Jammer Type Estimation in LTE with a Smart Jammer Repeated Game

Farhan M. Aziz, *Student Member, IEEE,* Jeff S. Shamma, *Fellow, IEEE,* and Gordon L. Stüber, *Fellow, IEEE*

***Abstract*—LTE/LTE-Advanced networks are known to be vulnerable to denial-of-service (DOS) and loss-of-service attacks from smart jammers. The interaction between the network and the smart jammer has been modeled as an infinite-horizon general-sum (non-zero-sum) Bayesian game with asymmetric information, with the network being the uninformed player. Although significant work has been done on optimal strategy computation and control of information revelation of the informed player in repeated asymmetric information games, it has been limited to zero-sum games with perfect monitoring. Recent progress on the strategy computation of the uninformed player is also limited to zero-sum games with perfect monitoring and is focused on expected payoff formulations. Since the proposed formulation is a general-sum game with imperfect monitoring, existing formulations cannot be leveraged for estimating true state of nature (the jammer type). Hence, a threat-based mechanism is proposed for the uninformed player (the network) to estimate the informed player's type (jammer type). The proposed mechanism helps the network resolve uncertainty about the state of nature (jammer type) so that it can compute a repeated-game strategy conditioned on its estimate. The proposed algorithm does not rely on the commonly assumed "full monitoring" premise, and uses a combination of threat-based mechanism and non-parametric estimation to estimate the jammer type. In addition, it does not require any explicit feedback from the network users nor does it rely on a specific distribution (e.g., Gaussian) of test statistic. It is shown that the proposed algorithm's estimation performance is quite robust under realistic modeling and observational constraints despite all the aforementioned challenges.**

***Index Terms*—LTE/LTE-A; smart jamming; Bayesian games with asymmetric information; threat-based mechanism; non-parametric estimation.**

I. Introduction

LONG Term Evolution (LTE) and LTE-Advanced (LTE-A) (cf. [1], [2]), networks have been providing advanced data, Voice-over-IP (VoIP), multimedia and location-based services to more than 1.4 billion subscribers in 170 countries around the world, cf. [3]. However, it has been shown that LTE networks are vulnerable to control-channel jamming attacks from *smart jammers* who can "learn" network parameters and "synchronize" themselves with the network even when they are not attached to it (cf. [4] - [10]). It is shown in the above-referenced articles that such a *smart jammer* can launch very effective *denial-of-service (DOS)* and *loss of service* attacks without even hacking the network or its components. Hence, pursuing autonomous techniques to address this potentially devastating problem has become an active research topic.

Game theory (cf. [11] - [15]) provides a rich set of mathematical tools to analyze and address conflict and cooperation scenarios in multi-player situations, and as such has been applied to a multitude of real-world situations in economics, biology, cyber security, multi-agent networks, wireless networks (cf. [16] - [18]) and more. The interaction between the LTE network and the smart jammer has been modeled as an infinite-horizon general-sum (non-zero-sum) Bayesian game with asymmetric information (cf. [7], [9]), with the network being the uninformed player. Asymmetric information games (cf. [12] - [15]) provide a rich framework to model situations in which one player lacks complete knowledge about the "state of nature". The player who possesses complete knowledge about the state of nature is known as the informed player and the one who lacks this knowledge is called the uninformed player. The informed player deals with the ultimate tradeoff of exploiting its superior information at the cost of revealing such information via its actions or some other (unavoidable) signals during repeated interactions with the uninformed player (cf. [12], [13]). In most game-theoretic literature on repeated games with asymmetric information, the informed player's strategy is computed based on how much information it should reveal for an optimal or suboptimal policy. Furthermore, many informed player zero-sum formulations model the uninformed player as a Bayesian player in order to solve asymmetric games (cf. [19] - [22]). However, relatively little work has been done to address the optimal strategy computation of the uninformed player in an infinite-horizon repeated zero-sum game with asymmetric information (cf. [23]). The main difficulty arises from the fact that the uninformed player lacks complete knowledge about the state of nature and informed player's belief state, which plays a crucial role in determining players' payoffs and strategies. This probelm gets further complicated for general-sum (non-zero-sum) games with imperfect monitoring, which is still an open problem (cf. [24]). This paper addresses the lack of information problem, in the infinite-horizon general-sum repeated game with imperfect monitoring by proposing a state estimation algorithm, hence, resolving the uncertainty for the uninformed player.

A. Rationale

The *smart jamming* (cf. [4] - [10]) problem in LTE/LTE-A networks has been previously modeled by the authors

F. M. Aziz and G. L. Stüber are with the Wireless Systems Laboratory (WSL), School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332, USA. E-mail: {faziz,stuber}@ece.gatech.edu.

J. S. Shamma is with the RISC Lab, Computer, Electrical and Mathematical Science and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia. E-mail: jeff.shamma@kaust.edu.sa.

Manuscript received XXX, XX, 2016; revised XXX, XX, 2016.

as an infinite-horizon general-sum (non-zero-sum) repeated Bayesian game with asymmetric information (cf. [7], [9]) in which the jammer has multiple types. The information asymmetry in the above-mentioned game is induced by the fact that the network is unaware of the arriving jammer type. At the beginning of the game, nature selects a jammer type from a finite set according to a common prior probability distribution. The jammer is informed of its type but the network is not. This situation leads to *asymmetric information* or *lack of information on one side* problem (cf. [12] - [15]), with the network and the jammer being the uninformed and informed players respectively. The LTE network can combat *smart jamming* attacks autonomously by employing the repeated game algorithms proposed in [7] and [9]. However, these network strategy algorithms are contingent upon a specific jammer type. Hence, a jammer type estimation algorithm is proposed in this article which is based on the threat mechanism in repeated games. The proposed algorithm neither requires any feedback from the network users nor does it rely on a specific distribution (e.g., Gaussian) of test statistic and is implemented without any notion of "full monitoring" (i.e., players cannot observe opponent's actions).

B. Related Work

Game-theoretic tools have been applied to model the interaction between the LTE network and the *smart jammer*. The authors have previously proposed network's repeated game strategies (cf. [7], [9]) to combat smart jamming attacks but they were contingent upon the type of adversary being faced. Threat and punishment based mechanisms are often used in non-cooperative game theory to induce cooperation and devise strategies to arrive at equilibria other than the minmax payoff equilibrium (cf. [11], [12]). The *threat-based state estimation algorithm* proposed in this article is utilized by the network to estimate the jammer type. This proposed algorithm is designed such that it does not rely on feedback from network users nor on a specific distribution (e.g. Gaussian) of test statistic prompting us to use non-parametric estimation. Furthermore, it does not require any "full monitoring".

