RESILIENCE OF LTE NETWORKS AGAINST SMART JAMMING ATTACKS:
A GAME-THEORETIC APPROACH

A Dissertation
Presented to
The Academic Faculty

By

Farhan Muhammad Aziz

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical & Computer Engineering (ECE)

Georgia Institute of Technology

August 2017

RESILIENCE OF LTE NETWORKS AGAINST SMART JAMMING ATTACKS: A GAME-THEORETIC APPROACH

Approved by:

Dr. Jeff S. Shamma, Advisor
Professor & Program Chair, Electrical Engineering
King Abdullah University of Science and Technology (KAUST)

Dr. Gordon L. Stüber, Co-Advisor
Joseph M. Pettit Chair Professor, School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Steven W. McLaughlin
Professor & Steve W. Chaddick School Chair, School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Eric M. J. Feron
Dutton/Ducoffe Professor, School of Aerospace Engineering
Georgia Institute of Technology

Dr. Matthieu R. Bloch
Associate Professor, School of Electrical & Computer Engineering
Georgia Institute of Technology

Dr. Justin K. Romberg
Schlumberger Professor & Associate Chair for Research, School of Electrical & Computer Engineering
Georgia Institute of Technology

Date Approved: May 1, 2017

“In the name of Allah, the Most Beneficent, the Most Merciful.

Read! In the Name of your Lord who created - Created the human from a clinging substance. Read! And your Lord is the Most Generous - He who taught by the pen, Taught the human that which he did not know.”

[The very first passage revealed from The Holy Quran to the mankind!]

To my late parents, Sabra Begum and Abdul Aziz Khan, who instilled the thirst of knowledge in their children, and sacrificed their own personal needs and comfort for the sake of their education! May Allah Almighty bless their souls with His mercy and with the bounties of the heaven, aameen

ACKNOWLEDGEMENTS

It is hard to believe that I am finally writing my dissertation but I certainly did not do it all by myself. It would not have been possible without the support and guidance from others. It was a long ride and I am indebted to so many for helping me reach this milestone in my life. First and foremost, I am grateful to my Lord Almighty for blessing me with life, faith, health, beautiful family, sincere friends, rational thinking and much more, to name a few. He helped me throughout my life and during this state of uncertainty and lengthy odyssey.

My research expedition at Georgia Tech started from smart grid communications to probabilistic computing to THz communications to finally, LTE security and game theory. It was a mere coincidence that I got to meet Dr. Jeff Shamma during a PhD proposal exam and later served as his course TA. It was him, who introduced me to the fascinating areas of game theory and dynamic programming. I was so inspired and intrigued by his research that I started talking to him about potential research ideas and avenues for collaboration and in Summer of 2012, I was part of his amazing research group. I never imagined that I would be working with a Controls professor for PhD! One can say that my undergrad Controls courses were not captivating enough but, the reality is that Dr. Shamma and his research is exhilarating! I am so grateful to him for being my advisor and mentor throughout the PhD process. Dr. Shamma not only advised me on research but also on life lessons - watching out for my welfare, and treating me with kindness and respect. He took time out of his busy schedule to discuss various research ideas and approaches with me very patiently. It was him that made it possible - Thank you, Dr. Shamma!

Although I met Dr. Shamma coincidently, Dr. Gordon Stüber was one of the reasons I came to the Georgia Tech. Dr. Stüber is one of the pioneers in the field of wireless communications and a marvel in his research. I have been talking to him even before coming to Georgia Tech. It was thrilling to work on a special problem with him and it is an honor for me to be his Ph.D. student in his wireless systems lab. I cannot thank him enough for providing me guidance and advice on research ideas, models, practical constraints and publications, throughout my pursuit. Without his help, I would not have been able to graduate! Thank you, Dr. Stüber!

I would also like to thank my proposal reading committee members, Dr. Steven McLaughlin and Dr. Eric Feron. Dr. McLaughlin's research on physical layer security inspired me to discover and define smart jamming problem in LTE networks. Dr. Feron not only guided me during my proposal process but also took care of my research funding when Dr. Shamma was on leave for two years. Thank you, Dr. McLaughlin, and Dr. Feron for your time and providing me valuable feedback and overall guidance on my research. I would also like to thank my final committee members, Dr. Matthieu Bloch and Dr. Justin Romberg for assessing my dissertation defense and providing valuable feedback. Thank you!

