Enhancing the Robustness of LTE Systems: Analysis and Evolution of the Cell Selection Process

Mina Labib, Vuk Marojevic, Jeffrey H. Reed, and Amir I. Zaghloul

The authors analyze the effect of different levels of RF spoofing applied to LTE. RF spoofing affects LTE devices during the initial cell selection process, where a strong nearby cell can impede access to a serving LTE network. This is a serious threat and can be caused unintentionally, in the case of dense and uncoordinated LTE deployment in unlicensed spectrum, or intentionally, where an adversary sets up a fake LTE cell in either licensed or unlicensed LTE spectrum.

Digital Object Identifier:
10.1109/MCOM.2017.1500706CM

Abstract

The commercial success of LTE makes it the primary standard for 4G cellular technology, and its evolution paves the path for 5G technology. Furthermore, LTE Unlicensed has been proposed recently to allow cellular network operators to offload some of their data traffic to LTE component carriers operating in the unlicensed band. Hence, it is critical to ensure that the LTE system performs effectively even in harsh signaling environments in both licensed and unlicensed spectrum. This article analyzes the effect of different levels of RF spoofing applied to LTE. RF spoofing affects LTE devices during the initial cell selection process, where a strong nearby cell can impede access to a serving LTE network. This is a serious threat and can be caused unintentionally, in the case of dense and uncoordinated LTE deployment in unlicensed spectrum, or intentionally, where an adversary sets up a fake LTE cell in either licensed or unlicensed LTE spectrum. This article analyzes and experimentally demonstrates the severity of these threats for the evolution of LTE and proposes effective mitigation techniques to prevent denial of service. These mitigation techniques improve the cell selection process at the LTE user equipment, and are backward-compatible with existing LTE networks. We recommend that these modifications be enforced in future releases for increasing the availability and scalability of LTE.

Introduction

Since the introduction of smartphones in 2007, the mobile data demand has been growing tremendously. During that time, Long Term Evolution (LTE) has been in the process of being standardized by the Third Generation Partnership Project (3GPP). Cellular network operators' attention was drawn toward LTE as the enabling technology to meet service demands. The LTE specifications were finalized by the 3GPP in March 2009 (LTE Rel-8), and the first LTE commercial network was launched in Sweden in late 2009. LTE soon became the primary standard for fourth generation (4G) wireless communications. The 3GPP offered several enhancements in subsequent releases. In June 2011, the 3GPP finalized the first specifications for LTE-Advanced (LTE-A) in Rel-10, which adds features such as advanced modes for multiple-input multiple-output (MIMO) systems and carrier aggregation. In Rel-11, coordinated multipoint (CoMP) transmission modes were defined. In Rel-12, features such as LTE-wireless LAN integration and machine type communications (MTC) were introduced. Several new features have been introduced in Rel-13, such as narrowband Internet of Things (IoT), enhancing LTE device-to-device (D2D) services and using LTE in unlicensed spectrum.

LTE offers better coverage, enhanced system capacity, higher spectral efficiency, lower latency, and higher data rates than its predecessors in a cost-effective manner. Currently, there are 494 commercially LTE networks in 162 countries, of which 127 operators have commercially launched LTE-A carrier aggregation in 61 countries [1]. The huge amount of research and development (R&D) that has been invested in the development and deployment of LTE makes it an ideal candidate for non-commercial service, too. It promises to become the standard for a unified broadband public safety network for providing better awareness of and faster recovery from emergency situations [2]. LTE is also considered for supporting mission-critical operations, inter-vehicle communications, machine-to-machine (M2M) communications, and many other applications. LTE/LTE-A is unarguably the primary standard for 4G cellular and is expected to play a big role in the development of 5G technology [3].

The success of LTE has pushed cellular network operators to strive for innovative and scalable solutions to keep pace with the steadily growing service demand. LTE Unlicensed has been proposed recently to operate in the 5 GHz band and will allow cellular network operators to offload some of their data traffic to unlicensed bands, which can lead to a significant increase in data rates offered for LTE users [4]. Currently, there are three proposed variants of LTE Unlicensed [5]. The first is called LTE-U and is developed by the LTE-U Forum to work with the existing 3GPP Releases 10/11/12. LTE-U is designed to operate in countries, such as the United States and China, that do not mandate implementing the listen-before-talk (LBT) technique. The second variant is called licensed assisted access (LAA) and is being standardized by the 3GPP in Rel-13. The major design target for LAA is to have a single unified global

Mina Labib, Vuk Marojevic, Jeffrey H. Reed, and Amir I. Zaghloul are with Virginia Tech; Amir I. Zaghloul is also with the U.S. Army Research Laboratory.

0163-6804/17/$25.00 © 2017 IEEE

framework that complies with all the regulatory requirements in the different regions of the world. Accordingly, several functionalities need to be supported for an LAA system such as LBT (which is mandated in Europe and Japan) and dynamic frequency selection (DFS) to avoid causing interference to radar systems. These functionalities are in addition to the requirement to extend the physical layer capabilities to support operation in the 5 GHz frequency band, with system bandwidths not less than 5 MHz. These new functionalities will require modifying several functions that are performed by the different layers of the protocol stack [6]. In Rel-13, the downlink operation for LAA is defined, and the uplink operation will be added in subsequent releases. Both variants, LTE-U and LAA, propose to use the licensed spectrum as the primary carrier for signaling (control channels) and to carry data of users with high quality of service (QoS) requirements. Carrier aggregation will be used to add secondary component carriers in the unlicensed spectrum to deliver data to users with best effort QoS requirements. The third variant of LTE Unlicensed is called MulteFire and is proposed by Qualcomm as a standalone version of LTE for small cells. This variant will use only the unlicensed spectrum in the 5 GHz band as the primary and only LTE carrier.

