Resilience of LTE Networks Against Smart Jamming Attacks

Farhan M. Aziz†, Jeff S. Shamma†‡ and Gordon L. Stüber†
†School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia 30332–0250
‡CEMSE Division, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
Email: {faziz, shamma, stuber}@ece.gatech.edu

***Abstract*—Commercial *LTE* networks are being studied for mission-critical applications, such as public safety and smart grid communications. In this paper, *LTE* networks are shown vulnerable to *Denial-of-Service (DOS)* and *loss of service* attacks from *smart jammers*, who may employ simple narrowband jamming techniques to attack without any need to hack the network or its users. We modeled the *utilities* of jamming and anti-jamming actions played by the jammer and the network under the framework of *single-shot* and *repeated Bayesian games*. In a single-shot game formulation the only *Nash Equilibria (NE)* are pure strategy equilibria at which network utility is severely compromised. We propose a *repeated-game learning and strategy algorithm* for the network that outperforms single-shot games by a significant margin. Furthermore, all of our proposed actions and algorithms can be implemented with current technology.**

Keywords: ***LTE, control channels, smart jamming, anti-jamming, Game theory, Bayesian games, repeated games, learning.***

I. Introduction

A. Rationale

Long Term Evolution (LTE) and *LTE-Advanced (LTE-A)* [1] are probably the most advanced broadband wireless networks deployed today. However, being a commercial wireless network, *LTE* specifications and protocols are publicly known to its designers, developers, users and the general audience around the world. Lately, some researchers have suggested using *LTE* for mission-critical applications like public safety and smart grid communications because of its ubiquity, high data rates, flexibility, mobility and ease of access. However, we will show that *LTE* networks are vulnerable to *smart jamming* attacks without being hacked by an adversary. A *User Equipment (UE)* can "learn" the network timing and synchronize itself with the network even when it is not *attached* to it. A *smart jammer* colludes with such a *UE* and jams various essential parts of the network known as *Common Control Channels* by employing narrowband jamming. It can launch effective *denial-of-service (DOS)* attacks against legitimate network users without using wideband jamming techniques or excessive transmit power. We will discuss some possible ways a *smart jammer* can attack the network and propose several countermeasures a network can take against such attacks.

B. Related Work

Some researchers have proposed using commercially and privately owned *LTE* networks for mission-critical applications like public safety (e.g., [2], [3]), and smart grid (e.g., [4], [5]) communications. Being a commercial network, *LTE* raises serious security concerns, such as *denial-of-service (DOS)*, data integrity and information privacy attacks [6]. Researchers in [7] and [8] pointed out further security vulnerabilities in *LTE* networks related to its flat all-IP based system architecture, access authentication procedures, etc. Some researchers have suggested schemes to combat jamming attacks on non-*Orthogonal Frequency Division Multiplexing (OFDM)*-based wireless networks. For example, [9] proposed network coding to protect broadcasting in multi-channel wireless networks. Similarly, researchers in [10] proposed uncoordinated spread spectrum techniques in order to enable anti-jamming broadcast communication in the presence of malicious receivers. However, *OFDM*-based systems like *LTE* are less resistant to jamming and interference as compared to their counterpart spread spectrum systems. Researchers in [11] analyzed the performance of multi-carrier systems like *OFDM* when *pilot* symbols are jammed causing noisy channel estimation leading to degraded system performance.

This paper deals with the intelligent jamming of *LTE* control channels. Thuente *et al.* [12] explored intelligent jamming in *IEEE 802.11b* networks. Liu *et al.* [13] explored the case of a cognitive radio ad-hoc network suffering from control channel jamming attack from inside jammers. The authors proposed algorithms for unique identification of the set of compromised nodes. Similarly, Petracca *et al.* [14] evaluated performance of GSM networks' robustness against control channel jamming attacks and showed that GSM network security can be significantly compromised by such attacks. Recently, Reed [15] brought the potential of control channel vulnerabilities in *LTE* networks to the attention of the US Department of Commerce. However, to the best of our knowledge, the impact of *smart jamming* on the performance of *LTE* networks is an open problem. We formulate and analyze this problem in a game-theoretic framework.

II. Jamming in LTE Networks

A. A Brief Overview of LTE Air Interface

LTE is an *OFDM*-based air interface designed to connect subscriber terminals known as *User Equipment (UE)* to the

This research was supported in part by the US AFOSR/MURI project # FA9550-10-1-0573 and ARO project # W911NF-09-1-0553.

network interface known as *eNode B* [1]. Here, we mainly focus on *Frequency Division Duplexing (FDD)* networks. An *LTE* network can be divided into *Downlink (DL)* and *Uplink (UL)* depending on the direction of data transfer, each occupying bandwidths of up to 20 MHz and configured into 10-ms long frames.