This research would not have been possible without funding assistance from AFOSRs MLMR Games MURI, Julian T. Hightower Chair in Systems and Controls, Joseph M. Pettit Chair in Telecommunications, and the School of Electrical & Computer Engineering. Thank you! Special thanks to Dr. Bonnie Ferri, Dr. George Riley, Dr. Daniela Staiculescu and LaToya Jordan for providing me academic and administrative support. Thank you!

I would also like to extend my special thanks to postdoctoral researchers Lichun and Kwang-Ki, not just for support and encouragement but also for taking out time to discuss asymmetric repeated games and Stackelberg game formulations with me. It was a stimulating experience and I felt privileged to find their company. Thank you!

Thanks is also due to Shared Spectrum Company for their understanding and accommodating my flexible work schedule during the last four months. I would also like to thank Chris Riddle, my mentor and former VP at Qualcomm, for his initial encouragement and support.

I was fortunate to know many wonderful and supporting friends at Georgia Tech including Bashir, Usman, Sajid, Hassan, Umer, and Omer. Your support, delightful discussions and tea treats will always be remembered. I would also like to thank my lab mates Malachi, Nicolas, Yusun, Yasin, Daniel, Sebastian, Keith, Georgios K., Georgios P., Ibrahim and Ceyhun from Georgia Tech, and Mohammad S., Mohammad A. K. and Ahmad from KAUST for their support, encouragement and providing a pleasant company in the labs. Thank you!

This journey is not complete without the help and support of my family members and close friends. I would like to thank my dear brothers Tariq, Kashif, Saqib, Adnan, Arsalan and Raheel; and beloved sisters Sumbul and Shazia and their families for their support, encouragement and prayers. Thank you! I would also like to thank my dear friends Arif, Baligh, Pranab, Mueez and Farhan for their ongoing support and encouragement. Thank you!

This was a long and fascinating quest and I truly enjoyed every minute of it, with all its ups and downs. However, truth be told it was not easy to leave the intriguing and rewarding job at Qualcomm; sincere friends; and the finest city of San Diego. Moving across the country and living with two little kids on a teaching/research assistant salary was a challenging experience. I still dont know how we did it but it was my wife Fauzia, who stood by me and embraced my passion for earning a Ph.D. with open arms. She did not only support me emotionally, but also psychologically and physically, while taking care of the kids, their education, entertainment and practically everything in and outside the home. I am grateful to her for her unconditional love, emotional support, friendship, patience and sacrifices. I am also thankful to my kids Abdullah and Maryam for standing by me and their mom. They left their birthplace and friends behind, and supported me in pursuit of this dream. Their presence is indeed a source of happiness, tranquility and strength in my life. I love you all so much! May ALLAH Almighty keep all of you happy and blessed, aameen!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

2G Second Generation Cellular Networks.

3G Third Generation Cellular Networks.

3GPP 3rd Generation Partnership Project.

4G Fourth Generation Cellular Networks.

5G Fifth Generation Cellular Networks.

ARQ Automatic Repeat Request.

cdma2000 Code Division Multiple Access, IMT-2000 (3G) standard.

CS-RS Cell-Specific Reference Signal.

DL Downlink.

eNode B E-UTRAN Node B or Evolved Node B (LTE/LTE-A Base Station).

GSM Global System for Mobile Communication, 2G standard.

IoT Internet of Things.

KPI Key Performance Indicator.

LTE Long Term Evolution, IMT-Advanced (4G) standard.

LTE-A Long Term Evolution - Advanced, IMT-Advanced (4G) standard.

MIB Master Information Block.

MIMO Multiple-Input Multiple-Output.

NE Nash Equilibria.

NP-hard Non-deterministic Polynomial-time hard.

OFDM Orthogonal Frequency Division Multiplexing.

PBCH Physical Broadcast Channel.

PCFICH Physical Control Format Indicator Channel.