Since LTE will keep playing a dominant role for broadband communications for years to come, reliability becomes an important aspect for the evolution of LTE. LTE security-related questions have been posed recently and investigated by several researchers. Despite the fact that LTE provides higher security than previous generations of cellular systems, such as UMTS (3G) or GSM (2G) [7], LTE is still vulnerable to natural or unintentional as well as intentional interference [8]. Unintentional interference has been broadly analyzed, and interference mitigation, coordination, and cancellation techniques have been proposed. Enhanced interference cancellation techniques are deployed today and continuously improved to allow for network densification as a means of increasing capacity. LTE was originally designed for use in licensed spectrum and has mechanisms for dealing with low signal-to-noise ratio. However, LTE lacks mechanisms for protecting control channels from intentional interference. Intentional interference at the physical layer can be in the form of jamming or RF spoofing. Jamming refers to intentional RF interference to a target signal. The work in [9] provides an overview of the physical layer resiliency of orthogonal frequency-division multiplexing (OFDM), the air interface of LTE. Jamming can be categorized under barrage jamming, partial-band jamming, pilot-tone jamming, and protocol-aware jamming. Protocol-aware jamming refers to interference generated to a specific subsystem by using knowledge of the different physical channels and signals, their locations, and their roles in effective system operation. The potential threat of LTE protocol-aware jamming was brought to light in a letter to the U.S. Department of Commerce [10]. As opposed to jamming, RF spoofing does not generate a noise-like signal that interferes with the target signal, but rather regenerates specific control signals that impede the user from attaching to the regular network and receiving communications service [11].

This article discusses the following aspect of the evolution of LTE: the need to ensure service availability to satisfy the growing dependence on 4G LTE services for different types of applications, including commercial and mission-critical. We identify an emerging threat that can slow down the evolution of LTE. This threat is in the form of RF spoofing, which affects the initial cell selection process as a result of natural or international interference. After providing the necessary background, this article analyzes the problem, proposes effective solutions, and discusses their impact.

There are a series of messages in LTE that are collectively called *system information* messages. Some of these system information messages comprise information regarding the cell and its configuration, and enable the UE to access the cell and establish a connection with the network.

The Initial Cell Selection Process in LTE

During initialization, the user equipment (UE) performs the cell selection process and acquires the basic network information. The UE then performs the random access procedure to access the network and set up a dedicated connection with the eNodeB. Once the connection is established, the UE requests to attach to the network, and the authentication procedure follows. In each of these stages, protocol-specific messages are exchanged between the different protocol layers of the UE and their counterparts at the eNodeB or the evolved packet core network. Figure 1 summarizes the main steps that the UE performs as part of the cell selection process. The protocol layers involved are the physical (PHY), radio resource control (RRC), and non-access stratum (NAS) layers. At power up, the UE tries to find a cell to camp on. *Camping on a cell* means tuning to the control channels of that cell and enables the UE to receive broadcast messages transmitted by the eNodeB. These are a series of messages that are collectively called *system information* messages. Some of these system information messages comprise information regarding the cell and its configuration, and enable the UE to access the cell and establish a connection with the network.

In order to select a cell, a public land mobile network (PLMN) should first be selected by the NAS layer, which then requests the RRC layer to select a cell of the selected PLMN (or its equivalents), that is, a cell that broadcasts in its system information messages that it belongs to the selected PLMN (or its equivalents) [12].

During the cell selection process, the UE sequentially scans the bands that it supports. This band scanning enables the UE to find the active RF channels on the supported LTE bands. (An RF channel is considered active if the received signal strength indicator, or RSSI, exceeds a certain threshold.) In the case where there is more than one LTE cell on an active RF channel, the UE selects the strongest cell as per the LTE 3GPP specifications, which state that "the UE needs only search for the strongest cell" at any given frequency [13]. The reason for this is to prevent UEs from creating uplink interference by choosing a cell other than the strongest. The UE acquires timing and frequency synchronization with the help of the cell's primary and secondary synchronization signals (PSS and SSS). More precisely, the PHY layer down-converts and digitizes the received signal on a carrier frequency and correlates it with three locally generated primary synchronization sequences in the time domain to find the strongest cell, that is, the cell that provides the highest correlation result. Based on the correlation results, RF spoofing in LTE can have two forms: intentional and unintentional. Intentional spoofing involves an attacker that creates a partial or full LTE downlink frame (fake cell) trying to deceive UEs and prevent them from camping on a legal cell. Unintentional spoofing happens when cells are densely deployed in an uncoordinated way.

the UE determines the cell's physical layer identity and acquires time and frequency synchronization. The PHY layer then detects the SSS, which is at a known position with respect to the PSS and carries the physical cell identity group. The physical cell identity group together with the physical layer identity provides the unambiguous physical cell identity (PCI). The UE also learns about the cyclic prefix (CP) type and the frequency-/time-division duplex (FDD/TDD) mode used by the cell.

Once the UE is time- and frequency-aligned with the LTE downlink frame, it looks for the reference signal (RS) at known locations for a cell quality check and for channel equalization, which is needed to decode the master information block (MIB). The MIB is part of the broadcast control channel (BCCH) carried over the physical broadcast channel (PBCH) and contains the essential LTE system access parameters, such as the LTE system bandwidth and the system frame number.

