knows what key to use to decrypt the messages. Note that an attacker would learn the id j but would not be able to know the key K_j that is being used to encrypt the broadcast messages.

If at any point a key was compromised, the network would be able to switch to a different key K_i and continue operating normally. A broadcast message would be sent to the mobile devices to alert them of this change. Incoming connections, either via handovers from other cells or new devices being turned on, would just receive the updated broadcast messages $[\, i|\text{enc}_{Ki}(\text{MIB})]$ and continue operating normally.

Note that the network could choose to use a different key at each cell/sector. This way, if an attacker managed to compromise a key, a potential attack during the time it would take the network to change to a new key would be localized and only impact one cell or sector.

In this section, the MIB message is used as example, but the same scheme could be applied to SIB messages as well.

4.2.4 Limitations and potential implementation

The main limitations for this security enhancement of LTE networks is the requirement for a global partnership of both cellular operators, device manufacturers (in the case of the deployment of a TPM), and SIM card providers. Moreover, a substantial editing of the standards would be necessary. Therefore, such a security solution, when

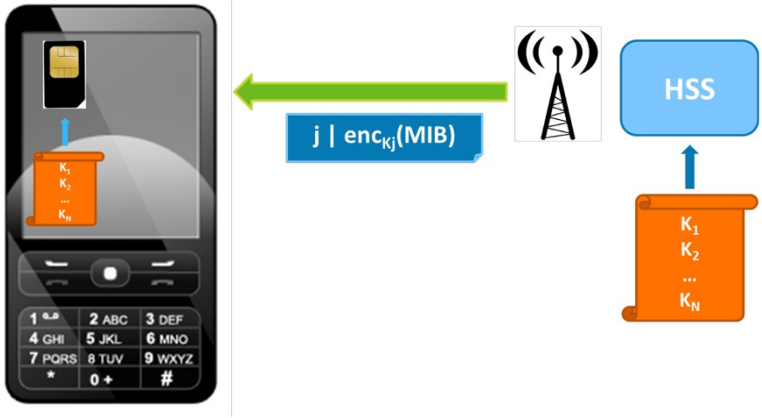

Figure 5 LTE MIB message encryption.

framed in the context of commercial wireless networks, would be more appropriate for the upcoming fifth generation of mobile networks, the standards of which are just being started.

In the context of high security demanding LTE-based communications, such as military networks or first responders, the encryption of broadcast messages is more feasible. Based on custom hardware equipped with state-of-the-art TPM and encryption schemes, such a system could be deployed.

It is important to note that, by itself, the encryption of the broadcast messages would not prevent an attack from jamming the LTE central subcarriers (downlink smart jamming) and block users from detecting and decoding the PSS and SSS and, therefore, connect to the cell.

4.3 Spread-spectrum and encryption combination

As introduced in Subsection 4.1, if an attacker obtained the sequence used to protect the central subcarriers of the LTE signal, the spread spectrum anti-jamming solution would be useless against a skilled attacker using a fully synchronized jamming device. In this section, we introduce an enhancement of the spread spectrum protection based on the encryption scheme described in Subsection 4.2.

4.3.1 Assumptions

In order to prevent an attacker from encoding the jamming signal with the right sequence and, therefore, bypass the protection, this spreading sequence must be only known by the UEs and the eNodeB. In parallel, the entire system cannot depend on a single spreading sequence because, if it was compromised, the protection would be bypassed. Therefore, the spreading sequence selection can be implemented as follows.

4.3.2 System description

The proposed enhanced security architecture is depicted on Figure 6. On the network side, either each eNodeB or the HSS stores a set of M secret spreading sequences. The value of M can be arbitrarily large. The eNodeB selects a sequence S_i with id i and scrambles the PBCH signal with it prior to broadcasting it. Along with the scrambled signal $\text{PBCH}(t) \cdot S_i(t)$, the eNodeB broadcasts the id i, either on the same channel or on a separate resource. This allows the UE to despread the PBCH with the right sequence. An attacker would just learn the id i but would not be able to extract the sequence C_i used to protect the DL signal.

Note that, when enhancing the resiliency against jamming of the MIB messages following this scheme, the sequence $S_i(t)$ used to scramble the signal can be seen as the equivalent of the key k_i used to encrypt the MIB.