PDCCH Physical Downlink Common Control Channel.

PDSCH Physical Downlink Shared Channel.

PHICH Physical Hybrid Indicator Channel.

PHY The Physical Layer of the OSI model.

PRACH Physical Random Access Channel.

PSS Primary Synchronization Signal.

PUCCH Physical Uplink Common Control Channel.

PUSCH Physical Uplink Shared Channel.

RB Resource Block (LTE's radio resource in time and frequency domain).

RRC Radio Resource Control.

SDR Software-Defined Radio.

SIB System Information Block.

SINR Signal-to-Interference-plus-Noise Ratio.

SNR Signal-to-Noise Ratio.

SSE Strong Stackelberg Equilibria.

SSS Secondary Synchronization Signal.

UAV Unmanned Aerial Vehicle.

UE User Equipment (LTE/LTE-A subscriber terminal).

UL Uplink.

USRP Universal Software Radio Peripheral.

WCDMA Wideband Code Division Multiple Access, IMT-2000 (3G) standard.

WiFi Wireless Fidelity (WLAN product based on IEEE 802.11 standards).

WiMAX Worldwide Interoperability for Microwave Access, 4G standard.

WLAN Wireless Local Area Network.

WWAN Wireless Wide Area Network.

SUMMARY

The objectives of this research are to identify security vulnerabilities in LTE/LTE-A air interface; model the network and the *smart jammer* dynamics under realistic constraints; and devise adept algorithms that can help the network combat *smart jamming* attacks autonomously. LTE/LTE-A networks provide advanced data, Voice-over-IP (VoIP), multimedia, and location-based services to more than a billion subscribers around the world. Lately, it has been suggested to utilize commercially and privately-owned LTE/LTE-A networks for mission-critical applications like public safety, smart grid and military communications. Although LTE/LTE-A air interface provides ease of accessibility, flexibility, mobility support, low latency, high data rates, and economy of scale, it also raises serious security concerns. It is shown that the LTE air interface is vulnerable to *denial-of-service (DoS)* and *loss of service* attacks from power and bandwidth-limited *smart jammers*, without being hacked by them. The interaction between the network and the *smart jammer* is modeled as a two-player *infinite-horizon Bayesian game with asymmetric information*, with the network being the uninformed player. This research investigates the *smart jamming* problem in LTE/LTE-A networks, by using heuristic analysis, threat mechanism, reinforcement learning and approximated value iteration in repeated games to construct autonomous policies for the network to help it combat these attacks. Moreover, this work is focused on devising policies (algorithms) that can be practically deployed in current networks under realistic constraints, without modifying 3GPP specifications.

The *smart jamming* problem poses many serious challenges in LTE/LTE-A networks. First and foremost, network countermeasures need to be investigated that can not only counteract *smart jamming* attacks, but can also be practically deployed within current 3GPP specifications. Furthermore, the LTE network, the *smart jammer* and their interaction need to be modeled in such a way that all the relevant components are represented accurately while keeping the model tractable. Moreover, the network is modeled as the uninformed

player in an *asymmetric information game* with almost no discernible signals in repeated game, which makes it very hard for the network to learn and strategize. In spite of all, the models and algorithms need to be designed for practical scenarios within realistic constraints and without relying on exogenous information.

The main contributions of this research are manifold. First of all, security vulnerabilities in the LTE/LTE-A air interface are identified that can make 4G networks susceptible to *denial-of-service (DoS)* and *loss of service* attacks. Second, *smart jamming* attacks and network countermeasures are proposed based on their feasible capabilities. Third, the LTE network and its interaction with the *smart jammer* is modeled naturally as a *non-cooperative game with asymmetric information*, with the *smart jammer* being the informed player with multiple types, and the LTE network being the uninformed player with a realistic learning and game dynamics model. Fourth, many efficient algorithms have been presented to estimate the jammer type and compute the strategies against the *smart jammer* and vice versa that can be deployed in real networks. Finally, the algorithms' performance is analyzed and characterized under realistic constraints, which provides reasonable guarantees in practical scenarios.