The UE next acquires the *SystemInformationBlockType1* or SIB1 message, which is also part of the BCCH, but is carried over the physical downlink shared channel (PDSCH). By decoding this message, the UE can complete its check if the cell

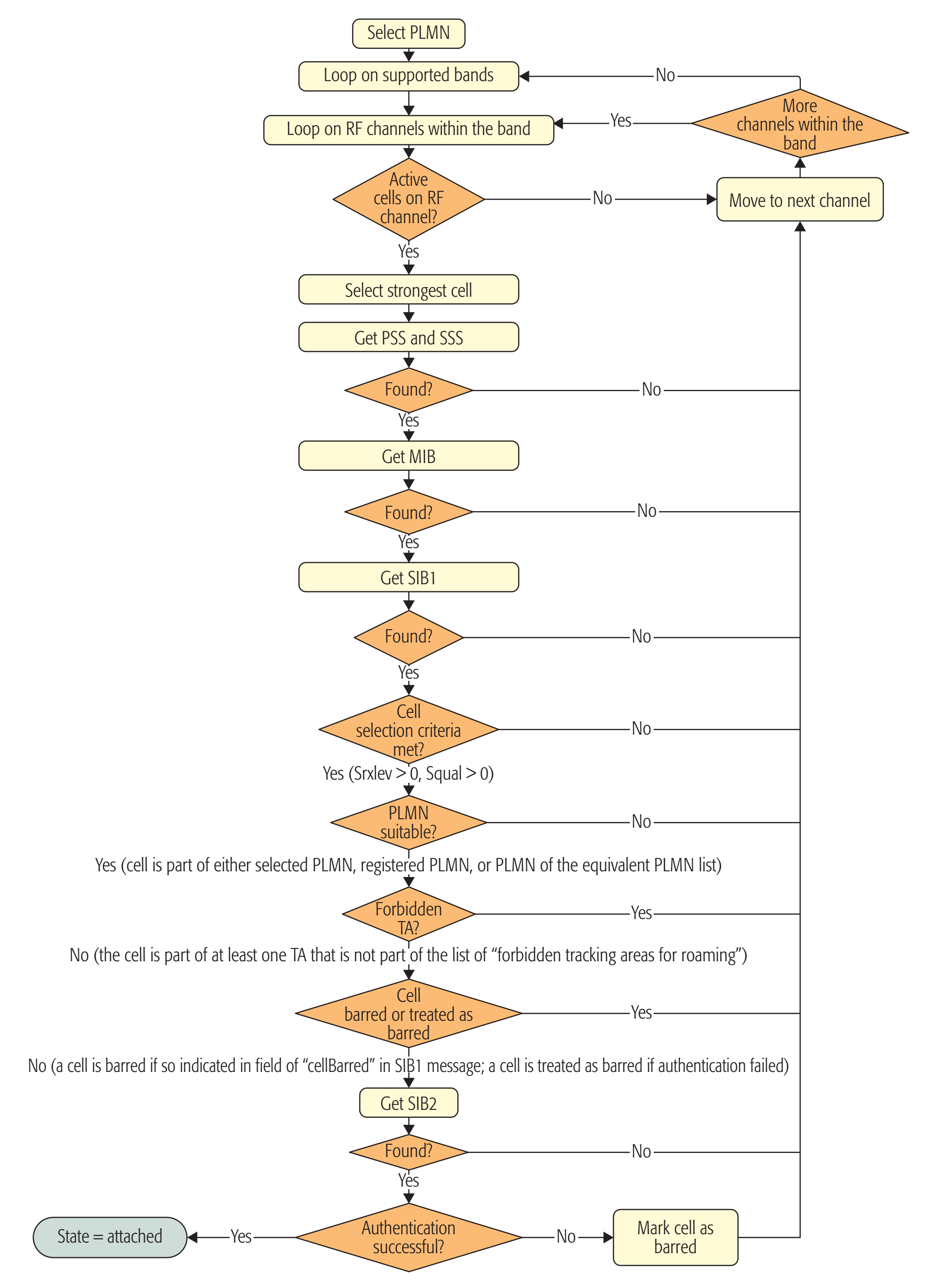

Select PLMN
Loop on supported bands
No
Loop on RF channels within the band
Yes
More channels within the band
Active cells on RF channel?
No
Move to next channel
Yes
Select strongest cell
Get PSS and SSS
Found?
No
Yes
Get MIB
Found?
No
Yes
Get SIB1
Found?
No
Yes
Cell selection criteria met?
No
Yes (Srxlev > 0, Squal > 0)
PLMN suitable?
No
Yes (cell is part of either selected PLMN, registered PLMN, or PLMN of the equivalent PLMN list)
Forbidden TA?
Yes
No (the cell is part of at least one TA that is not part of the list of "forbidden tracking areas for roaming")
Cell barred or treated as barred
Yes
No (a cell is barred if so indicated in field of "cellBarred" in SIB1 message; a cell is treated as barred if authentication failed)
Get SIB2
Found?
No
Yes
State = attached
Yes
Authentication successful?
No
Mark cell as barred

Figure 1. Initial cell selection process for the UE.

is suitable for camping. A cell is suitable for camping if it satisfies the following criteria:

- The *S-criterion*, meaning that the cell has a good power level and quality, measured in terms of reference signal received power (RSRP) and reference signal received quality (RSRQ).
- The cell is part of either the selected PLMN, the registered PLMN, or a PLMN from the equivalent PLMN list. The selected PLMN or its equivalents are provided by the NAS layer to the RRC layer when requesting to select a cell. The PLMN to which the cell belongs is advertised in the SIB1 message.
- The cell is part of at least one tracking area (TA) that is not part of the list of *forbidden tracking areas for roaming*. The *forbidden tracking areas for roaming list* is provided by the NAS layer. The SIB1 message contains the tracking area code (TAC) to which the cell belongs.
- The cell is not barred or treated as a barred cell. A cell is barred if it is indicated as such in the SIB1 message field *cellBarred*. A cell is treated as barred when the mutual authentication between the UE and the network fails.

The SIB1 message also contains other important information, such as the cell identity and the *intraFreqReselection* flag, which indicates whether the UE is allowed to choose the second strongest cell at the same frequency in case the strongest cell is barred or to be treated as barred by the UE.

If all the conditions for camping are satisfied, the RRC layer considers the cell suitable for camping and instructs the PHY layer to acquire the *SystemInformationBlockType2* or SIB2 message. Like the SIB1 message, the SIB2 message is also part of the BCCH and is carried over the PDSCH. The UE is now camped on the cell, and the initial cell selection procedure terminates. Otherwise, if the UE finds that the strongest cell is not suitable for camping (one or more suitable cell criteria are not met), it will try to camp on the strongest cell on another active carrier in a given band. If no suitable cell is found on all active RF channels in a band, the UE will continue searching for a suitable cell on another band that is supported by the UE. The network is acquired when a suitable cell for camping is found.