An *LTE* network broadcasts *System Information (SI)* in *Resource Blocks (RB)* on the *Physical Broadcast Channel (PBCH)* and *Physical Downlink Shared Channel (PDSCH)* and notifies UEs of its validity and changes. A UE applies SI acquisition upon either power on/selecting a cell; reselecting to a cell; after handover completion; after entering *Evolved Universal Terrestrial Radio Access (E-UTRA)* from another *Radio Access Technology (RAT)*; return from out of coverage; or receiving a notification that SI has changed [1], [16]. When powered on or after finding a suitable cell from *Out-of-Service (OOS)*, a UE must first send an *attach request* to the network before transitioning to the *Radio Resource Control (RRC) Idle* state. Also, a UE must transition to *Radio Resource Control (RRC) Connected* state before it can make any data transfer. Moreover, a typical *LTE* network usually transitions the UEs in *Connected* state to *Idle* state after a little dormancy so that it can utilize its resources more efficiently and reduce interference. Hence, UEs need to establish RRC connection on a regular basis. When a UE powers on or finds coverage after being *OOS* it first decodes *Sync Signals PSS/SSS* to get *System Frame Number (SFN)*/subframe boundaries, then decodes PBCH to get *Master Information Block (MIB)* (Bandwidth, SFN, PHICH-config), then decodes PDSCH to get *System Information Block (SIB) 1* (cell suitability, PLMN, cell access info, scheduling of other SIBs), then decodes PDSCH to get *SIB 2* (paging, PRACH, BCCH, PDSCH, PUSCH, PUCCH scheduling). At this point a UE can send an *attach request* on *Physical Random Access Channel (PRACH)/Physical Uplink Control Channel (PUCCH)* to *camp* on the network and finally completes SI acquisition by decoding PDSCH to get *SIB 3* (cell reselection), *SIB 4-8* (neighbor info) and *SIB 9* (home eNode B) [1], [16].

During Downlink data transfer, a UE first decodes *Physical Control Format Indicator Channel (PCFICH)* to get *Physical Downlink Control Channel (PDCCH)-config*, then decodes PDCCH to get *DL Control Information (DCI)* and resource assignments in PDSCH, then finally decodes PDSCH to get DL data and sends ACK/NAK on PUCCH/PUSCH [1], [16]. Similarly, if a UE wants to send data on Uplink, it first sends initial access and UL sync requests on PRACH, then sends *UL Control Information (UCI)* on PUCCH/PRACH to eNode B scheduler. In response eNode B sends UL resource assignments on PDCCH and UE sends UL data, *Buffer Status Report (BSR)* and *Power Headroom (PHR)* on *Physical Uplink Shared Channel (PUSCH)*. eNode B completes data transfer by sending ACK/NAK on *Physical Hybrid ARQ Indicator Channel (PHICH)* [1], [16].

Further, if a UE is unable to receive *Cell-Specific Reference Signal (CS-RS)* reliably ($\leq 2\%$) for 5-10 *Discontinuous Reception (DRX)* cycles then it goes *out-of-sync* [16].

B. Some Possible Jamming Attacks on an LTE Network

A wireless jammer can be classified as either a *barrage jammer*, *pulse jammer*, *partial-band jammer*, *single-tone/multi-tone jammer* or a *smart jammer* based on its jamming technique. A *smart jammer* can "learn" the network timing and physical layer parameters to jam more effectively. Since *LTE* is a commercially deployed network, an *LTE*-capable UE can easily learn the network timing and synchronize itself with the network without even sending an *attach request*. If an *LTE*-capable UE colludes with a simple yet reconfigurable narrowband jammer then such a collusion may result in a *smart jammer*. A typical UE spends most of its time in *RRC Idle* state and transitions to *RRC Connected* state only when it needs to send/receive some data. Also, it cannot remain in *RRC Connected* state indefinitely in order not to waste network resources and battery life. If a jammer somehow blocks the transition of existing UEs in the cell to *RRC Connected* state or prevents incoming UEs from transitioning to the cell or increases the rate of *Radio Link Failures (RLFs)* significantly then it can launch effective *DOS* attacks. This task can be accomplished by a *smart jammer* by jamming common control channels and *OFDM pilot symbols* (known as *Cell-Specific Reference Signal (CS-RS)* in *LTE*).