CHAPTER 1
INTRODUCTION

1.1 The Research Problem

The objectives of this research are to identify security vulnerabilities in LTE/LTE-A air interface; model the network and the *smart jammer* dynamics under realistic constraints; and devise adept algorithms that can help the network combat *smart jamming* attacks autonomously.

1.2 Rationale

Communication networks play a major role in the modern world - they are not only used to connect people but also provide machine-to-machine and human-machine connectivity. These connectivity applications range from social networking to business enterprises; from smart homes to UAVs; from e-health to smart grid; and from Internet-of-Things (IoT) to global communication. Commercial wireless communication networks [1, 2], hold a unique place in the arena of communication networks and cover a wide landscape of Wireless Personal Area Networks WPANs (e.g. Bluetooth), Wireless Local Area Networks WLANs (e.g. WiFi), Wireless Wide Area Networks WWANs (e.g. LTE, LTE-A), device-to-device communication, Internet-of-Things and others. With so many varieties of current and emerging applications of commercial wireless networks a logical question comes arises - how secure and reliable are these networks? Researchers have been looking into security aspects of commercial LTE and LTE-Advanced wireless networks from different perspectives such as physical layer secrecy; network layer security; authentication and encryption; interference and jamming. This research is focused on adversarial jamming of LTE/LTE-A networks, that is, intentional jamming of a network with the intent to sabotage or cheat.

LTE/LTE-A and other commercial cellular networks can be compromised severely by adversarial jamming attacks or high-interference scenarios. If the interference is caused by poor network planning or network overloading, several techniques can be applied to mitigate its effects. However, if this interference is afflicted maliciously (i.e. jamming), its treatment can be very different and may require human intervention. This research is focused on addressing smart jamming problems without any need for human intervention and uses heuristic analysis, threat mechanism, game-theoretic learning and reinforcement learning, and linear programming techniques to design robust network architectures that can combat jamming attacks.

Long Term Evolution (LTE) and LTE-Advanced (LTE-A) [3, 4], networks have been providing advanced data, Voice-over-IP (VoIP), multimedia and location-based services to more than 1.6 billion subscribers in 186 countries around the world [2]. 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. [5, 6, 7, 8, 9, 10, 11, 12]). 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.

LTE/LTE-A networks offer high data rates, flexibility, ease of accessibility, mobility support, ubiquitous coverage and economy of scale [3, 4]. Lately, some researchers have proposed using commercially and privately-owned LTE and LTE-A wireless networks for public safety communications, (cf. [13, 14, 15, 16, 17, 18]); smart grid communications, (cf. [19, 20, 21, 22, 23]); and military communications, cf. [24, 25]. However, being a commercial wireless network its specifications and protocols are publicly known to its designers, developers and general audience around the world. It is a very attractive feature for a commercial network but may not be such a good idea for communication networks used for mission-critical applications. These networks can be severely compromised by jamming attacks that jeopardize operation and robustness of underlying mission-critical applications, such as smart grid, public safety and military operations. This research involves designing algorithms to build robust LTE/LTE-A networks that can combat jamming attacks autonomously. These dynamics are studied and analyzed from a game-theoretical point of view in which the network and the adversary both play opposing roles. By incorporating heuristic analysis, threat mechanism, game-theoretic and reinforcement learning in repeated games, it can be argued confidently that this research culminates in secure communication architectures for mission-critical applications.

1.3 Related Work

A brief survey of the cutting edge theoretical and practical development is presented here as it pertains to this research. Nevertheless, this survey is not complete by any means due to the time and space constraints; and the fact that some of the research areas have recently been very actively pursued among the scientific community.

1.3.1 PHY-layer Security of Wireless Systems

Information security is a real concern for this day and age, and lately its breach has been so widespread that it is terrifying for not only ordinary people but also for big corporations and even the US government [26]. Security attacks in wireless networks can be classified into two broad categories, i.e. *passive* and *active* attacks [27]. Passive attacks include *traffic analysis* and *eavesdropping*. *Shannon* first developed the theory of secrecy systems in his landmark paper [28] to complement the cryptographic techniques used to secure a communication system. Later on, Wyner introduced the wiretap channel in his classic paper [29] as a model of eavesdropper. Since then, information-theoretic security and secrecy has been extensively studied and applied to all areas of information systems including wireless channels [30]. Active security attacks include *denial-of-service (DoS)* attacks, *resource consumption, masquerade* attacks, *replay* attacks, *information disclosure* and *message modification* [27]. This research is focused on *denial-of-service (DoS)* and *loss of service* attacks.