After network acquisition, the UE starts the connection establishment procedure in order to attach to the network. Attaching to the network means that the UE registers itself with the network, followed by the mutual authentication process. If the UE successfully authenticates with the network, the attachment procedure is completed successfully. If the mutual authentication between the UE and the network fails, the UE will treat the cell as barred. The UE shall exclude the barred cell, or the cell that is treated as barred, for 300 s [13].

The initial cell selection process was first standardized in 3GPP Rel-8 and was not changed through Rel-12. All LTE service consumers need to go through the initial cell selection process every time the UE is turned on or returns from being out of coverage. Whereas making it simple and flexible was the primary objective when LTE was first launched, the massive deployment of LTE in dense urban areas, the need for providing extensive new applications, and the LTE evolution into the unlicensed spectrum require revisiting the cell selection process and analyzing its robustness against unintentional and intentional RF interference.

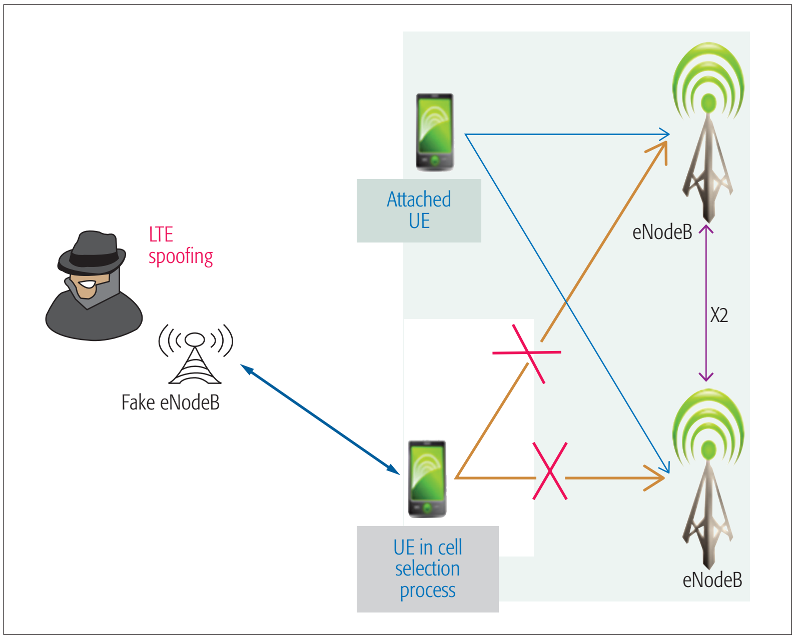


Figure 2. Intentional LTE RF spoofing.

RF Spoofing in LTE

RF spoofing in LTE can have two forms: intentional and unintentional. Intentional spoofing involves an attacker that creates a partial or full LTE downlink frame (fake cell) trying to deceive UEs and prevent them from camping on a legal cell. Unintentional spoofing happens when cells are densely deployed in an uncoordinated way.

Intentional RF Spoofing

RF spoofing in LTE was introduced in [11] and refers to setting up a fake eNodeB that transmits some of the LTE signals and higher-layer control messages (which is why it can be called LTE control channel spoofing), but does not have the authentication keys or offer any service. If this fake eNodeB appears as the strongest cell at the UE for a given frequency channel, the UE will try to camp on this fake cell and will not be able to select any other LTE cell in that channel. The different levels of spoofing range from creating a fake LTE frame that contains only the PSS/SSS to creating a fake LTE frame that contains most of the LTE downlink control signals and channels. The concept of intentional RF spoofing is illustrated in Fig. 2.

Synchronization Signal Spoofing: The simplest way of RF spoofing is PSS & SSS spoofing, which is a PHY layer signaling attack. A PSS along with an SSS are created according to the LTE specifications. That is, the fake eNodeB arbitrarily chooses the synchronization sequences (PSS and SSS) and periodically transmits them asynchronous to, but on, the LTE carrier frequency of the legal eNodeB. When the PHY layer of the UE reports to the RRC layer that it has received the PSS and SSS, the RRC will expect to receive the MIB message next. Since no PBCH is transmitted, the RRC layer

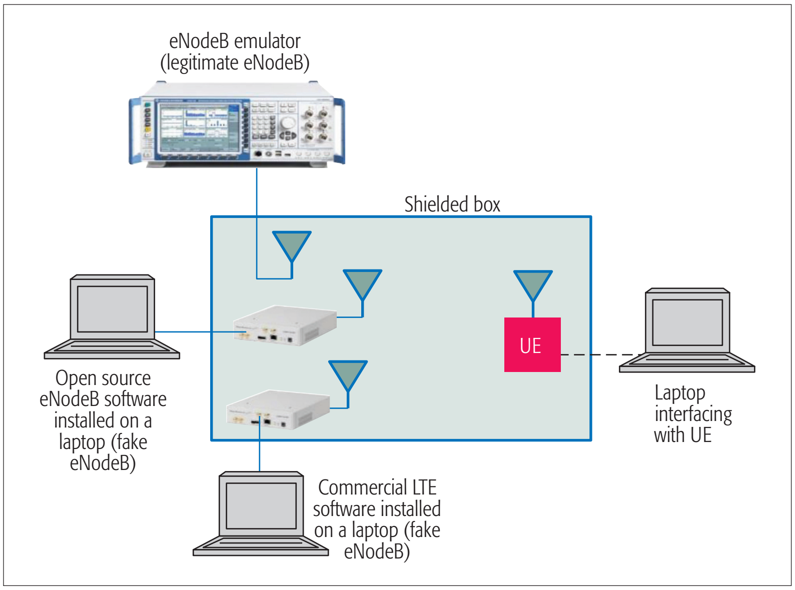

eNodeB emulator
(legitimate eNodeB)
Shielded box
UE
Open source eNodeB software installed on a laptop (fake eNodeB)
Laptop interfacing with UE
Commercial LTE software installed on a laptop (fake eNodeB)

Figure 3. Block diagram of the testbed.

eventually instructs the PHY layer to search for another cell at another frequency.