Traditionally, zero-sum formulations have been studied extensively in the game-theoretic literature concerning asymmetric information repeated games, such as, Chapter 5 of [12], Chapter 4 of [13], Chapters 2 - 4 of [14], and Chapter 2 of [25]. However, most of the prior work on asymmetric zero-sum repeated games revolves around the informed player's viewpoint. For example, [12] and [13] pointed out that the informed player might reveal its superior information implicitly by its actions and, hence, may want to refrain from certain actions in order not to reveal that information. Furthermore, [14] showed that the informed player's belief state (conditional probability of the game being played given history of informed player's actions) is his sufficient statistics to make long-run decisions. Moreover, [26] showed that computing the optimal value of the infinite-horizon repeated game is non-convex, identifying computational complexities involved in solving infinite-horizon games. Hence, many informed player's strategies (cf. [19] - [22]) presented in the game-theoretic literature use the belief state as their sufficient statistics and approximate the optimal game value via linear programming. However, compared to the vast research work done on the informed player, limited work has been done for the uninformed player's optimal strategy computation [23]. It is, however, known that the uninformed player's security strategy exists in infinite-horizon repeated zero-sum games, and that it does not depend on the history of his own actions (cf. [22], [27]). The uninformed player's sufficient statistics and computation of his optimal security strategy still are open problems. Recently, [23] suggested that the uninformed player could use expected payoff for each candidate game as his sufficient statistics, as he is unaware of the game being played due to lack of information. Similarly, [22] used realized vector payoff as the uninformed player's sufficient statistics to compute its efficient but suboptimal strategy in finite-horizon asymmetric zero-sum repeated games. However, all of these formulations are based on "perfect monitoring" in which players can perfectly observe their opponent's actions.

Most of the classic general-sum (non-zero-sum) game-theoretic literature like Chapter 6 of [12] and Chapters V and IX of [15] focus on the characterization and existence of equilibria in repeated games with asymmetric information, and deal with the optimal strategy construction for the "full monitoring" case (when both players can observe each other's actions after every stage). Chapter V of [15] also suggests using *approachability theory* for the construction of the uninformed player's strategy for the "full monitoring" case. However, none of these formulations result in efficient computation of the uninformed player's optimal strategy. Furthermore, in our case the "full monitoring" assumption is not realistic since both the network (the uninformed player) and the jammer (the informed player) cannot observe their opponent's actions with certainty. Moreover, [24] pointed out that the solution of a stochastic game with both incomplete knowledge and imperfect monitoring is an open problem and there is no well-established solution available so far. To the best of our knowledge, this is still the case for repeated as well as stochastic games and, hence, characterization of the equilibrium as well as the computation of optimal strategies are beyond the scope of this paper.

Bayesian approaches have also been widely used to solve asymmetric information problems in game-theoretic literature. They are used as a tool for updating the internal notion of a player's knowledge related to another. For example, [19] - [21] modeled the uninformed player as a Bayesian player in order to compute the informed player's suboptimal strategies efficiently in repeated zero-sum games. Similarly, [28] - [30] used a Bayesian approach to devise an uninformed player's strategy based on expected payoff. Similarly, [24] employed Bayesian Nash-Q learning in an incomplete information stochastic game and used Bayes' formula to update belief of an Intrusion Detection System (IDS), but it assumes that players can observe their opponent's actions (full monitoring) and quality functions. However, Bayesian approaches are rather useful for devising strategies based on expected payoffs, not for estimating the opponent's type. Another technique used to address lack of information problems is state estimation. For

example, [31] used a Kalman filter to estimate the state of an observable, linear, stochastic dynamic system in an infrastructure security game. Since, our system of interest is nonlinear and may not be completely-observable, applicability of these techniques is also very limited.

There has been tremendous amount of work done on the application of game theory on wireless systems and networks (cf. [16] - [18]) as well as network security (cf. [32], [33]). Among the security games, Security Stackelberg Games (SSGs) (cf. [33], [34]) are most commonly used to model interaction between a defender (leader) and an attacker (follower). However, it is usually modeled that the attacker has incomplete knowledge of network (defender) resources as opposed to our proposed formulation. The same assumption is followed in network interdiction games (cf. [35]), in addition to perfect monitoring. In some cases, it is modeled that the leader plays a Bayesian Stackelberg game against an unknown follower of multiple types (cf. [36]), similar to our proposed formulation. However, [36] points out that finding the leader's optimal strategies spanning multiple rounds of the game with a Bayesian prior over follower's preferences is an open problem, and proposes a Monte Carlo Tree Search based algorithm to address it. In another adversarial scenario [37], the Iterated Best Response (IBR) technique is employed to update players' actions. Each player announces its Best Response (BR) to a strategy announced by the opponent (full monitoring) and the players try to minimize the error in an expected sense. The above-mentioned article also shows that the computation of an equilibrium (even in the scalar case) requires global knowledge. Other game-theoretic Stackelberg formulations have also been proposed for jamming in wireless networks (cf. [38], [39]) in which the jammer can tune its transmit power, adapt attack duration and choose to save energy similar to our proposed model. However, there are many fundamental differences between these formulations and our proposed model. For example, [38] used a Stackelberg game to model a jamming defense problem in the presence of a smart jammer who can learn transmission power of the user. In [38], the user is aware of the jammer's existence and intelligence, which is in contrast with our proposed model that requires jamming sense. Also, [38] assumes that the user can compute the jammer's Best Response (BR) and fading channel gains of the opponent player are known. Our proposed model makes no such assumptions for its algorithm design and analysis. On the other hand, [39] proposed a game-theoretic formulation to model the interaction between a legitimate node and a jammer, and suggested using numerical methods for solving the imperfect knowledge case. But, this model utilizes a timing channel for resilience that cannot be jammed and is applicable for only low-rate and covert communication. No such mechanism exists in LTE/LTE-A networks, which are designed and optimized for very high data rates.

Although this literature survey is not complete by any means, none of the formulations studied so far deal with the informed player's type estimation in an infinite-horizon general-sum (non-zero-sum) repeated game without "full monitoring". To the best of our knowledge, this article attempts to solve a unique problem. It is shown that the proposed *jammer type (state) estimation* algorithm achieves remarkable performance, while working under the constraints of realistic models (e.g., no full monitoring) and available statistics (e.g., no feedback from UEs).

II. Smart Jamming in LTE Networks

Potential *smart jamming* attacks and suggested network countermeasures are briefly presented in this section. These actions are taken from [7] and [9] and are presented here again for the sake of completeness.

A. Smart Jamming Attacks on an LTE Network

A power-limited *smart jammer* may jam specific common control and broadcast channels instead of jamming the entire network bandwidth to initiate *Denial of Service (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. Hence, a *smart jammer* does not need to "infiltrate" the network in order to achieve its goals. It may transmit an unknown jamming signal at specific time and frequency resources to jam selective channels in a given radio frame, which can be easily implemented using a software-defined radio (SDR). It is modeled that a *smart jammer* can launch jamming attacks by playing following actions[1]:

1) Inactive *(no jamming)*
2) Jam *CS-RS*
3) Jam *CS-RS + PUCCH*
4) Jam *CS-RS + PBCH + PRACH*
5) Jam *CS-RS + PCFICH + PUCCH + PRACH*

The *smart jammer* also uses its probability of jamming (p_j) and transmit power (P_j) to decide when to jam the network and how much power to use for the jamming attack. Each action is also associated with its corresponding duty cycle, which is modeled in the utility function as well. All these parameters dictate the (battery) power consumption of the *smart jammer*.