A power-limited *smart jammer* may jam specific critical control channels instead of jamming the entire network bandwidth in order to initiate *DOS* or loss of service attacks. All of the required frequency and timing information for these channels is broadcasted by the network as per *3GPP* specifications so that all incoming UEs can easily "learn", synchronize and attach to the network. Hence, a *smart jammer* does not need to "infiltrate" the network in order to "learn" its configuration. It may transmit an unknown jamming signal at specific time and frequency resources to jam the following common control and broadcast channels:

- Cell-Specific Reference Signal (CS-RS)
- Physical Broadcast Channel (PBCH)
- Physical Control Format Indicator Channel (PCFICH)
- Physical Uplink Control Channel (PUCCH)
- Physical Random Access Channel (PRACH)

Jamming *CS-RS* may prevent users from demodulating the data channels, degrade *cell quality* measurements for cell reselection and handover, and block initial cell acquisition. This jamming technique can be applied to any pilot-based OFDM network, such as *LTE, IEEE 802.11g, WiMAX* etc. [11]. Jamming PCFICH may cause loss of *Control Format Indicator (CFI)* in the Downlink. *CFI* indicates the control region associated with PDCCH which carries all essential control information and grants associated with both Uplink and Downlink. A UE may attempt blind CFI decoding but it could be too slow resulting in missed grants which might force the network to declare RLF or UE might go *out-of-sync*. Jamming PUCCH may cause eNode B to loose track of critical feedback information from UEs. Jamming PBCH and PRACH may block reselection and handover of UEs from neighboring cells to the jammed cell, and may also block *out-of-sync* and Idle mode UEs in the jammed cell to get Uplink synchronized and transition to *Connected* state, respectively. Since PRACH is assumed to be contention-based for initial access and synchronization, we assume that a fraction of UEs try to access it at any given resource instant. If the jammer's signal is received by the eNode B along with other legitimate users, it will need to perform contention resolution which may fail because of jammer being present. Hence, the jammer only needs to make sure that its signal is received with high enough power at the eNode B receiver.

C. Suggested Network Countermeasures against Jamming

Network operators rely on the intervention of skilled network engineers triggered by poor network statistics to rectify jamming and interference problems. However, a *smart jammer* can go undetected by network engineers if it keeps changing its location frequently in a random manner and launches jamming attacks probabilistically. In the event of incomplete jamming information available by the network, we propose that an *LTE* network can take the following countermeasures:

- Increase CS-RS Transmit Power (*Pilot boosting*)
- Throttle All UEs' Throughput (*threat mechanism*)
- Change eNode B Frequency
- Change eNode B Timing
- Change SIB 2 (*PRACH and PUCCH config*)

eNode B may increase CS-RS transmit power at the expense of other DL channels that may help against CS-RS jamming, which is probably the most important signal in the network. It may also throttle all active users' throughput in the fear of a jamming attack. This countermeasure may be used as a threat against a user who is trying to "cheat" the network for its own benefits. eNode B may also "relocate" its center frequency and move all of its active UEs to different channels chosen randomly within its allocated spectrum, hence, moving PSS/SSS and PBCH to another frequency. *LTE* networks have the flexibility of occupying bandwidths ranging from 1.4 MHz to 20 MHz. A 20-MHz network can reconfigure itself into a 15-MHz or less bandwidth network while operating in its allocated spectrum. This may help combat jamming of critical control channels at the expense of reduced operating bandwidth and excessive overhead required to move all active data sessions to new frequencies. Further, the eNode B may also change its frame, slot and symbol timing after it forcefully hands over all the UEs with active data sessions to neighboring cells. The Idle mode UEs would autonomously reselect to neighboring cells. After the change is made, all the UEs may transition back to the original cell. Since all the control channels are transmitted at specific time and frequency resources, this countermeasure may help alleviate control channel jamming by moving it to data channels like PDSCH or PUSCH. However this would require very carefully planned reconfiguration at the network side and the cell would not be available during the transition period. Moreover, SIB 2 parameters' change may prevent PRACH and PUCCH failures caused by jamming.

III. Game-Theoretic Modeling of Smart Jamming

We model the *smart jammer* as a combination of a *colluding UE* and a re-configurable *narrowband jammer*. We classify potential *network adversaries* into two categories:

1) **Cheater**
2) **Saboteur**

A *Cheater* jams the network with the intent of getting more resources for itself as a result of reduced competition among UEs. Thus a *Cheating UE* is always present in the network with an active data session. On the other hand, a *Saboteur* jams the network with the intent of causing highest possible damage to the network resources. Thus a *Sabotaging UE* may not have any interest in getting more network resources and may even be unattached to the network. We assume that the *colluding UE* and *narrowband jammer* are not necessarily co-located and the *colluding UE* has the capability of canceling the interference caused by the *narrowband jammer* because of their collusion. We model these network dynamics as *competitive games*. Here, we define a *competitive game* as a non-cooperative game [17] in which unilateral changes in a player's actions do not result in bilateral utility improvement with the exception of dominated strategies.