The 3GPP specifications for RRC [14] state that if the RRC is in the idle mode and does not receive either the MIB or SIB1 message, the UE shall treat this cell as barred and perform barring as if the *intraFreqReselection* flag is set to *allowed*. Hence, the UE may select the second strongest cell. However, many UE manufacturers may overlook the importance of choosing the second strongest cell for the sake of simplifying the interface between the PHY and RRC layers. The implications of this would be allowing the RRC to instruct the PHY to scan only a specific frequency, and the PHY is programmed to deliver only the strongest cell and does not have the ability to distinguish between a barred and a non-barred cell, as demonstrated in [15].

Partial LTE Downlink Frame Spoofing: A more sophisticated way of spoofing is when the fake eNodeB transmits a partial LTE frame using the PLMN of the legal eNodeB. This frame contains the PSS, SSS, RS, PBCH, and the PDSCH's SIB1 message, but not SIB2. The 3GPP specifications state that if the UE does not receive the SIB2 message, it shall treat this cell as barred and shall refer to the received SIB1 message to learn if it is allowed to select another cell within the same frequency by reading the *intraFreqReselection* flag in the SIB1 message. The attacker simply needs to set this flag to *notAllowed* to prevent the UE from camping on a cell at this frequency. This type of vulnerability is not implementation-specific, but rather standard-specific [15].

If the attacker sends a SIB2 message as well, the UE initiates the mutual authentication process after decoding the SIB2 message. The authentication process fails since the fake eNodeB does not have the valid keys. As a result, the UE treats this cell as barred, and the RRC layer starts a new cell selection process. During this new cell selection process, the PHY layer will again report the strongest cell; the RRC layer will find that the cell is to be treated as barred and consequently instruct the PHY layer to resume the cell search on a different frequency [11].

System Information Message Spoofing: The fake eNodeB transmits specific parameters in the SIB messages to cause denial of service. The *cellBarred* field in the SIB1 message was introduced by the 3GPP to enable mobile operators to perform testing and maintenance on any cell before allowing users to actually access it. If the *cellBarred* field is set to *True*, the particular cell will be barred. In this case, and according to the 3GPP specifications, the UE will exclude the barred cell for 300 s. If the fake cell transmits the same PCI as the legal eNodeB, the legal eNodeB will be wrongly excluded by the UE for 300 s, even if the fake cell is turned off in the meanwhile. The fake cell could operate at a low duty cycle and still permanently prevent a UE from camping on the legal cell by repeatedly barring it [11].

Unintentional RF Spoofing

MulteFire entails multiple private small cell eNodeBs transmitting exclusively in the unlicensed band. If there are two eNodeBs belonging to different networks that happen to transmit on the same frequency, an effect similar to RF spoofing may occur. When a UE receives an LTE frame from a neighbor eNodeB with higher power than its own eNodeB, it will try to access this network. The authentication process will fail because the UE does not belong to the network it tries to access. It is important to point out that this may happen only if the two eNodeBs have the same PLMN, and the PLMN consists of a Mobile Country Code (MCC), which is 3 digits, and a Mobile Network Code (MNC), which is 2 or 3 digits. Given the fact that we are considering the case where MulteFire will be operated in an uncoordinated way for private and dense small cells, and a PLMN can be set up by the user during the initial eNodeB setup and configuration, this scenario is not unlikely. Furthermore, the authentication process for MulteFire has not been identified yet, and there is a discussion about removing the need for a SIM card at the UE to keep it as simple as WiFi.

In this case, once the UE synchronizes to the strongest cell, it will not be able to resynchronize to a weaker cell, as explained above and demonstrated later. Hence, denial of service will occur. Given that for MulteFire the cell is not expected to offer access through another type of wireless technology (e.g., 3G or 2G), the UE will not be able to receive any service at all.

Experimental Assessment

We have created a lab-scale testbed in order to validate the effect of LTE control channel spoofing on the UE. Figure 3 shows the block diagram of the testbed. The test results consistently show that RF spoofing impedes UEs that are in the initial cell selection process from attaching to the legal eNodeB. The UE is able to attach to the legal eNodeB after the fake or uncoordinated cell is turned off. The test procedures and results are summarized in Fig. 4.

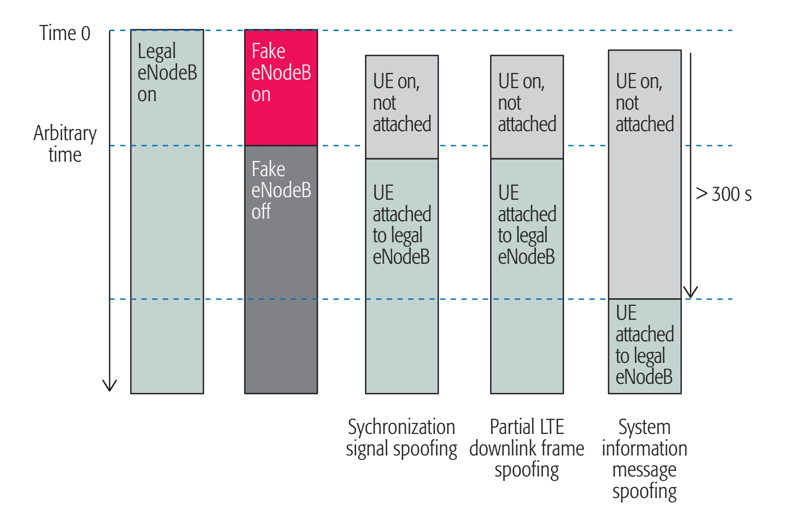
For LTE and LTE-A systems, a fake eNodeB that transmits part of the LTE frame can enforce the UE to search for an LTE signal in a different RF channel or band. Given that most LTE networks are based on a single frequency, this will cause permanent denial of service for the UE to the LTE network. In this case, the UE will have to downgrade its service to a 3G or 2G system, which offers a much slower data rate and is vulnerable to other types of security attacks. It is worth mentioning that rebooting the UE device will not solve the problem. The UE is not able to attach to the LTE network as long as the UE receives the fake synchronization signals at a higher power level than those that are transmitted from the legal eNodeB.