B. Suggested Network Countermeasures

Today's network operators rely on the intervention of skilled network engineers (triggered by poor network statistics) to rectify jamming problems by neutralizing the jammer. However, a *smart jammer* can go undetected by network engineers if it keeps changing its location randomly and launches jamming attacks probabilistically. In the event of incomplete jamming information (jammer's location, jamming waveform, probability of jamming, etc.) available to the network, it is proposed that an LTE network can take the following countermeasures:

1) Normal *(default action)*
2) Increase *CS-RS* Transmit Power *(pilot boosting)*
3) *Throttle* All UEs' Throughput *(threat mechanism)*
4) Change *eNode B* f_c *+ SIB2 (interference avoidance)*
5) Change eNode B *Timing (interference avoidance)*

[1]See [1] or [2] for the description of various LTE channels

None of the above-mentioned countermeasures require any significant changes in the LTE standard nor do they rely on exogenous information. However, employing interference cancellation techniques at the UEs or eNode B is not suggested due to technical difficulties, particularly the unknown jamming waveform and the absence of any "pilot" data from the jammer. Furthermore, blind interference cancellation may not converge in time and may require heavy computational resources, especially at resource-constrained UEs. Beamforming is also not suggested for similar reasons and the need for regular updating of weights, cf. [40]. Similar to the *smart jammer*, the network's actions are also associated with corresponding duty cycles modeled in its utility function. In addition, the network's proposed interference avoidance mechanisms also incur fixed costs associated with the required overhead and setup time delay. The average duty cycle and network's transmit power (P_0) determine the power consumption of the network corresponding to the anti-jamming operation.

III. LTE Network & Smart Jammer Dynamics

A. Network Model

The LTE network is modeled as follows, similar to the one used in [9].

1) Channel Model: The large-scale path loss is modeled by the *Simplified Path Loss Model* [40] and small-scale multipath fading is modeled by *3GPP/ITU's wideband Extended Vehicular A (EVA)* [1] channel model with a maximum Doppler frequency of 70 Hz.

2) SINR Model: In an OFDM-based system like LTE, the instantaneous SINR $\Gamma[k]$ of a particular subcarrier k can be modeled as:

$$\Gamma[k] = \frac{P_0[k]|h|^2 K(\frac{R_0}{d_0})^{-\gamma}}{\sigma^2 + P_j[k]|g|^2 K(\frac{R_j}{d_0})^{-\gamma}} \tag{1}$$

where P_0 and P_j are desired and jammer transmit powers, $|h|^2$ and $|g|^2$ are *Rayleigh-faded exponentially distributed* channel gains, $K(dB) = 20\log_{10}\left(\frac{\lambda}{4\pi d_0}\right)$ is a constant, R_0 and R_j are large-scale distances from desired transmitter and jammer respectively, d_0 is the outdoor reference distance for antenna far field, γ is the path loss exponent, and σ^2 is the noise variance at the receiver. Since, *Inter-Cell Interference (ICI)* is independent of jamming, it does not affect the test statistic. Therefore, any residual ICI can be lumped together in σ^2 for the scope of this article. It is assumed that σ^2 is the same at all receivers.

The SINR in (1) can also be re-written in terms of *Carrier-to-Jammer ratio* ($\frac{C}{J}$), i.e., ratio of average carrier power to average jammer power, which helps us to assess the performance of a channel at a given ($\frac{C}{J}$).

$$\Gamma[k] = \frac{(\frac{C}{J})|h|^2 K(\frac{R_0}{d_0})^{-\gamma}}{(\frac{\sigma^2}{P_j[k]}) + |g|^2 K(\frac{R_j}{d_0})^{-\gamma}} \tag{2}$$

However, (1) or (2) can only be utilized to model the SINR of a narrowband flat-faded signal. Since, LTE control channels like CS-RS, PCFICH and PUCCH are not wideband signals and are transmitted via subcarriers which are spaced across the bandwidth, (1) or (2) can be used to model their SINR accurately. However, (1) or (2) cannot be used to model the SINR of LTE's wideband data channels like PDSCH and PUSCH. Furthermore, SINR estimation is done in the frequency domain as described in [41].

3) BLER & Throughput Model: It is modeled that both eNode B and UE are unable to decode control channels below certain Block Error Rate (BLER) thresholds. 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. Moreover, the same throughput model with *Proportional Fair Scheduling (PFS)* (cf. [42]) is used as described in [9], based on AWGN channel capacity as an upper bound for data channels.

4) Network Dynamics: An *LTE* network can be abstracted as a *highly nonlinear dynamical system* that can be described as follows:

$$\chi^+ = f(\chi, \theta, a_0, a_j, \omega) \tag{3}$$

where $\chi \in \mathbb{R}^{M\times K}$ represents state of the network (not to be confused with the state of nature) with each row corresponding to the user $m \in M$, including K elements for each user (such as, SINRs Γ_m of its control and data channels, and average throughput for user $m \in M$); θ represents the state of nature (jammer type) as described in the next section; $a_0 \in \mathcal{A}_0$ represents eNode B action; $a_j \in \mathcal{A}_j$ represents jammer's action and ω characterizes the randomness in the network induced by the channel, arbitrary user locations, varying transmit power levels, PFS scheduling, etc. These network dynamics evolve at a uniform rate of T_s samples/second, and can be modeled as a *Markov process* if enough depth required by PFS is taken into consideration. Since, not all the states are observable by all the players (jammer cannot access network users and eNode B is not aware of jammer's and colluding UE's location, jamming waveform, etc.), it leads to a *Partially-Observable Markov Decision Process (POMDP)*.

The above-mentioned network dynamics and SINR model, along with nonlinear SINR thresholds make the entire network abstraction mathematically intractable. Hence, this abstracted model is simulated in *MATLAB*.

B. Game-Theoretic Model

The network dynamics (interaction between the LTE network and the smart jammer) are modeled as an **infinite-horizon two-player general sum Bayesian game $\mathcal{G}$ with asymmetric information** similar to that in [9] but with the additional assumption of a **myopic jammer**. The game $\mathcal{G}$ is described by

- N = {eNode B, jammer}, the set of players; Θ, the set of states of nature (jammer types); π, the prior probability distribution on Θ which is common knowledge.
- $\mathcal{A}_i$, the set of pure actions of player $i \in N$ as described in Section II.
- H, a set of sequences such that each $h \in H$ is a history of observations; $\mathcal{I}_i$, the information partition of player i.
- $\mathcal{U}_i \colon \Theta \times \mathcal{A}_0 \times \mathcal{A}_j \to \mathbb{R}$, the utility function of player i.

1) Jammer Types: The type $\theta \in \Theta$ of *smart jammer* is classified as:

- *Type 0:* **Normal** *(when jammer is not present)*
- *Type I:* **Cheater**
- *Type II:* **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 be unattached to the network. It is modeled that the colluding UE and narrowband jammer are not necessarily co-located but the colluding UE has the capability of canceling the interference caused by the narrowband jammer due to their collusion.

2) Strategies: The network is modeled as *strategic* whereas the jammer is modeled as *"myopic" (non-strategic)*, i.e., the jammer would play a myopic best response to the leader's strategy observed in the previous stage. The assumption of a myopic follower (i.e., jammer) is not new and has been used by many researchers, cf. [36]. Also, this assumption makes perfect sense in our model as the jammer wants to either "cheat" the network or inflict maximum damage to it in the shortest possible time without getting caught.