4.3.3 Limitations and potential implementation

With the combination of the MIB and SIB message encryption and the spread spectrum protection against jamming, an attacker cannot leverage the knowledge of the id i, broadcasted in the clear, to optimize the attack. However, if the attacker was able to jam the actual broadcast transmission of the id i, the wireless system would be inoperative as no legitimate user would be able to determine what spreading code is being used in a given cell.

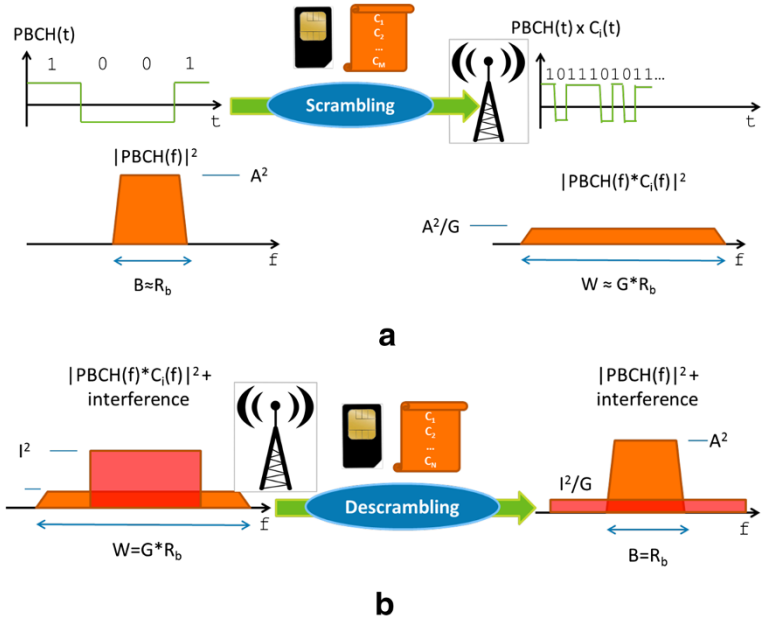

Figure 6 CDMA-based protection of the PBCH: scrambling (a) and descrambling (b).

This could be prevented in different ways. In the case of LTE-based systems with a specific application, such as military ad-hoc networks or first responder wireless systems, the id i could be distributed through an out of band secondary channel or known a priori before deploying the ad-hoc network. Alternatively, the id i could be broadcasted in a more complex yet secure manner, such as the primary scrambling code detection in UMTS networks [26]. In this case, a receiver detects which one of the 512 possible primary scramble codes is being used within a cell by applying a correlation receiver. The necessary signals for the primary scrambling code detection are often transmitted in a way that they can be received and decoded at a low SNR regime. A similar procedure could be implemented to, for example, broadcast which one of 512 possible sequences C_i with $i = \{1, 2, ..., 511\}$ is being used.

Finally, the sequence id could be broadcasted repeatedly in a frequency hopping scheme over the entire system bandwidth. Although this would require substantial changes to the LTE standards, it would force an attacker to jam the entire band to jam the id broadcasting operation. Therefore, the goal of counteracting the advantage a jammer has in LTE networks would be achieved as the only feasible option would be barrage jamming.

4.4 LTE UL control channel PRB scrambling

The PRB allocation of the Physical Uplink Control Channel (PUCCH) is known a priori as defined by the standards. The UL control signaling on this channel is transmitted in a frequency region on the edges of the system BW. In parallel, the PRB allocation of other essential UL control channels, such as the RACH, can be extracted from the SIB messages.

4.4.1 System description

The proposed security architecture scrambles the PRB allocation of UL control channels so they cannot be the target of an uplink smart jamming attack. Based on the encryption scheme described in Section 4.2, a legitimate UE would be able to decode the system configuration and normally operate on the UL control channels. An attacker, though, would not be able to locate any UL control channel and its best UL jamming strategy would be equivalent to a basic barrage jamming.

4.4.2 Limitations and potential implementation

Periodically modifying the PRB allocation of certain UL control channels, such as the RACH, would not be challenging given the multiple possible configurations of the RACH in current LTE networks. However, the allocation of the PUCCH away from the edges of the spectrum would generate new limitations. The frequency diversity achieved through frequency hoping would not be maximized anymore. In parallel, the maximum achievable PUSCH data rate would decrease due to the fact that uplink allocations must be contiguous in frequency to maintain the single-carrier nature of the uplink LTE signal [1]. Random allocation of the UL control channels could potentially pose a challenge to SC-FDMA scheduling because it could break up the continuity of user allocations.