Despite the recent interest and significant progress towards securing wireless physical layer systems, Trappe [31] pointed out that physical layer security techniques still face some real challenges for practical deployments, and that the adversary and wireless channel modeling oversights need to be looked into for such deployments. One of the most common forms of physical layer security attacks include *denial-of-service (DoS)* attacks; and hence physical layer security requirements include resistance to eavesdropping and jamming [27]. Radio frequency jamming attacks can be easily launched by an adversary, causing interference with the normal operation of a wireless network, and cannot be adequately addressed via cryptographic techniques [32]. In the next section, radio frequency jamming attacks pertaining to Wireless Wide Area Networks (WWAN) will be discussed.

1.3.2 Jamming in Wireless Wide Area Networks

Wireless Wide Area Networks (WWAN) provide voice, data, multimedia, and location-based services to billions of subscribers around the world [1, 2]. These networks connect to subscriber terminals (devices) through an air interface, commonly known as 4G, 3G, or 2G wireless networks. All of these cellular/mobile air interfaces, such as LTE/LTE-A, WiMAX, cdma2000, WCDMA, GSM etc., are composed of control and data channels [3, 4]. The control channels carry the critical “handshake” and data channels’ configuration information between the network and the subscriber terminals in order to ensure and utilize efficient operation of data channels and, hence, exchange of user data. However, commercial cellular networks are deployed for public use, and as such their specifications and deployments are easily accessible to the general audience. This makes commercial cellular networks more vulnerable to jamming attacks than their private counterparts and LTE/LTE-A is not an exception.

LTE being a commercially deployed wireless network raises serious security concerns, such as *denial-of-service (DoS)*, data integrity and information privacy attacks [33]. Researchers in [34, 35] also pointed out security vulnerabilities in LTE networks related to flat all-IP based system architecture, access authentication procedures, etc. Moreover, OFDM-based systems like LTE are less resistant to jamming and interference as compared to their counterpart spread spectrum systems. Hence, researchers like Stüber, Clancy, Trappe, and their colleagues, have independently identified and analyzed the performance of OFDM systems under pilot jamming [36], pilot nulling [37] and synchronization jamming [38] attacks respectively. However, vulnerability of wireless networks to jamming attacks is not limited to LTE and as such all wireless networks are susceptible to it. For example, [39] studied the performance of a WiMAX system under jamming attacks; [40] evaluated the performance of GSM robustness against smart jamming attacks; and [41] studied the effects of protocol-aware shot-noise pulse-based jamming attacks in WiFi networks.

Radio frequency jamming refers to intentional blocking or disruption of ongoing communication between two or more devices/networks, and can be either benign or malicious. It works by decreasing the Signal-to-Interference-plus-Noise ratio (SINR) at the desired receiver by injecting interference in the wireless channel or directing it at the receiver. In addition, cellular networks are subjected to unintentional *Inter-Cell Interference (ICI)* from surrounding cells, on a regular basis during their normal operation. A well-designed cellular system is, by nature, interference-limited [42]. Lately, there has been increasing interest within the engineering community in alleviating ICI in LTE/LTE-A and other cellular networks. Andrews *et al.* [42] discussed prospects of various existing and potential ICI mitigation techniques, such as frequency reuse, Multiuser Detection (MUD), interference cancellation, stream control etc., and advocated the use of strategic techniques like networked MIMO, and distributed antenna architectures that require very little channel knowledge. Yang [43] provided an industry perspective of ICI mitigation techniques, including Fractional Frequency Reuse (FFR), and Coordinated Multi-Point (CoMP) techniques. CoMP techniques require coordinated transmissions from all the nodes participating in the scheme and utilize geographically distributed multiple antennas to reduce ICI. Burchardt and Haas [44] discussed the development of various cooperation techniques in large cellular networks including user-based cooperation, system-wide optimization and multiple-base-station transmission. They argued that simple frequency reuse and power control may not be enough to meet the growing demand of mobile data communication. Similarly, Soret *et al.* [45] discussed the potential of enhanced Inter-Cell Interference Coordination (eICIC) and cooperative inter-site Carrier Aggregation (CA) techniques for co-channel interference and dedicated carrier deployments in a heterogeneous LTE-A network. Lastly, El Ayach *et al.* [46] discussed practical challenges associated with deployment of interference alignment techniques that require coordination among multiple transmitters. However, since this research deals with the malicious interference, i.e. the jamming problem, it is assumed that ICI has already been managed by the network.