The repeated-game strategy algorithms presented in [9] showed that the network can recover some of its performance loss in case of a jamming attack and may even force an adversary to retract. The myopic and strategic strategies for the players are designed based on the simulation results obtained using above-mentioned algorithms.

3) Information Partitions: The adversary is informed of the state of nature θ, i.e., its own type. However, eNode B is only informed about the prior probability distribution π on the states of nature Θ. This results in a *game with asymmetric information*, with lack of information on the network side. Our proposed algorithm estimates $\hat{\theta}$ for a given $\theta \in \Theta$.

4) Observable Signals: Although players can observe their own payoffs they cannot observe opponent's actions due to the inherent randomization and inaccessibility of information in the network. This means that the "full monitoring" assumption cannot be realistically made in the proposed dynamics. The eNode B observable signals include the number and throughput statistics of UEs with active radio links. UEs also measure parameters related to Cell-Specific Reference Signal (CS-RS) including *Reference Signal Received Power (RSRP)*, *Reference Signal Received Quality (RSRQ)*, and *Channel Quality Indicator (CQI)* which are reported back to the eNode B on a regular basis. From these measurements, eNode B can infer *Signal-to-Noise Ratio (SNR)* and carrier *Received Signal Strength Indicator (RSSI)* for each UE. However, eNode B cannot observe signals from RLF UEs, which are most adversely affected by jamming attacks. Also, eNode B cannot observe the jammer and colluding UE's locations, probability of jamming and jamming waveform. All of these impediments make adversary type and actions' estimation very difficult for eNode B, further complicated by inherent channel variations.

The Cheater's observable signals include its own DL SNRs, RB assignments and eNode B frequency and timing change directives. Since eNode B frequency and timing change messages are sent to all the *Connected mode* UEs, the Cheater would be able to observe these actions perfectly. On the other hand, the Saboteur does not have any *Connected mode* UEs in the network and, hence, cannot listen to any *Connected mode* directives from the network. The Saboteur, however, synchronizes with the network periodically.

5) Utilities: Players' utilities are computed as weighted sums of *Key Performance Indicators (KPIs)*, normalized over a baseline jamming-free scenario. The utility function of player i can be concisely written as follows:

$$\mathcal{U}_i = \sum_{l=1}^{L} \alpha^l \mathbb{E}_\omega[g_i^l(\theta, a_i, a_{-i})] - C_i(a_i) \tag{4}$$

where α^l represents weight of the l^{th} KPI normalized w.r.t. the baseline jamming-free scenario, $\mathbb{E}_\omega$ represents the spatio-temporal expectation w.r.t. randomness caused by ω, g^l represents the l^{th} normalized KPI as a function of the jammer type θ, action of the ith player a_i, and action of the player other than the ith player a_{-i}, and C_i represents fixed cost of ith player's action a_i.

The KPIs are functions of observable parameters only, for example, eNode B's utility is a function of parameters observed from *Connected Mode* UEs only. For eNode B, KPIs include throughput/UE, number of *Connected Mode* UEs, CS-RS, PUCCH, PCFICH SINR, PRACH failure rate, and duty cycle. For Cheater they include its own throughput and duty cycle, and for Saboteur they include the negative of the eNode B throughput/UE, the negative of number of *Connected Mode* UEs and its own duty cycle. Different weights are assigned to each individual KPI based on its significance. For example, eNode B might care more about the number of users it can support as compared to average throughput/UE and so on. The duty cycle of each player is used to model its energy consumption and, hence, is treated as a cost for both players. It is to be noted here that the average duty cycle is derived from the actions taken by each player representing the ON time for the transceiver. Moreover, the fixed cost of an action does not depend on the opponent's action and is used to model quantities like required overhead and additional delay, etc. For example, fixed cost is used to model overhead needed for additional reconfiguration messages and set up time delay for eNode B's interference avoidance mechanisms. Furthermore, each player's transmit power and probability of jamming p_j are implicitly included in the utility function.

The above-mentioned utility functions provide a comprehensive utility (cost and benefit) model encompassing all important and relevant quantities a player might care about. However, this results in a *general sum (non-zero-sum)* game due to the asymmetry of objectives and KPIs among different players.

6) Game Play: At the beginning of the game, nature flips a coin and selects $\theta \in \Theta$ (type of adversary) according to $\pi \in \Delta(\Theta)$, which remains fixed for the rest of the game. The jammer is informed about its selected type but eNode B is not. However, in a *repeated game*, eNode B's history would evolve with time which could affect its belief about θ.

IV. Proposed Algorithm & Simulation Results

A. Proposed Test Statistic & Statistical Hypothesis Test

Although UEs report CQI, RSRP and RSRQ (and hence indirectly RSSI) to eNode B on regular basis, these measurements are mostly based on a reference signal and are not reported frequently enough (due to control channels scheduling and saturation constraints) to keep up with the network dynamics in case of a jamming attack. Furthermore, these measurements are only available from *Connected mode* UEs and no feedback (at least immediate) is possible from the UEs who suffer RLF either due to channel variations or possible jamming attack. In our initial studies, RSSI measurements were found to be more indicative of jamming attacks than RSRQ due to inherent wideband measurements, but consolidating these measurements from multiple UEs in the network does not provide a robust jamming detection statistic.

It is proposed to use *"number of Connected mode UEs"* as a more reliable test statistic to detect jamming attacks and estimate jammer type in the network. Clearly, eNode B has instantaneous access to this statistic, without requiring any explicit feedback from its users. It is also proposed to use non-parametric statistical hypothesis tests for jammer sensing, with *null hypothesis* being *no jamming*, even though they are less powerful than their counterpart parametric tests. However, most of the parametric tests assume some kind of *Normal* distribution or its approximations. It is argued that neither SINR nor LTE network dynamics (and, hence, number of *Connected mode* UEs) can be modeled or approximated using a Gaussian distribution which has been empirically validated by our simulations as well. Hence, using *Wilcoxon's non-parametric Rank-Sum test* a.k.a. *Mann-Whitney-Wilcoxon test* (cf. [43]) is proposed for jamming detection. It does not require the assumption of any specific distribution (e.g., Gaussian). The only required assumption is that the underlying distribution must be symmetric about its median.

B. Proposed Threat Mechanisms

The following threat mechanisms are proposed for various jammer types.

1) 'Throttling': The eNode B throttles *Resource Block (RB)* assignments for all the *Connected mode* UEs as a threat mechanism against the *Cheater* for a fixed duration. Since eNode B is unaware of the cheating UE, it would inflict throttling to all the UEs with active data sessions. This mechanism acts like a credible threat to the Cheater, since Cheater cares deeply about its own throughput.

2) 'f Change' - Interference Avoidance: eNode B "relocates" its center frequency and moves all *Connected mode* UEs to new frequencies within its occupied bandwidth for a fixed duration, hence, potentially moving jamming effects from control channels to PDSCH and PUSCH data channels. SIB 2 parameters are also changed in order to remedy PRACH and PUCCH failures. This mechanism acts like a credible threat to Saboteur since Saboteur cares deeply about sabotaging the LTE network and the proposed interference avoidance scheme alleviates jamming of control channels until Saboteur re-synchronizes with the network.