Mitigation

We propose simple modifications to the LTE cell selection process that would effectively mitigate the effect of RF spoofing. Figure 5 indicates the proposed modifications. They can be summarized as follows:

- The PHY layer should report to the RRC layer a list of all cells that are detected along with their corresponding PCI and received power levels. The RRC layer should save this list.
- The RRC layer should create two separate flags, one for a barred cell as received in the SIB1 message, and one for a cell to be treated as barred to ensure that the UE will handle these two cases differently. The cell should be treated as barred in the following cases:
  –When the mutual authentication process between the UE and the network fails at the UE side
  –When the UE does not receive any of the control messages, specifically the MIB, SIB1, or SIB2 messages, within a specific time frame, which also needs to be specified
- The RRC layer should first check if the cell is to be treated as barred, before checking if the cell is barred.
- When the cell is to be treated as barred, the UE should be allowed to select the second strongest cell at the same frequency.
- If the *cellBarred* flag in SIB1 is *True*, the RRC layer should check for any duplicate PCI at the same frequency. If the RRC finds that *cellBarred* is *True*, and the PCI of that cell is not unique, the RRC layer should flag this cell to be treated as barred.

To elaborate further, we propose allowing the UE to select the second strongest cell at the same frequency only for the case when the strongest cell is to be treated as barred. The reason for the 3GPP specifications mandating the UE to select the strongest cell is to not create excessive uplink interference by the UE to other UEs when communicating with a farther cell. The proposed modifications allow selecting the second strongest cell if and only if the strongest cell is to be treated as barred. In the case of licensed spectrum, when the cell is flagged as "to be treated as barred," there are no UEs attached to it. Hence, the UE will not create any uplink interference if it selects the second strongest cell. This proposed modification will not affect the current UE procedure in case of roaming or handover, as these only affect the UE initialization process when the authentication fails at the UE side, and it will be an effective mitigation technique against partial LTE downlink frame spoofing. In the case of unlicensed spectrum, when the strongest cell is marked as "to be treated as barred," this means that cell is not the serving eNodeB for this UE. In this case, the UE should keep searching for its own eNodeB by allowing it to select the second strongest cell.



Time 0
Arbitrary time
Legal eNodeB on
Fake eNodeB on
Fake eNodeB off
UE on, not attached
UE attached to legal eNodeB
UE on, not attached
UE attached to legal eNodeB
UE on, not attached
> 300 s
UE attached to legal eNodeB
Sychronization signal spoofing
Partial LTE downlink frame spoofing
System information message spoofing

Figure 4. Summary of test results for the different types of RF spoofing.

We also propose to create a timer at the RRC layer for receiving any of the essential LTE control messages (e.g., the MIB, SIB1, or SIB2 messages), and when the timer expires, the RRC marks this cell as "to be treated as barred." This then allows the UE to select the second strongest cell in case of failing to receive any of the required control messages. If the RRC layer does not receive the expected message within the specified time, the RRC can mark this cell to be treated as barred. Hence, the UE would mark a cell to be treated as barred when the mutual authentication fails or when the UE does not receive a control message within the specified timeframe. This is our proposed mitigation method against synchronization signal spoofing.

By creating two separate flags, one for a cell to be treated as barred and one for a barred cell, we ensure that the UE will handle the two cases differently. In the case where the fake eNodeB broadcasts itself as barred in the SIB1 message, we propose that the UE checks if this PCI is duplicated in the list of the received PCIs at that frequency. If so, we recommend that the UE treats this cell as barred. This would allow the UE to select the second strongest cell rather than automatically search on a different frequency. The network can eventually hand over the UE to the strongest cell, which was mistakenly barred as a result of RF spoofing, and so avoid denial of service caused by system information message spoofing.

For the case of unintentional spoofing, after the UE fails to authenticate the network that is transmitting the strongest cell, the proposed modifications will enable the UE to select the second strongest cell, which belongs to its own network.

The proposed modifications collectively provide an effective mitigation method against the different types of intentional and unintentional RF spoofing discussed in this article. These changes ensure backward compatibility with the deployed LTE devices and networks, and do not

With the advent of LTE operating in unlicensed bands, the availability of the LTE network can become increasingly compromised the more networks are deployed. This is not only because of the classical inter-cell interference, but also because of the cell selection process that does not scale well for uncoordinated operation in unlicensed bands.

introduce excessive uplink interference. Hence, the proposed modifications will not lead to any performance degradation when compared to the current LTE system deployments and operation.

Conclusions

We have shown how RF spoofing, whether intentional or unintentional, can prevent LTE/LTE-A users from accessing the network and obtaining 4G services. As the number of users grows and new LTE technologies appear, this can become a serious threat that will impede scaling LTE to fulfill the emerging needs.