In this case, the implementation of this security solution would require changes in the LTE standards. However, a potential application for security-demanding military and first responder LTE-based networks could be implemented using nonstandard hardware on both transmitting and receiving sides.

4.5 Selective uplink smart jamming interference cancelation

In order to enhance their coverage range and apply diversity techniques, cell towers are equipped with multiple antennas. The number of antennas at the cell tower is commonly three but some network operators are pushing this number to five in LTE networks to expand further the system's capacity [29]. The cell range in the DL is often bounded by the base station's transmitted power, which is significantly higher than that of a UE. Therefore, the multiple antennas implement spatial diversity in the UL to extend the cell's range limited by the UE.

The proposed security architecture includes a further application that exploits the availability of multiple antennas to suppress the interfering signal of the smart UL jammer, defined in Subsection 3.2. Similar methods have been proposed in the literature aiming to mitigate the effects of a jamming signal in a wireless system by means of jointly mechanically adjusting an array with two antennas and applying an interference cancelation algorithm [30].

4.5.1 System description

The proposed security scheme implements beam-forming techniques at the eNodeB that leverage the availability of up to five antennas in reception. By means of a configurable signal feed, with variable delays and gains, the radiation pattern of an antenna array can be molded to achieve either enhanced directivity or strongly attenuate the signal coming from a specific direction [31]. Assuming the location of the jammer was known, a null in the antenna radiation pattern of the eNodeB could be generated to selectively block the interference. Figure 7 depicts an example of such application.

The attenuation of the interfering signal will depend on the null of the radiation pattern. In order to locate the source of the interference, a narrow directive radiation pattern can be shifted while monitoring SNR and traffic congestion metrics on the UL control channels, scanning

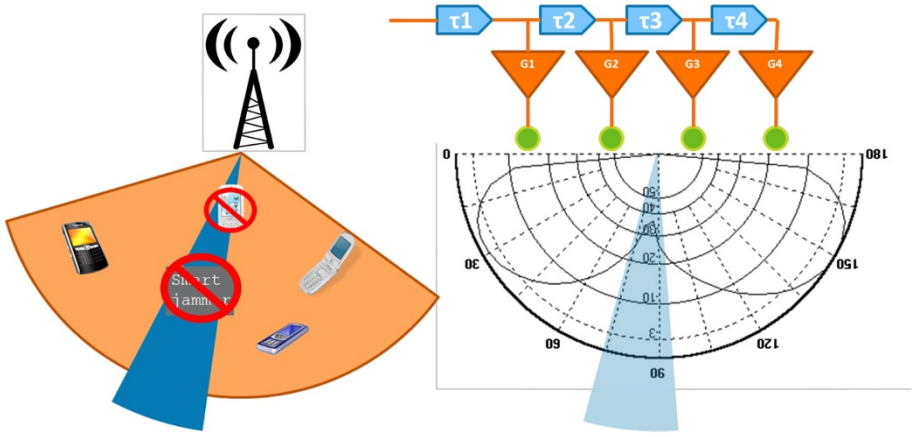

Figure 7 Beam-forming scheme for selective cancelation of UL smart jamming.

this way the entire cell or sector. This would allow to determine the angle of arrival of an incoming UL jamming signal.

4.5.2 Limitations and potential implementation

Note that the proposed architecture requires the multiple antennas of the eNodeB to perform both spatial diversity and beam-forming. The spatial separation between antennas required to optimize the diversity receiver substantially increase the phase or delay between each antenna element. In terms of the beam-forming, this could result in a suboptimal radiation pattern with considerable side lobes and a wider null in the radiation pattern. A trade-off should be found between the performance of the array in terms of diversity/MIMO and the ability to generate a narrow beam.

In parallel, all the UEs located in line with and in the close vicinity of the jammer would not be able to access the networks. Nevertheless, the range of the jammer would be significantly reduced, efficiently mitigating any uplink smart jamming attack.

It is important to note that this particular security enhancement is completely independent and both the hardware (multiple antennas at each eNodeB) and the technology (beamforming) already exist. A potential implementation could be framed within the concept of self-organizing networks (SON), as a an automatic smart jamming attack detection plus self-healing security function. Upon detection of an anomaly in a given eNodeB, in the shape of a strong decrease in the load or anomalous decrease in the SNR, the cell would go into detection mode. A narrow reception beam would scan the cell or sector. In the case of an ongoing uplink smart jamming attack, the cell would then go into a defense state, creating a null in reception and blocking the malicious interfering signal.