C. Proposed Algorithm

Our proposed algorithm is shown in Fig. 1. The network collects its baseline statistics (or accesses it from a database based on time of the day, day of the week basis) prior to any jamming activity (if any) on regular basis. This data corresponds to the *null hypothesis*. After sensing the jamming attack, the network runs a series of tests to "filter" the jammer type based on myopic best-response behavior of the jammer using non-parametric hypothesis testing and conditional probabilities $p(\theta|j)$ and $p(\theta|\bar{j})$, where j and $\bar{j}$ represent *'Jamming'* and *'No Jamming'* respectively. The network uses a combination of above-mentioned *threat mechanisms* to compel a systematic response from the smart jammer, and exploits it to estimate the jammer type.

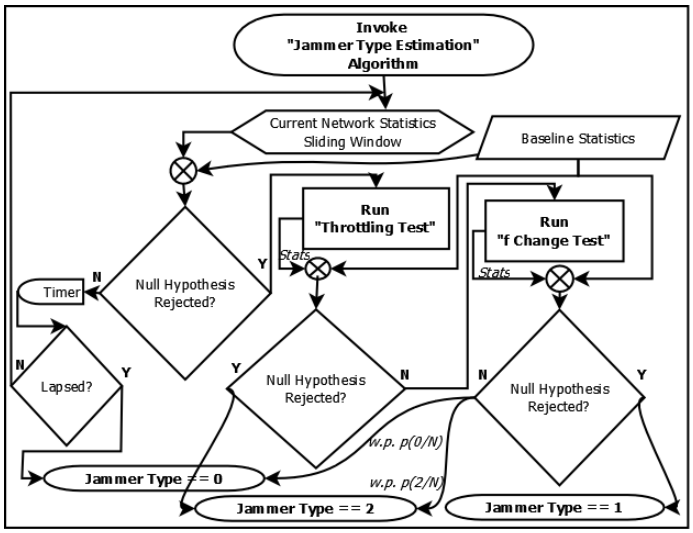

Fig. 1: eNode B's jammer type estimation algorithm

1) Initial Jamming Sense: The proposed algorithm is invoked by the network on a regular basis (or event-driven basis), such as, daily or weekly, etc. The network uses a sliding-window to collect current statistics, which are compared against its baseline statistics and the P-value is calculated using *Wilcoxon's rank-sum test* at a pre-determined significance level α_1. If the network fails to reject null hypothesis at α_1 for the duration T_{sense}, then the algorithm terminates with a declaration of *"No Jammer"* in the network. However, if resulting P-value is less than α_1, then the null hypothesis is rejected and *"network under jamming attack"* is declared by the algorithm, which is followed by a series of tests described below to estimate the jammer type.

2) 'Throttling' Test - Threat against Cheater: A non-parametric *Wilcoxon's rank-sum test* is performed at a pre-determined significance level α_2 using test and baseline statistics. If the null hypothesis (no jamming) is rejected at α_2, then the algorithm terminates with a final determination of *"Saboteur"*; otherwise the algorithm proceeds to the second test *"f Change"*.

3) 'f Change' Test - Threat against Saboteur: Wilcoxon's rank-sum test is performed at significance level α_2 using test and baseline statistics. If the null hypothesis (no jamming) is rejected at α_2, then the algorithm terminates with a final

determination of *"Cheater"*. However, if the network *fails to reject* null hypothesis at α_2, then the final determination of *"No Jammer"* and *"Saboteur"* is made with conditional probabilities $p(\theta = 0|\bar{j})$ and $p(\theta = 2|\bar{j})$ respectively.

4) Jammer's Best Response: The pure *security strategies* of both the Cheater and the Saboteur require them not to jam the network, which is obviously not optimal for them. Moreover, computing optimal strategies for an infinite-horizon repeated game might be too complicated and resource-constraining for the jammer. Therefore, the jammer resorts to playing myopic best-responses to eNode B's observed strategy. Since the jammer is myopic, it always tries to maximize its short-term utility based on single-shot simulation results.

Cheater has a *Connected mode* UE in the network, hence, it can observe the network's *'interference avoidance'* and *'throttling'* actions and play best response to them according to a single-shot formulation. For example, in case of *'throttling'* and *'f Change'*, Cheater would play *'Inactive'* and *'Jam CS-RS + PUCCH'*, respectively, and so on. However, it cannot easily distinguish between *'Normal'* and *'pilot boosting'* network actions. Therefore, it assumes that the network plays both of those actions equally likely when not in receipt of a special network directive. In that case, Cheater would respond by playing *'Jam CS-RS + PCFICH + PUCCH + PUCCH'* with probability 3/4 and *'Jam CS-RS + PUCCH'* with probability 1/4.

On the other hand, *Saboteur* does not have any *Connected mode* UE in the network and, hence, plays an open-loop best response to eNode B's actions. In the absence of the instantaneous observation of eNode B actions, it assumes that eNode B plays all of them equally likely and, hence, plays a best-response with the same probability. Thus, Saboteur would play *'Jam CS-RS + PUCCH'* with probability 3/5 and *'Inactive'* with probability 2/5.

After sensing a jamming attack, the network runs a series of tests to "filter" the jammer type based on the myopic best-response behavior of the jammer. At the end of the first test, it uses conditional probability $p(\theta|j)$ to decide the jammer type. If no jamming is sensed, it runs the second test and again decides jammer type according to $p(\theta|j)$. If no jamming is sensed at the end of the second test, conditional probability $p(\theta|\bar{j})$ is used to estimate jammer type.

D. Simulation Results

The proposed algorithm's performance is characterized using MATLAB simulations. The algorithm is parameterized by initial jamming sense duration T_{sense}, its corresponding significance level α_1, specific type detection test duration T_{test} and its corresponding significance level α_2. Moreover, the algorithm's error probability p_e and true estimation probability $p(\hat{\theta} = k|\theta = k)$, $k = \{0, 1, 2\}$ performance is dependent on the carrier-to-jammer ratio $\frac{C}{J}$ and probability of jamming p_j as well. Since, this article is focused on characterizing the proposed algorithm's performance under varying jammer characteristics like $\frac{C}{J}$ and p_j, parameters T_{test}, α_1, and α_2 are fixed to 120 ms (i.e. 120 subframes), 10%, and 5% respectively. A curious reader may also want to vary these parameters to observe interesting trade-offs.

Similar to any statistical estimator, the proposed algorithm has Type I error (false alarm), Type II error (missed detection) and misclassification errors (classifying *Cheater* as *Saboteur* and vice versa). Type I and Type II error probabilities are plotted against initial jamming sense duration T_{sense} in Fig. 2 and Fig. 3, respectively, for various levels of $\frac{C}{J}$ (p_j = 1.0). T_{sense} provides a reasonable trade-off between Type I and Type II errors. Higher T_{sense} increases Type I error, while reducing Type II errors and vice versa. In addition, *Saboteur* (state = 2) missed detection error probability is generally lower than that of *Cheater* (state = 1) especially at higher T_{sense}.