A. Single-Shot Game

In the *single-shot game*, a *smart jammer* infringes on regular network communication by playing one of the following actions. Since jammer is power and resource limited, it tries to jam as few control channels as possible while maximizing its *utility*.

1) *Inactive*
2) *Jam CS-RS*
3) *Jam CS-RS + PUCCH*
4) *Jam CS-RS + PBCH + PRACH*
5) *Jam CS-RS + PCFICH + PUCCH + PRACH*

Here, *Inactive* refers to the scenario when jamming is not performed hence normal network operations may continue. A *smart jammer* might cause more damage to the network performance by jamming multiple channels in a given frame with no additional power requirements. However, it would need to distribute its transmit power among multiple channels and transmit both in the Uplink and Downlink to achieve its goals.

The eNode B counteracts as a result of jammer's infraction and plays one of the following actions as described earlier:

1) *Normal*
2) *Increase CS-RS Transmit Power*
3) *Throttle All UEs' Throughput*
4) *Change eNode B Frequency + SIB 2*
5) *Change eNode B Timing*

These are modeled as two-player matrix games with eNode B as the row player and adversary as the column player. As per famous *Nash's existence theorem* every finite strategic game has a mixed strategy *Nash Equilibrium (NE)* [17]. Players do not get any improvement in their utilities by moving unilaterally from a NE.

B. Single-Shot Game Simulation

We assume that UEs arrive in the cell according to a *homogeneous 2D Stationary Spatial Poisson Point Process (SPPP)* with the rate λ per unit area and a fraction of them are in active data session with eNode B. UEs are *uniformly distributed* over the entire cell conditioned on total number of users *N*. Jammer keeps changing its location randomly on a regular basis and launches jamming attacks probabilistically in order to escape detection by the network. We assume that UEs have little or no mobility but total number of UEs in the cell and, hence, their locations keep changing on regular basis albeit at a rate much slower than jammer hopping. All transmit signals go though large-scale path loss modeled using *Simplified Path Loss Model* [18] as $P_r = P_t K d^{-\gamma}$ where P_r is the received power, P_t is the transmitted power, $K(dB) = 20log_{10}\left(\frac{\lambda}{4\pi d_0}\right)$ is a constant and γ is called *path loss exponent* with typical values from 2.7 - 3.5 for urban microcells. We model SINR Γ at a particular receiver (either a UE or the eNode B) as follows:

$$\Gamma = \frac{P_0 |h_0|^2 R_0^{-\gamma}}{\sigma^2 + P_J |h_J|^2 R_J^{-\gamma}} \tag{1}$$

where P_0 and P_J are transmit powers, $|h_0|^2$ and $|h_J|^2$ are *exponentially distributed* channel gains caused by small-scale *Rayleigh fading*, R_0 and R_J are corresponding large-scale distances from desired transmitter and jammer respectively, γ is the path loss exponent and σ^2 is the noise variance at the receiver. We assume that noise variance remains the same at all the receivers for simplification purposes.

It is widely known that fading channel's capacity is modeled as a fraction of AWGN channel capacity [18]. Since *LTE* data channels operate very close to *Shannon Capacity* at high data rates and *smart jamming* does not target data channels, we assume that *DL PDSCH Throughput* $\mathcal{R}_{PDSCH}$ scheduled over $\mathcal{B}_{PDSCH}$ *resource blocks* can be modeled as *Shannon's AWGN Channel Capacity* as a first-order approximation i.e.

$$\mathcal{R}_{PDSCH} = \mathcal{B}_{PDSCH} log_2(1 + \Gamma_{PDSCH}) \tag{2}$$

We also assume that both eNode B and UE are unable to decode control channels below a certain *Block Error Rate (BLER)* threshold and failure to decode these critical control channels would result in declaring *Radio Link Failure (RLF)* or very poor performance of data channels' decode and missed grants. For uncoded signals like CS-RS we use well-known closed form expression for QPSK *Symbol Error Rate (SER) performance in Rayleigh fading* [18] in order to convert desired BLER performance threshold into required average SINR i.e. $\bar{P}_s = \left(1 - \sqrt{\frac{\bar{\gamma_s}/2}{1+\bar{\gamma_s}/2}}\right)$ (where $\bar{P}_s$ = avg. QPSK symbol error prob. in Rayleigh fading, and $\bar{\gamma_s}$ = avg. SNR per symbol). For coded signals like PBCH, PCFICH, and PUCCH there are no closed form expressions available for coded PSK performance in Rayleigh fading. So we use a combination of the *Union Bound for coded PSK symbol error probability* [19] i.e. $P_M < 2^k \binom{2d_{min}-1}{d_{min}} \left(\frac{1}{4R_c\bar{\gamma_b}}\right)^{d_{min}}$ (where P_M = coded M-PSK symbol error prob., $M = 2^k$, R_c = code rate, d_{min} = minimum distance of channel code and $\bar{\gamma_b}$ = avg. SNR per bit). Channel code's *free distance* d_{free} is derived from 3GPP *LTE* specifications [1] assuming equally likely symbol error probability across entire block of a particular signal in order to convert desired BLER performance into required average SINR.