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 [24].

Jamming attacks have been in the scope of network and security research for several years already [16]. As new network standards arise, jamming attacks spread their threat over new technologies such as wireless sensor networks (WSNs) [15] and WLANs [4]. Mobility networks, the main commercial wireless networks, have also been considered in radio jamming studies [14].

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 networks by overloading the system at the paging channel [32] or with a spike in core network signaling messages [33]. Some other sophisticated jamming techniques have been proposed for UMTS networks [34].

The author of [20] 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 [35] and WSNs [15].

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 (barrage 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 networks. 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 make 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 propose 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 traditionally 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 Network. 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 system security. The same kind of proactive approach should be taken in order to mitigate potential DoS jamming attacks against mobility networks.

Competing interests
The authors declare that they have no competing interests.

Authors' information
Dr. Raghavan participated in this work while being a member of the AT&T Radio Access and Devices team.

Author details
[1] AT&T Security Research Center, New York, NY 10007, USA. [2] Blue Clover Devices, San Bruno, CA 94066, USA.

Received: 14 November 2013 Accepted: 27 March 2014
Published: 16 April 2014

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 Feb 2014
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 *ACM MOBIHOC; 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/wp-operation-shady-rat.pdf.
9. D Perez, J Pico, A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications, in *In BlackHat DC*, (2011). http://goo.gl/KGN3j.
10. A Rossler, Cell search and cell selection in UMTS LTE. White paper, Rhode & Schwarz (2009). http://goo.gl/ntWJPA.
11. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation. 3GPP TS 36.211 vol. v9.1.0 (2010)
12. Ettus Research. USRP. http://www.ettus.com/. Accessed Mar 2014
13. Kestrel Signal Processing, Inc. The OpenBTS Project. http://openbts.sourceforge.net/.
14. M Stahlberg, Radio jamming attacks against two popular mobile networks, in *Helsinki University of Technology. Seminar on Network Security. Mobile Security*, (2000). Accessed Apr 2014
15. W Xu, K Ma, W Trappe, Y Zhang, Jamming sensor networks: attack and defense strategies. IEEE Netw. **20**(3), 41–47 (2006)

16. T Basar, The Gaussian test channel with an intelligent jammer. IEEE Trans. Inform. Theor. **29**, 152–157 (1983)
17. 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
18. 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)
19. 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)
20. D Spaar, A practical DoS attack to the GSM network, in *In DeepSec*, (2009). http://tinyurl.com/7vtdoj5.
21. LTE/WiMAX link budget calculator (2010). http://goo.gl/phn2we. Accessed Mar 2014
22. K Ramadas, R Jain, WiMAX system evaluation methodology, in *Wimax Forum, Jan*, (2007). http://goo.gl/sNlj70.
23. B Wojtowicz, OpenLTE. An open source 3GPP LTE implementation. http://sourceforge.net/projects/openlte/. Accessed Apr 2014
24. K Nohl, S Munaut, Wideband GSM sniffing. In 27th Chaos Communication Congress (2010). http://goo.gl/wT5tz.
25. E Gadaix, GSM and 3G security, in *In BlackHat Asia*, (2001). http://tinyurl.com/85plhlv.
26. 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.
27. AJ Viterbi, *CDMA: Principles of Spread Spectrum Communication, Volume 129*. (Addison-Wesley Boston, MA, 1995)
28. P Vig, Trusted platform module. Microsoft secret weapon in the mobile arena. Zunited (2012). http://goo.gl/Iqldu.
29. S Marek, AT&T's Rinne: using SON helps improve throughput and reduce dropped calls. FierceBroadband Wireless (2012). http://goo.gl/xV70k.
30. TD Vo-Huu, EO Blass, G Noubir, Counter-jamming Using mixed mechanical and software interference cancellation, in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks,* WiSec '13 (ACM New York, 2013), pp. 31–42
31. C Balanis, *Antenna Theory: Analysis and Design*. (Wiley, New York, 1982)
32. 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
33. 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)
34. G Kambourakis, C Kolias, S Gritzalis, J Park, DoS attacks exploiting signaling in UMTS and IMS. Comput. Commun. **34**(3), 226–235 (2011)
35. 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

doi:10.1186/1687-417X-2014-7
Cite this article as: Piqueras Jover *et al.*: **Enhancing the security of LTE networks against jamming attacks.** *EURASIP Journal on Information Security* 2014 **2014**:7.