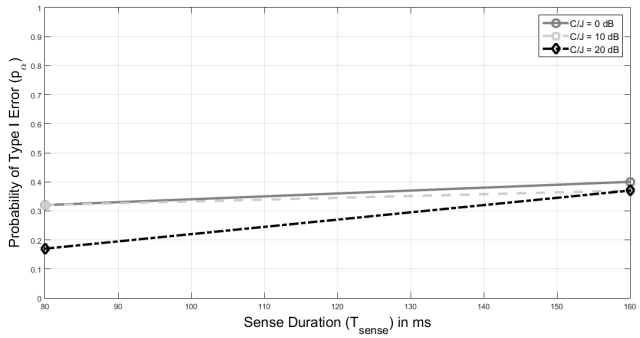

Fig. 2: Type I error (false alarm probability) vs. initial jamming sense duration T_{sense}

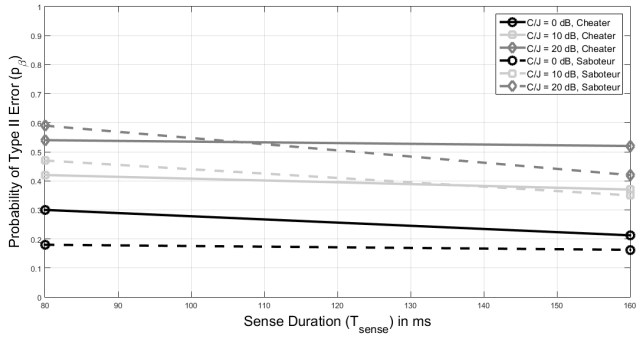

Fig. 3: Type II error (missed detection probability) vs. initial jamming sense duration T_{sense}

The algorithm's missed detection error performance (Type II errors) also depends on the jamming probability p_j. Type I (false alarm) and Type II (missed detection) errors are plotted against p_j in Fig. 4 for $\frac{C}{J}$ = 0 dB and T_{sense} = 160 ms. The false alarm error probability does not depend on probability of jamming p_j as expected, whereas the missed detection probability decreases with increasing p_j. However, higher Type II error (missed detection) at lower p_j may not be too devastating for the network as the jamming impact is considerably reduced at lower p_j.

Furthermore, the proposed algorithm's true estimation probability $p(\hat{\theta} = k|\theta = k)$, $k = \{0, 1, 2\}$ is plotted against $\frac{C}{J}$ in Fig. 5 for various levels of T_{sense} and p_j = 1.0. State 0 (*Normal*) error probability only includes Type I error (false alarm), whereas state 1 (*Cheater*) and state 2 (*Saboteur*) error probabilities include Type II errors (missed detection)

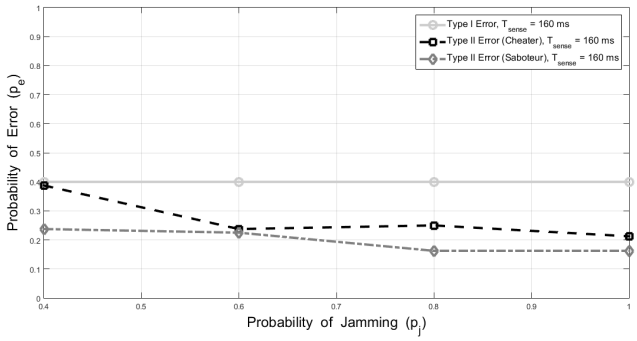

Fig. 4: Probability of error (p_e) vs. probability of jamming (p_j) for $\frac{C}{J}$ = 0 dB

as well as misclassification errors. *Normal* state's (state 0) true estimation probability does not change much with $\frac{C}{J}$ in general and is found to be equal to or higher than 0.68 and 0.63 for T_{sense} = 80 ms and T_{sense} = 160 ms respectively. State 1 and 2 true estimation probability goes down with decreasing jamming power (increasing $\frac{C}{J}$). Also, *Saboteur's* (state 2) true estimation probability decreases more rapidly than that of the *Cheater* (state 1) due to relatively higher misclassification errors $p(\hat{\theta} = 1|\theta = 2)$ at lower jamming powers (higher $\frac{C}{J}$). It is to be noted here that jamming effects become less detrimental at lower jamming powers (higher $\frac{C}{J}$), hence, causing less damage to the test statistic. Nevertheless, state 1 true estimation probability at $\frac{C}{J}$ = 0 dB was observed to be 0.52 and 0.68 for T_{sense} = 80 ms and 160 ms, respectively. Similarly, state 2 true estimation probability at $\frac{C}{J}$ = 0 dB was observed to be 0.66 and 0.61 for T_{sense} = 80 ms and 160 ms, respectively.

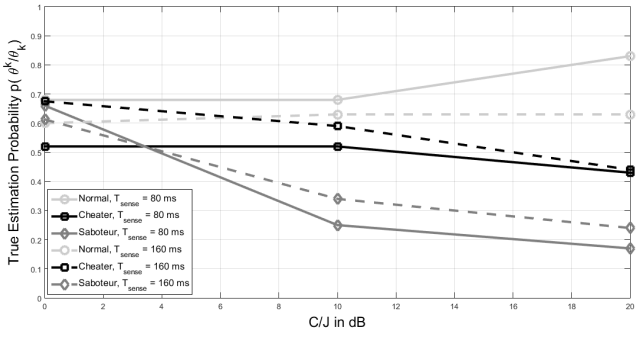

Fig. 5: True estimation probability $p(\hat{\theta} = k/\theta = k)$ vs. $\frac{C}{J}$ (p_j = 1.0)

Finally, the algorithm converges in 267 ms and 324 ms on average for initial jamming sense duration T_{sense} of 80 ms and 160 ms, respectively.

E. Performance Analysis

Although the proposed algorithm uses non-parametric hypothesis tests (*Wilcoxon's rank-sum test*) as compared to more powerful parametric tests, it is still able to detect true jammer type with a probability of 0.61 or higher at $\frac{C}{J}$ = 0 dB, with initial jamming sense duration T_{sense} of 160 ms. This performance mark improves with lower T_{sense} with an exception for state 1 (*Cheater*), when it goes down from 0.68 to 0.52. Also, the algorithm converges remarkably fast in 267 ms and 324 ms for initial jamming sense duration of 80 ms and 160 ms, respectively. Moreover, its estimation performance is quite robust against probability of jamming p_j and carrier-to-jammer ratio $\frac{C}{J}$. Furthermore, *Normal* state's (state 0) true estimation performance does not degrade with decreasing jamming power (increasing $\frac{C}{J}$), and that of states 1 (*Cheater*) and 2 (*Saboteur*) degrade gracefully with increasing $\frac{C}{J}$.

The algorithm provides several parameters to tweak its performance and trade-off different kinds of inherent errors in an estimator. For example, initial jamming sense duration T_{sense} and α_1 can be tweaked to trade-off Type I (false alarm) and Type II (missed detection) errors. Similarly, specific type test duration T_{test} and α_2 can be tweaked to trade-off misclassification errors and average convergence time.