Although jamming is detrimental to wireless networks in general, it can sometimes be used by the network to block access to unwanted users and protect desired communication, cf. [47, 48, 49, 50]. For example, Yener and Ulukus [50] discussed the idea of cooperative jamming, in which secrecy rate of a multiple access wiretap channel can be increased by introducing judicial interference by some terminals in the network. Similarly, researchers have come up with some interesting schemes to combat jamming attacks in non-OFDM-based wireless networks. For example, Asterjadhi *et al.* [51] proposed the use of network coding in order to protect broadcasting in multi-channel wireless networks. Also, [52, 53, 54, 55] proposed anti-jamming frequency-hopping techniques for spread spectrum systems; for example, Pöpper *et al.* [54] proposed uncoordinated spread spectrum techniques to enable anti-jamming broadcast communication in the presence of malicious receivers.

This research deals with the intelligent jamming of control channels, which has been actively researched lately. Thuente *et al.* [56] explored the effectiveness of intelligent jamming in IEEE 802.11b networks. Petracca *et al.* [40] evaluated performance of GSM networks' robustness against control channel jamming attacks. The authors showed that GSM network's security can be significantly compromised by such attacks. Similarly, Lo and Akyildiz [57] addressed the problem of intelligent jamming of control channels in Cognitive Radio Ad Hoc Networks (CRAHNs) by proposing a jamming-resilient control channel algorithm that enables user cooperation. Moreover, Liu *et al.* [58] explored the case of a cognitive radio ad-hoc network suffering from control channel jamming attacks from inside jammers. The authors proposed algorithms for unique identification of the set of compromised nodes. Furthermore, Hussain *et al.* [41] investigated the effects of shot-noise based protocol-aware jamming in WiFi networks.

This research particularly deals with the "smart" jamming of LTE/LTE-A control channels. Recently, Reed [5] brought the attention of the US Department of Commerce to potential control channel vulnerabilities in LTE networks. Since then, a team of researchers led by Reed and Clancy at Virginia Tech, cf. [6, 9, 59], has been independently involved in identifying potential vulnerabilities of LTE networks to hostile interference and proposing possible solutions, such as randomization of reference signals, and use of cryptographic techniques. Similarly, Jover *et al.* [7] explored the issue of smart jamming attacks on an LTE network and proposed some possible solutions, like use of spread-spectrum techniques, LTE system message encryption, uplink control channel scrambling, and uplink interference cancellation. However, these proposed solutions often require major changes in LTE/LTE-A specifications which are not backward-compatible with existing deployments, and sacrifice network efficiency and availability significantly due to excessive overhead and suggested solutions. Furthermore, they do not prevent attacks caused by "rogue" LTE-capable devices. Nevertheless, the impact of "smart jamming" attacks on the performance of LTE/LTE-A networks is an open problem and has not been well researched yet.

1.3.3 Game Theory in Wireless Networks

Game theory (cf. [60, 61, 62, 63, 64, 65, 66]) 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. [67, 68, 69, 70]) 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. [8, 10]), with the network being the uninformed player. Asymmetric information games (cf. [61, 63, 64, 65, 66]) 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. [61, 63]). 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. [71, 72, 73, 74]). 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 ([75]). 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 problem gets further complicated for general-sum (non-zero-sum) games with imperfect monitoring, which is still an open problem [76]. This research addresses the lack of information problem, in the infinite-horizon general-sum repeated game with imperfect monitoring, by devising a state estimation algorithm to resolve the uncertainty of the uninformed player.