We propose that eNode B uses *Proportional Fair Scheduling (PFS)* [18] algorithm to assign resources to its users that survive jamming attacks. PFS provides a good balance between eNode B throughput performance and fairness among users. Players' *utilities* are calculated as normalized improvement (or degradation) over *baseline jamming-free* scenario. The *eNode B Utility Function* is computed as:

$$\mathcal{U}_{eNB} = \mathcal{R}_{eNB} - \mathcal{Q}_{eNB} \tag{3}$$

where $\mathcal{U}$, $\mathcal{R}$ and $\mathcal{Q}$ denote *utility, reward* and *penalty* functions respectively. They are computed for *eNode B* as follows:

$$\mathcal{R}_{eNB} = \alpha_r \bar{R}_{eNB}^{dB_{norm}} + \alpha_m \bar{M}_{eNB}^{dB_{norm}} + \alpha_{rs} \Delta\bar{\Gamma}_{rs}^{dB} + \alpha_{uc} \Delta\bar{\Gamma}_{uc}^{dB} \tag{4}$$

$$\mathcal{Q}_{eNB} = \beta_{ra} \bar{\Psi}_{ra_{fail}} + \mathcal{C}_{fixed} \tag{5}$$

where $\bar{R}$, $\bar{M}$, $\bar{\Gamma}_{rs}$, $\bar{\Gamma}_{uc}$, and $\bar{\Psi}_{ra_{fail}}$ denote normalized averages of total throughput, number of active users, CS-RS SNR, PUCCH SNR, and PRACH failure rate respectively, and α and β are their corresponding assigned weights used for utility computation. Whereas, $\mathcal{C}_{fixed}$ denote fixed costs associated with a particular eNode B action. Similarly, the adversaries' utilities are computed as follows:

$$\mathcal{U}_c = \alpha_r \bar{R}_c^{dB_{norm}} - \beta_\tau \bar{\tau}_c \tag{6}$$

$$\mathcal{U}_s = -\alpha_r \bar{R}_{eNB}^{dB_{norm}} - \alpha_m \bar{M}_{eNB}^{dB_{norm}} - \beta_\tau \bar{\tau}_s \tag{7}$$

where $\bar{\tau}_c$, and $\bar{\tau}_s$ denote average duty cycle of *Cheater* and *Saboteur* respectively. The two cases will be dealt separately due to differences in their utility computation.

C. Single-Shot Game Simulation Results

We chose the following simulation parameters based on their anticipated significance: $\alpha_r = 50$, $\alpha_m = 80$, $\alpha_{rs} = 10$, $\alpha_{uc} = 8$, $\beta_{ra} = 25$, $\beta_\tau = 25$, $\mathcal{C}^{rs} = 20$, $\mathcal{C}^{\text{throttle}} = 0$, $\mathcal{C}^{\text{f Change}} = 50$, $\mathcal{C}^{\text{T Change}} = 80$, $\textit{BLER}_{\text{threshold}} = 10\%$, $C/J = 20$ dB and $p_J = 0.7$, where C/J, and p_J denote *carrier-to-jammer power ratio* and *probability of jamming* respectively. The utility results obtained from our simulations are tabulated below in the form of *two-player matrix games* with the network being the *row player* and the adversary being the *column player*. The $\mathcal{U}_{eNB,c}$ utility matrix is:

$$- \begin{bmatrix} 0,0 & 190,-10 & \textbf{526,-260} & 180,3 & \textbf{520,-260} \\ 4,14 & 180,3 & 528,-245 & 172,15 & 526,-251 \\ 431,431 & 642,431 & 1118,443 & 629,441 & 1116,442 \\ 84,57 & 282,47 & 620,-199 & 273,59 & 618,-199 \\ 80,0 & 270,-10 & 606,-260 & 260,3 & 600,-260 \end{bmatrix}$$