F. Practical Implementation Challenges

Although implementing the proposed algorithm on an experimental test bed is out of scope for this paper, it can be implemented by an infra vendor on a realistic eNode B if its IP blocks and algorithms are accessible and modifiable. However, emulating the proposed algorithm on a USRP-based experimental test bed is non-trivial because it involves implementing multiple LTE/LTE-A subcomponents, ranging from PHY-only signals to control and data channels to the resource scheduler. Furthermore, all of these subcomponents are interdependent on each other and often require real-time operation and significant computational power and/or specialized IP blocks. Similarly, a *smart jammer* can be emulated on a USRP-based test bench but it also requires access to the UE timing and control information in order to launch the attacks. Despite these practical implementation challenges, the authors are confident that the proposed algorithm would perform well if implemented on a realistic eNode B.

V. Concluding Remarks

In this paper, a *threat-based jammer type estimation algorithm* is proposed for an infinite-horizon non-zero-sum repeated game with imperfect monitoring, and its estimation performance is characterized and analyzed for LTE/LTE-A networks. The algorithm performs remarkably well in estimating the actual type of the jammer in the network, despite the fact that it does not depend on the notion of "full monitoring" and uses a less powerful non-parametric hypothesis test. The number of *Connected mode* UEs is used as the test statistic, which does not require any feedback from the users. The algorithm is able to estimate actual jammer type with a probability of 0.61 or higher and converges in 324 ms on average. Moreover, the proposed algorithm provides several parameters to tweak its estimation performance and trade-off error probabilities (e.g. false alarm and missed detection errors). Furthermore, the proposed algorithm's false alarm error performance is

quite robust against probability of jamming p_j and carrier-to-jammer ratio $\frac{C}{J}$, whereas missed detection error performance degrades gracefully with decreasing p_j and jamming power (increasing $\frac{C}{J}$). It is to be noted here that jamming effects are less detrimental at lower probability of jamming p_j and jamming power (higher $\frac{C}{J}$), hence, causing less change to the test statistic. Nevertheless, the proposed algorithm provides a practical yet robust way to estimate jammer type without requiring any feedback from the network users nor making any unrealistic assumptions.

ACKNOWLEDGMENT

The research reported in this publication was supported in part by funding from the US AFOSR/MURI project # FA9550-10-1-0573, the US ARO project # W911NF-09-1-0553, and the King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia.

REFERENCES

[1] 3rd Generation Partnership Project (3GPP): Technical Specifications; LTE (Evolved UTRA) and LTE-Advanced Radio Technology Series (Rel 14) [Online]. Available: http://www.3gpp.org/ftp/Specs/latest/Rel-14/

[2] 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.

[3] The Global mobile Suppliers Association (GSA). (2016, Oct.) GSA Report: Evolution to LTE - Oct. 27, 2016. [Online]. Available: http://gsacom.com/paper/gsa-evolution-lte-october-2016/

[4] 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.

[5] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *Proc. 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP),* pp. 285-288, Dec. 2013.

[6] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP Journal on Information Security,* 2014, 2014:7.

[7] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks," in *Proc. 2014 IEEE Globecom,* Austin, TX, pp. 734-739, Dec. 2014.

[8] C. Shahriar, M. L. Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-layer resiliency in OFDM communications: a tutorial," *IEEE Comm. Surveys & Tutorials,* vol. 17, no. 1, pp. 292-314, Jan. 2015.

[9] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks: wideband model," in *Proc. 2015 IEEE 26th International Symposium on PIMRC,* Hong Kong, China, pp. 1534-1538, Aug - Sep. 2015.

[10] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Comm. Magazine,* vol. 54, no. 4, pp. 54-61, Apr. 2016.

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

[12] R. J. Aumann, and S. Hart (Eds.), *Handbook of Game Theory with Economic Applications.* vol. 1. Amsterdam, The Netherlands: Elsevier, 1992.

[13] R. J. Aumann, and M. Maschler, *Repeated Games with Incomplete Information.* Cambridge: The MIT Press, 1995.

[14] S. Sorin, *A First Course on Zero-Sum Repeated Games.* vol. 37. Berlin Heidelberg: Springer-Verlag, 2002.

[15] J-F. Mertens, S. Sorin, and S. Zamir, *Repeated Games.* New York: Cambridge University Press, 2015.

[16] A. B. Mackenzie, and L. A. DaSilva, *Game Theory for Wireless Engineers.* San Rafael, California: Morgan & Claypool Publishers, 2006.

[17] E. Altman, T. Boulogne, R. El-Azouzi, T. Jimenez, and L. Wynter, "A survey on networking games in telecommunications," *Computers & Operations Research,* vol. 33, no. 2, pp. 286-311, 2006.

[18] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications.* New York: Cambridge University Press, 2011.

[19] M. Jones, and J. S. Shamma, "Policy improvement for repeated zero-sum games with asymmetric information," in *Proc. 51st IEEE Conference on Decision and Control (CDC) 2012,* pp. 7752-7757, Dec. 2012.

[20] L. Li, and J. S. Shamma, "LP formulation of asymmetric zero-sum stochastic games," in *Proc. 53rd IEEE Conference on Decision and Control (CDC) 2014,* pp. 1930-1935, Dec. 2014.

[21] L. Li, and J. S. Shamma, "Efficient computation of discounted asymmetric information zero-sum stochastic games," in *Proc. 54th IEEE Conference on Decision and Control (CDC) 2015,* pp. 4531-4536, Dec. 2015.

[22] L. Li, E. Feron, and J. S. Shamma, "Finite stage asymmetric repeated games: Both players' viewpoints," in *Proc. 55th IEEE Conference on Decision and Control (CDC) 2016,* pp. 5310-5315, Dec. 2016.

[23] V. Kamble, *Games with vector payoff: a dynamic programming approach.* PhD dissertation, UC Berkeley, CA, Fall 2015.

[24] X. He, H. Dai, P. Ning, and R. Dutta, "Dynamic IDS configuration in the presence of intruder type uncertainty," in *Proc. 2015 IEEE Global Communications Conference (GLOBECOM),* Dec. 2015.

[25] H. P. Young, and S. Zamir (Eds.), *Handbook of Game Theory with Economic Applications.* vol. 4. Amsterdam, The Netherlands: Elsevier, 2015.

[26] T. Sandholm, "The state of solving large incomplete-information games, and application to poker," *AI Magazine,* vol. 31, no. 4, pp. 13-32, 2010.

[27] B. De Meyer, "Repeated games and partial differential equations," *Mathematics of Operations Research,* vol. 21, no. 1, pp. 209-236, 1996.

[28] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *Information Forensics and Security, IEEE Trans. on,* vol. 9, no. 8, pp. 1278-1287, Aug. 2014.

[29] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "Security games with unknown adversarial strategies," *Cybernetics, IEEE Transactions on,* vol. 46, no. 10, pp. 2291-2299, Oct. 2016.

[30] A. Garnaev, and W. Trappe, "A bandwidth monitoring strategy under uncertainty of the adversary's activity," *Information Forensics and Security, IEEE Trans. on,* vol. 11, no. 4, pp. 837-849, Apr. 2016.

[31] M. Baykal-Gürsoy, Z. Duan, H. V. Poor, and A. Garnaev, "Infrastructure security games," *European Journal of Operational Research,* vol. 239, no. 2, pp. 469-478, 2014.

[32] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR),* vol. 45, no. 3, 2013.

[33] M. Tambe, *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned.* Cambridge University Press, 2011.