With the advent of LTE operating in unlicensed bands, the availability of the LTE network can become increasingly compromised the more networks are deployed. This is not only because of the classical inter-cell interference, but also because of the cell selection process that does not scale well for uncoordinated operation in unlicensed bands. Future mission-critical networks likewise can suffer from this. Public safety and mil-

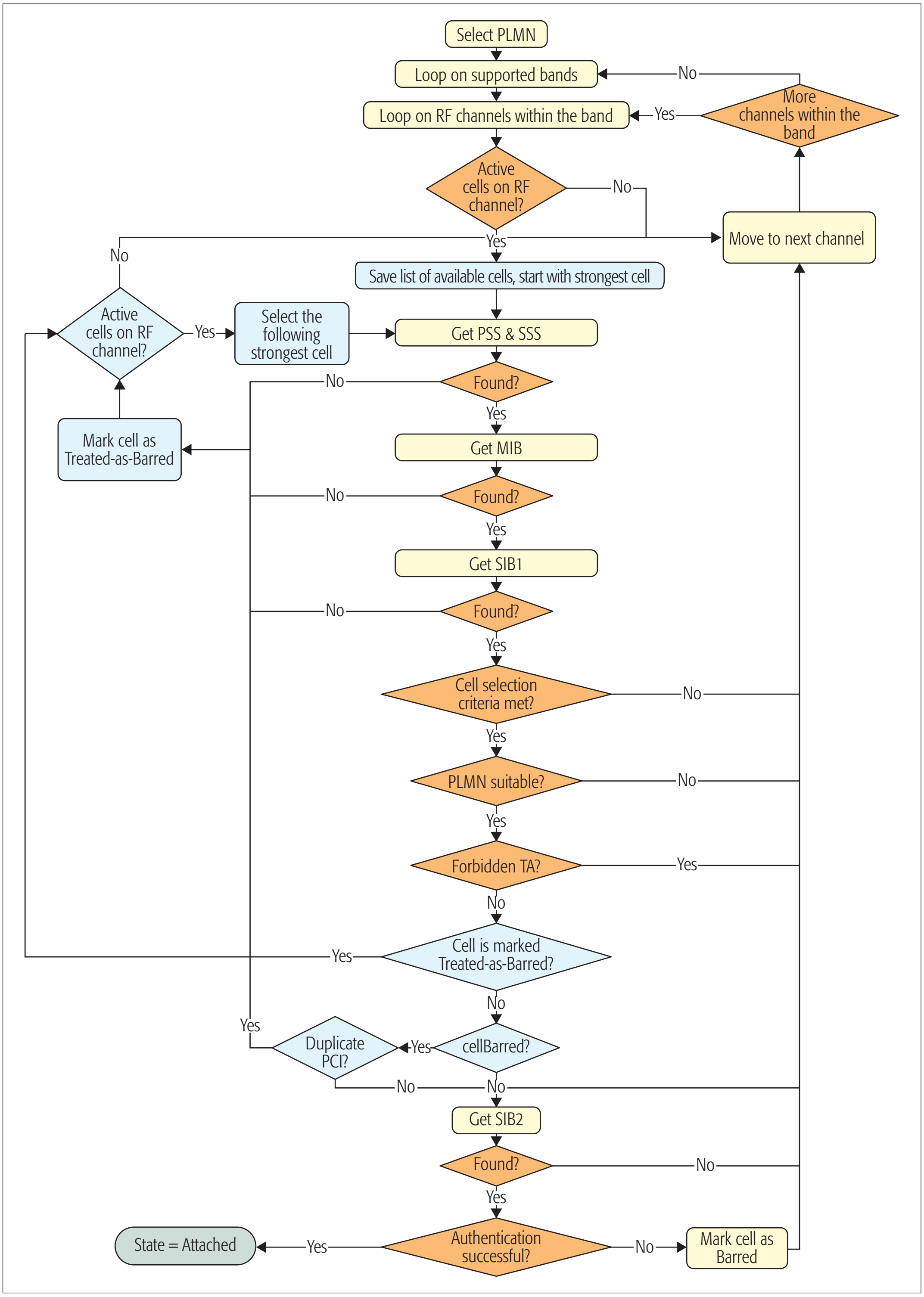

Select PLMN
Loop on supported bands
No
Loop on RF channels within the band
Yes
More channels within the band
Active cells on RF channel?
No
Yes
Move to next channel
No
Save list of available cells, start with strongest cell
Active cells on RF channel?
Yes
Select the following strongest cell
Get PSS & SSS
No
Found?
Yes
Mark cell as Treated-as-Barred
Get MIB
No
Found?
Yes
Get SIB1
No
Found?
Yes
Cell selection criteria met?
No
Yes
PLMN suitable?
No
Yes
Forbidden TA?
Yes
No
Yes
Cell is marked Treated-as-Barred?
No
Yes
Duplicate PCI?
Yes
cellBarred?
No
No
Get SIB2
Found?
No
Yes
State = Attached
Yes
Authentication successful?
No
Mark cell as Barred

Figure 5. Proposed cell selection process.

itary systems will use LTE Rel-8 or higher. Hence, we recommend adopting these simple fixes in future releases of LTE-A and use these releases for networks that will offer mission-critical services.

Beyond LTE-A, next generation networks need to be more reliable by providing robust network access. Research is needed to redesign the network access procedure and help avoid potential problems that can arise from exploiting the openness of standards and control channel dependency.

Beyond LTE-A, next generation networks need to be more reliable by providing robust network access. Research is needed to redesign the network access procedure and help avoid potentail problems that can arise from exploiting the openness of standards and control channel dependency.

Acknowledgment

Portions of this work are covered under U.S. Patent Application 62/156377. This work was supported in part by Vencore Inc., the Defense University Research Instrumentation Program (DURIP) contract numbers W911NF-14-1-0553/0554 through the Army Research Office, and the National Science Foundation (NSF) contract number CNS-1642873.

References

[1] GSA, "Evolution to LTE Report: 4G Market and Technology Update," Global Mobile Suppliers Assn., tech. rep., Apr. 2016; http://www.gsacom.com.

[2] T. Doumi *et al.*, "LTE for Public Safety Networks," *IEEE Commun. Mag.*, vol. 51, no. 2, Feb. 2013, pp. 106–12.