Similarly, $\mathcal{U}_{eNB,s}$ utility matrix is:

$$-\begin{bmatrix} 0,0 & 193,-40 & 539,-226 & 183,-22 & 532,-220 \\ 4,-14 & 182,-39 & 541,-238 & 175,-24 & 539,-236 \\ 431,-431 & 646,-492 & 1134,-821 & 633,-471 & 1132,-820 \\ 84,-57 & 88,-53 & 88,-35 & 91,-45 & 88,-36 \\ \mathbf{80,0} & \mathbf{84,3} & 83,22 & 87,11 & 84,21 \end{bmatrix}$$

In case of **Cheater**, game has two *pure strategy NE* at *(Normal, Jam CS-RS + PUCCH)* and *(Normal, Jam CS-RS + PCFICH + PUCCH + PRACH)* with an expected payoff of **(-526,260)** and **(-520,260)** respectively. Whereas, in case of **Saboteur**, game has *mixed strategy NE* with expected payoff of **(-81.32,0.68)**. This mixed strategy NE corresponds to assigning probability distribution of *(0.04,0.05,0,0,0.91)* and *(0.67,0.28,0,0,0.05)* to the network and saboteur actions respectively. This can be loosely translated to *(Change Timing, Inactive)* and *(Change Timing, Jam CS-RS) pure strategy NE*. Thus, the **network's utility is severely compromised in case of a jamming attack** evident from its very low (negative) utility values. Also, some network actions are strictly dominated against a particular type of adversary, e.g., *f Change* and *Timing Change* against *Cheater*. Hence, the **network strategy may depend on adversary action as well as its type.** Similar trends are observed at other values of C/J and p_J.

D. Repeated Bayesian Game with Incomplete and Asymmetric Information

Since single-shot games are less appealing from convergence and implementation point of view, we turn our attention to *repeated Bayesian games* [17]. Also, *repeated games* can potentially provide us further opportunities for improving network utility by learning and utilizing game dynamics. We propose a *repeated game algorithm* for the network and the adversaries. All of the measurements and actions required by our algorithm are within the capabilities of both the network and the adversaries without changing *LTE* technology significantly. In other words, they are practically implementable in current *LTE* networks with minor changes.

E. Proposed Repeated Game Learning and Strategy Algorithm

We assume that a certain probability of occurrence is associated with each adversary, and at most only one type of adversary can be present in the network with the network being jamming-free most of the time. Adversaries with dual or mixed *personality types* are beyond the scope of this paper. Based on single-shot game simulation results, the network's *best response* depends on the type of adversary. Hence, it is very important for the network to determine the type of jamming adversary if detected. We propose the algorithm in Fig. 1 for the network to determine the jammer type. The network uses its long-run baseline parameter values such as *average CS-RS SNR* and *average PUCCH SNR*, collected as a result of its learning and feedback from UEs to decide if jamming is in effect. Here p_{false}, *Throttling Test*, and *f Change Test* refers to *false alarm probability*, *playing 'Throttle'* and *playing 'Change f'* for few consecutive frames respectively. After jammer type determination, eNode B uses the algorithm proposed in Fig. 2 to counteract jamming attacks. If no jammer is detected by eNode B, it will keep playing *'Normal'*. Here p_{high} refers to *high probability* and *'throttling duration'* refers to the parameter describing number of consecutive frames for which this action is played. Note that eNode B merely forms an estimate of jammer type which may or may not represent the true state. Also the proposed actions' algorithm forms beliefs about network state and adversary's actions based on its measurements and may not always be true as well. This phenomenon is typical for a stochastic environment with incomplete information.

Fig. 1. Proposed Algorithm for eNode B Jammer Type Determination

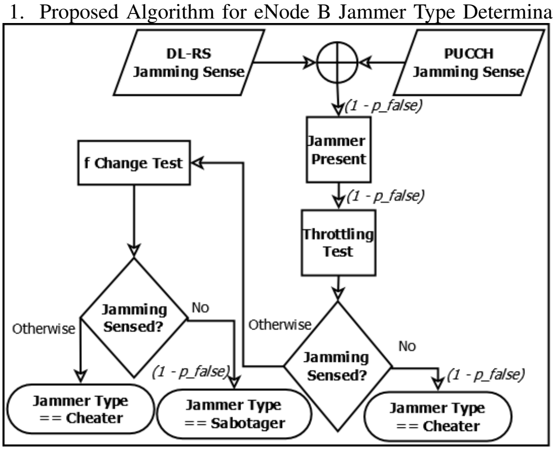
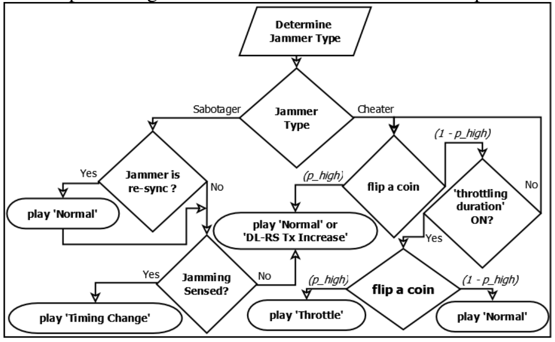