[34] H. Von Stackelberg, *The Theory of the Market Economy.* London: Oxford University Press, 1952.

[35] J. Zheng, and D. A. Castann, "Dynamic network interdiction games with imperfect information and deception," in *Proc. 2012 IEEE 51st IEEE Conference on Decision and Control (CDC),* pp. 7758-7763, Dec. 2012.

[36] J. Marecki, G. Tesauro, and R. Segal, "Playing repeated Stackelberg games with unknown opponents," in *Proc. 11th International Conf. on Autonomous Agents and Multiagent Systems - Vol. 2,* pp. 821-828, 2012.

[37] S. D. Bopardikar, A. Speranzon, and C. Langbort, "Trusted computation with an adversarial cloud," in *Proc. 2015 IEEE American Control Conference (ACC),* pp. 2445-2452, Jul. 2015.

[38] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: a game-theoretic analysis," *Wireless Communications, IEEE Trans. on,* vol. 14, no. 5, pp. 2337-2352, May 2015.

[39] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A Stackelberg game approach," in *Wireless Communications, IEEE Trans. on,* vol. 12, no. 8, pp. 4038-4047, Aug. 2013.

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

[41] H. Arslan, and S. Reddy, "Noise power and SNR estimation for OFDM based wireless communication systems," in *Proc. IASTED Inter. Conf. on Wireless and Optical Communications,* 2003.

[42] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *Info. Theory, IEEE Trans. on,* vol. 48, no. 6, pp. 1277-1294, Jun. 2002.

[43] R. V. Hogg, J. McKean, and A. T. Craig, *Introduction to Mathematical Statistics.* (7th ed.) Essex, UK: Pearson, 2012.

Farhan M. Aziz (S'98) is a Ph.D. (EE) candidate at the School of Electrical & Computer Engineering, Georgia Institute of Technology, Atlanta, GA. His Ph.D. research is focused on identification of security vulnerabilities in LTE/LTE-A air interface and devising autonomous policies to combat smart jamming attacks in LTE/LTE-A networks. He is also currently working as a Sr. Systems Engineer at Shared Spectrum Company (SSC), Vienna, VA, where his primary job responsibilties include design and development of dynamic spectrum access (DSA) algorithms and techniques for military radios (e.g.,WNW and WNaN) and satellites; and writing project proposals for utilizing DSA technology for communication in various tactical and strategic situations. Aziz received a Bachelor of Engineering (B.E.) degree in Electrical Engineering from the NED University of Engineering & Technology, Karachi, Pakistan in 1999 and a Master of Science (M.S.) degree in Electrical Engineering from the Virginia Polytechnic Institute & State University, Blacksburg, VA in 2003. His Masters' thesis was focused on utilizing IEEE 802.11b technology for the design,deployment and analysis of a wireless network for high-mobility telematics at Virginia's Smart Road. From 2004 - 2010, he worked at Qualcomm CDMA Technologies (QCT) division of Qualcomm Inc., San Diego, CA as a Staff Engineer where he got hands-on experience in LTE, HSPA, WCDMA, cdma2000, GSM, 802.11b/g/n, Bluetooth and GPS modems and multimedia subsystems. Aziz was part of QCT modem architecture, power systems and modem performance analysis teams at Qualcomm and led QCT's multidisciplinary power systems competitive analysis project for many years. He holds two US patents on modem and multimedia power optimization in mobile handsets. From 1999 - 2000, he worked at Alcatel Pakistan as a Field Engineer working on configuration and expansion of countrywide voice/data communication network consisting of Alcatel's proprietary switching nodes, microwave and drop/insert DRS links. Aziz's research interests lie in the general areas of communication systems and networks, applied game theory, radio network security, PHY-layer security, THz communications, smart grid communications and probabilistic computing.

Jeff S. Shamma (F'06) is a Professor and Chair of Electrical Engineering at the King Abdullah University of Science and Technology (KAUST) in Thuwal, Saudi Arabia, where he is also the director of the Robotics, Intelligent Systems & Control laboratory (RISC). He is the former Julian T. Hightower Chair in Systems & Control in the School of Electrical and Computer Engineering at Georgia Tech. He also has held faculty positions at the University of Minnesota, The University of Texas at Austin, and the University of California, Los Angeles. Shamma received a Ph.D. in Systems Science and Engineering from MIT in 1988. He is the recipient of an NSF Young Investigator Award, the American Automatic Control Council Donald P. Eckman Award, and the Mohammed Dahleh Award. Shamma is a Fellow of the IEEE and the International Federation of Automatic Control (IFAC) and a current distinguished lecturer of the IEEE Control Systems Society. He is the deputy editor-in-chief for the IEEE Transactions on Control of Network Systems and an associate editor for the journal Games. Shamma's research is in the general area of feedback control and systems theory. His most recent research has been in decision and control for distributed multiagent systems and the related topics of game theory and network science, with applications to cyberphysical and societal network systems.

Gordon L. Stüber (S'81-M'82-SM'96-F'99) received the B.A.Sc. and Ph.D. degrees in Electrical Engineering from the University of Waterloo, Ontario, Canada, in 1982 and 1986 respectively. In 1986, he joined the School of Electrical and Computer Engineering, Georgia Institute of Technology, where he is the Joseph M. Pettit Chair Professor in Communications.

Dr. Stüber is author of the wireless textbook Principles of Mobile Communication, Kluwer Academic Publishers, 1996, 2/e 2001, 3/e 2011. He was co-recipient of the Jack Neubauer Memorial Award in 1997 for the best systems paper published in the IEEE Transactions on Vehicular Technology. He became an IEEE Fellow in 1999 "for contributions to mobile radio and spread spectrum communications." He received the IEEE Vehicular Technology Society James R. Evans Avant Garde Award in 2003 "for his contributions to theoretical research in wireless communications." In 2007, he received the IEEE Communications Society Wireless Communications Technical Committee Recognition Award (2007) "for outstanding technical contributions in the field and for service to the scientific and engineering communities." He was an IEEE Communication Society Distinguished Lecturer (2007-2008) and IEEE Vehicular Technology Society Distinguished Lecturer (2010-2012). Finally, he was co-recipient of the Neal Shepherd Memorial Best Propagation Paper Award in 2012, for the best propagation paper published in the IEEE Transactions on Vehicular Technology.

Dr. Stüber served as Technical Program Chair for the 1996 IEEE Vehicular Technology Conference (VTC'96), Technical Program Chair for the 1998 IEEE International Conference on Communications (ICC'98), General Chair of the Fifth IEEE Workshop on Multimedia, Multiaccess and Teletraffic for Wireless Communications (MMT'2000), General Chair of the 2002 IEEE Communication Theory Workshop (CTW'02), and General Chair of the Fifth YRP International Symposium on Wireless Personal Multimedia Communications (WPMC'2002). He is a past Editor for Spread Spectrum with the IEEE Transactions on Communications (1993-1998), and a past member of the IEEE Communications Society Awards Committee (1999-2002). He served as an elected Member-at-Large on the IEEE Communications Society Board of Governors (2007-2009), and is currently an elected member of the IEEE Vehicular Technology Society Board of Governors (2001-2018). He received the IEEE Vehicular Technology Society Outstanding Service Award in 2005.