[3] J. Andrews *et al.*, "What Will 5G Be?," *IEEE JSAC*, vol. 32, no. 6, June 2014, pp. 1065–82.

[4] R. Zhang *et al.*, "LTE-Unlicensed: The Future of Spectrum Aggregation for Cellular Networks," *IEEE Wireless Commun.*, vol. 22, no. 3, June 2015, pp. 150–59.

[5] D. R. Brenner and J. W. Kuzin, "Before the Federal Communications Commission: Reply Comments of Qualcomm Incorporated," June 2015; http://apps.fcc.gov/ecfs/document/view?id=7022130311.

[6] 3GPP, "Study on Licensed-Assisted Access to Unlicensed Spectrum (Release 13)," TS 36.889, 2015; http://www.3gpp.org/dynareport/36889.htm.

[7] J. Cao *et al.*, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 1, 1st qtr. 2014, pp. 283–302.

[8] R. Jover, "Security Attacks against the Availability of LTE Mobility Networks: Overview and Research Directions," *2013 16th Int'l. Symp. Wireless Personal Multimedia Commun.*, June 2013, pp. 1–9.

[9] C. Shahriar *et al.*, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 1, 1st qtr., 2015, pp. 292–314.

[10] J. H. Reed and M. Lichtman, "FirstNet Conceptual Network NOI — Comments of Wireless @ Virginia Tech," before the Dept. of Commerce, Docket No. 120928505250501, RIN 0660XC002, Nov 2012; http://www.ntia.doc.gov/files/ntia/va_tech_response.pdf.

[11] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing," *IEEE Conf. Standards for Commun. and Net. Proc.*, Oct. 2015, pp. 160–65.

[12] S. Sesia, I. Toufik, and M. Baker, *LTE — The UMTS Long Term Evolution: From Theory to Practice*, 2nd ed., Wiley, 2011.

[13] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Procedures in Idle Mode (Release 12)," TS 36.304, Mar. 2015; http://www.3gpp.org/dynareport/36304.htm

[14] —, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) (Release 12)," TS 36.331, Mar. 2015; http://www.3gpp.org/dynareport/36331.htm

[15] M. Labib *et al.*, "How to Enhance the Immunity of LTE Systems against RF Spoofing," *Int'l. Conf. Computing, Networking and Commun.*, Feb. 2016.

Biographies

Mina Labib (mlabib@vt.edu) received his B.S. degree from Ain Shams University, Cairo, Egypt, in electronics and communications engineering, and his M.Sc. degree from Carleton University, Ottawa, Ontario, Canada, in systems and computer engineering. He is currently working toward his Ph.D. degree at the Bradley Department of Electrical and Computer Engineering at Virginia Tech within the Wireless@VirginiaTech research group. He has wide industrial experience, especially in the field of physical and MAC layer design. His current research interests are in the broad areas of wireless communications, with a particular emphasis on LTE systems, enhancing the security of wireless communication systems, LTE-Unlicensed, spectrum sharing, and game theory.

Vuk Marojevic(maroje@vt.edu) received his M.S. from the University of Hannover, Germany, and his Ph.D. from the Universidad Politècnica de Catalunya, both in electrical engineering. He joined Wireless@Virginia Tech in 2013. His research interests are in software-defined radio, spectrum sharing, 4G/5G cellular technology, wireless testbeds and testing, and resource management with application to public safety and mission-critical networks and unmanned aircraft systems.

Jeffrey H. Reed [F] is the founder of Wireless@Virginia Tech, and served as its director until 2014. He is the founding faculty member of the Ted and Karyn Hume Center for National Security and Technology, and served as its interim director when founded in 2010. His book *Software Radio: A Modern Approach to Radio Design* was published by Prentice Hall ,and his latest textbook, *Cellular Communications: A Comprehensive and Practical Guide*, was published by Wiley-IEEE in 2014. He is co-founder of Cognitive Radio Technologies (CRT), a company commercializing cognitive radio technologies; Federated Wireless, a company developing spectrum sharing technologies; and PFP Cybersecurity, a company specializing in security for embedded systems. In 2005, he became a Fellow of the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education. In 2013 he was awarded the International Achievement Award by the Wireless Innovations Forum. In 2012 he served on the President's Council of Advisors of Science and Technology Working Group, which examines ways to transition federal spectrum for commercial use. He is a past member of CSMAC, a group that provides advice to the NTIA on spectrum issues.

Amir I. Zaghloul [LF] is an ARL Fellow with the Sensors and Electron Devices Directorate (SEDD) of the U.S. Army Research Laboratory (ARL), Adelphi, Maryland. After 24 years at COMSAT Laboratories performing and directing R&D efforts on satellite communications and antennas, he joined Virginia Tech in 2001 as a professor in the Electrical and Computer Engineering Department. In 2008, he was assigned as an IPA from Virginia Tech to the ARL, and subsequently switched to full-time at ARL in 2012, maintaining his affiliation with Virginia Tech as a research professor. He is also affiliated with the University of Delaware (2012–present). He has held positions at the University of Waterloo, Canada (1968–1978), the University of Toronto, Canada (1973–1974), Aalborg University, Denmark (1976), and Johns Hopkins University, Maryland (1984–2001). He is a Fellow of the Applied Computational Electromagnetics Society (ACES) and an Associate Fellow of the American Institute of Aeronautics and Astronautics. He is also the International Vice-Chair of Commission C of the International Union of Radio Science (URSI), and has held several positions at the IEEE, URSI, and ACES. He has received several research and patent awards, including the Exceptional Patent Award at COMSAT and the 1986 Wheeler Prize Award for Best Application Paper in *IEEE Transactions on Antennas and Propagation*. He received his Ph.D. and M.A.Sc. degrees from the University of Waterloo in 1973 and 1970, respectively, and his B.Sc. degree (Honors) from Cairo University, Egypt, in 1965, all in electrical engineering. He also received an M.B.A. degree from George Washington University in 1989.