Fig. 2. Proposed Algorithm for eNode B's Actions in Repeated Game



Similarly, *Cheater* and *Saboteur* devise their own corresponding strategy for the repeated game. Their proposed strategy is shown in Figs. 3 and 4, respectively. Similar to eNode B, adversaries are also unaware of network state and actions and, hence, can only form an estimate based on their own capabilities and measurements. *Saboteur* is naturally limited in this regard, since it does not have access to dynamic resource allocation of eNode B and can be kept in dark by the network. Therefore, *Saboteur* keeps re-synchronizing itself with the network on regular intervals denoted by $period_J$ in Fig. 4. On the other hand, *Cheater* might be able to estimate network actions more accurately and can act accordingly. It forms its own *baseline* during the "observation" *(inactive)* period so that future network behavior can be interpreted in terms of eNode B actions. In addition, jammers use a probability distribution over frames to jam the network randomly in order to escape detection by the network.

Fig. 3. Proposed Algorithm for Cheater's Actions in Repeated Game

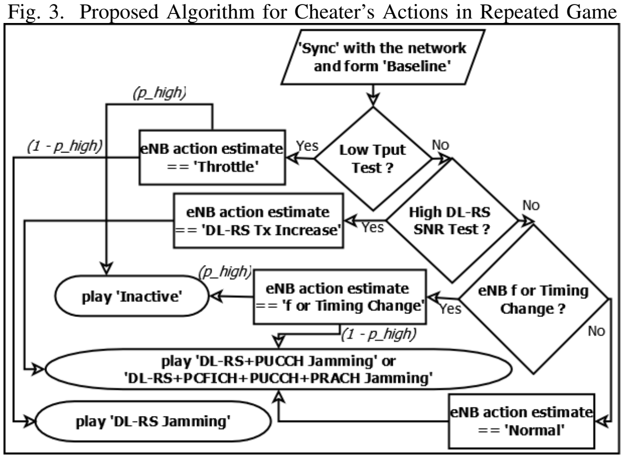
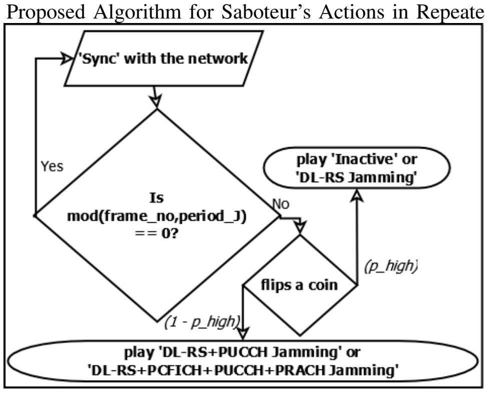

'Sync' with the network and form 'Baseline'
(p_high)
(1 - p_high)
eNB action estimate == 'Throttle'
Yes
Low Tput Test ?
No
eNB action estimate == 'DL-RS Tx Increase'
Yes
High DL-RS SNR Test ?
No
(p_high)
play 'Inactive'
eNB action estimate == 'f or Timing Change'
Yes
eNB f or Timing Change ?
No
(1 - p_high)
play 'DL-RS+PUCCH Jamming' or 'DL-RS+PCFICH+PUCCH+PRACH Jamming'
play 'DL-RS Jamming'
eNB action estimate == 'Normal'

Fig. 4. Proposed Algorithm for Saboteur's Actions in Repeated Game


'Sync' with the network
Yes
Is mod(frame_no,period_J) == 0?
No
play 'Inactive' or 'DL-RS Jamming'
(p_high)
flips a coin
(1 - p_high)
play 'DL-RS+PUCCH Jamming' or 'DL-RS+PCFICH+PUCCH+PRACH Jamming'

F. Proposed Repeated Bayesian Game Simulation Results

We used the same parameters as single-shot case with following frequency of jammer occurrence: $f_c = 9.33\%$, and $f_s = 5.67\%$. As a result, we get following ***repeated game utility*** values: $\mathcal{U}^{\mathbf{repeated}}_{\mathbf{eNB}} = \mathbf{-23.2}$, $\mathcal{U}_c^{repeated} = 466.2$, and $\mathcal{U}_s^{repeated} = -511.3$. The corresponding ***single-shot utility*** at NE would be $\mathcal{U}_{eNB}^{single} = (-523)f_c + (-81.3)f_s = -53.4$. Evidently, eNode B enjoys 57% relative improvement in its utility when using *proposed repeated game algorithm* as compared to playing *best response* in single-shot scenario.

G. A Brief Discussion on Simulation Results

Based on our simulation results it becomes clear that the network can improve its utility significantly by using our proposed algorithm in case of an attack. In a single-shot game network may not have enough information and leverage against adversaries, whereas it can learn jammer type and use threats against them in a repeated game. Similarly, *Cheater* can also improve its utility as a consequence of repeated game formulation. Also, our proposed *jammer type determination algorithm* is quite robust for various jammer types based on their expected behavior. It is to be noted here that our simulation results are probabilistic in nature and only long-term averages are reported above.

IV. Conclusion

We showed that *LTE* networks are vulnerable to *denial-of-service (DOS)* and *loss of service* attacks from *smart jammers* even if the jammers are resource-constrained. An adversary can easily launch these network-wide jamming attacks with the help of a *smart jammer*. As a result, the network suffers significant performance loss and may not be able to recover itself using current protocols. However, if our proposed *repeated game learning and strategy algorithm* is used by the network, it can recover most of its performance loss and may even force an adversary to retract. In the future, we intend to study the effects of *smart jamming* on a multi-cell configuration.

References

[1] 3rd Generation Partnership Project (3GPP): Technical Specifications; LTE (Evolved UTRA) and LTE-Advanced Radio Technology Series (Rel 11) [Online]. Available: http://www.3gpp.org/DynaReport/36-series.htm

[2] R. Ferrús, O. Sallent, G. Baldini, and L. Goratti, "LTE: The technology driver for future Public Safety communications," *IEEE Comm. Magazine,* vol. 51, no. 10, pp. 154-161, Oct. 2013.

[3] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, "LTE for Public Safety networks," *IEEE Comm. Magazine,* vol. 51, no. 2, pp. 106-112, Feb. 2013.

[4] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for Smart Grid applications," presented at the 2010 IEEE Power and Energy Society General Meeting, pp. 1-7.

[5] Z. Feng, L. Jianming, H. Dan, and Z. Yuexia, "Study on the application of advanced broadband wireless mobile communication technology in Smart Grid," in *Proc. 2010 Int. Conf. on POWERCON.*

[6] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the Smart Grid," in *Proc. 2010 IEEE MILCOM,* pp. 1830-1835.

[7] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Comm. Surveys & Tutorials,* vol. 16, no. 1, pp. 283-302, 1st Quarter, 2014.

[8] Y. Park, and T. Park, "A survey of security threats on 4G networks," in *Proc. 2007 IEEE Globecom Workshops,* pp. 1-6.

[9] A. Asterjadhi, R. Kumar, T. La Porta, and M. Zorzi, "Broadcasting in multi channel wireless networks in the presence of adversaries," in *Proc. 2011 8th Annual IEEE ComSoc Conf. on SECON,* pp. 377-385.

[10] C. Pöpper, M. Strasser, and S. Čapkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Comm.,* vol. 28, no. 5, pp. 703-715, Jun. 2010.

[11] C. S. Patel, G. L. Stüber, and T. G. Pratt, "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming," in *Proc. 2004 IEEE WCNC,* pp. 954-958.

[12] D. J. Thuente, and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. 2006 IEEE MILCOM.*

[13] S. Liu, L. Lazos, and M. Krunz, "Thwarting control-channel jamming attacks from inside jammers," *IEEE Trans. on Mobile Computing,* vol. 11, no. 9, pp. 1545-1558, Sep. 2012.

[14] M. Petracca, M. Vari, F. Vatalaro, and G. Lubello, "Performance evaluation of GSM robustness against smart jamming attacks," in *Proc. 2012 5th Int. Symp. on ISCCSP,* pp. 1-6.

[15] J. H. Reed, "Comments of Wireless @ Virginia Tech in the matter of NTIA development of the nationwide interoperable Public Safety broadband network," Virginia Tech, Blacksburg, VA, November 2012.

[16] S. Sesia, I. Toufik, and M. Baker (Eds.), *LTE - The UMTS Long Term Evolution: From Theory to Practice.* (2nd ed.) West Sussex, UK: Wiley, 2011.

[17] M. J. Osborne, and A. Rubinstein, *A Course in Game Theory.* Cambridge: The MIT Press, 1994.

[18] A. Goldsmith, *Wireless Communications.* New York: Cambridge University Press, 2005.

[19] J. Proakis, *Digital Communications.* (4th ed.) New York: McGraw-Hill, 2000.