Although the interaction between the network and the jammer is modeled as a *Bayesian game with asymmetric information*, this interaction can also be modeled as a *Bayesian Stackelberg game with asymmetric information*, with the network being the leader and the jammer being the follower. *Stackelberg leadership* or *commitment model* was originally introduced by von Stackelberg in 1934 [77] for a static duopoly, in which the leader moves first and commits to a strategy followed by the follower(s) who *best responds* after observing leader's move. It is now very frequently applied to solve competitive scenarios in wireless networks, cf. [78, 79, 70]. The main solution concepts for simultaneous-moves and Stackelberg games are NE and SSE respectively. Conitzer and Sandholm [80] discussed how to compute optimal strategies to commit to in a Bayesian Stackelberg game, under both types of commitment scenarios, i.e., commitment to pure strategies and commitment to mixed strategies. They argued that if commitment to mixed strategies is possible, as opposed to simultaneous play, then optimal commitment never hurts the leader. They further showed that the problem of finding an optimal pure strategy to commit to is NP-hard in general Bayesian games, but can be solved efficiently for two-player Bayesian games when the leader has only a single type. Moreoever, the problem of finding an optimal mixed strategy to commit to is NP-hard in general Bayesian games, even for the two-player case when leader has only a single type. This implies that computing optimal network strategies for such a problem could be quite challenging.

There has been substantial work done on a specific type of Stackelberg games in the security community, namely *Stackelberg Security Games (SSGs)* - two-player games in which the defender commits to a randomized deployment of security resources and the attacker *best responds* by attacking a target that maximizes his utility. Krozhyk *et al.* [81] discussed interchangeability, equivalence, and uniqueness of SSE vs. NE in a security game. It showed that NE in security games are interchangeable, alleviating the equilibrium selection problem for simultaneous-move games, and under very specific additional constraints SSE strategies are a subset of NE strategies. However, SSE strategies fail to be a subset of NE strategies when either of those restrictions fail, or attacker can attack multiple targets. Similarly, Vorobeychik and Singh [82] showed that there does not always exist a SSE in Markov stationary policies in stochastic Stackelberg games, and presented a finite-time mixed-integer non-linear program for computing a Stackelberg equilibrium when the leader is restricted to Markov stationary policies. Moreover, Vorobeychik *et al.* [83] showed that the defender's Markov stationary policies can be arbitrarily suboptimal for a specific class of security games known as infinite-horizon discounted Adversarial Patrolling Games (APGs), in which the attacker can observe the current location of the defender and can exploit this knowledge to infer future moves. Xu *et al.* [84] proposed strategically revealing information about sampled pure strategy to improve defender's utility beyond SSE in SSGs. Balcan *et al.* [85] argued that optimal defender strategies in SSGs require significant information about potential attackers, and proposed a no-regret online learning algorithm instead. Furthermore, Zheng and Castanon, cf. [86, 87], formulated network interdiction problems (zero-sum games between an attacker and an intelligent defender who adapts its operations to counteract the effects of attacker), as zero-sum min-max Stackelberg games.

This research is focused on computing network strategies that it can deploy while being uninformed about the jammer type, but not in Stackelberg game setting. Apparently, there is vast literature available on SSGs and network interdiction games, and there are many similarities between our work and SSGs and network interdiction problems. Yet, our research model differs significantly from those models, and realistic modeling and observational constraints make solving the underlying research problem much more challenging!

1.3.4 Asymmetric Information Games

Game-theoretic tools have been applied to model the interaction between the LTE network and the *smart jammer*. The network's repeated game strategies (cf. [8], [10]) to combat smart jamming attacks are presented in Chapter 4, but they are 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. [62], [61]). The *evolved threat-based state estimation algorithm* presented in Chapter 4 is utilized by the network to estimate the jammer type. This 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 [61], Chapter 4 of [63], Chapters 2 - 4 of [64], and Chapter 2 of [65]. However, most of the prior work on asymmetric zero-sum repeated games revolves around the informed player's viewpoint. For example, [61] and [63] 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, [64] 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, [80] 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. [71, 72, 73, 74]) 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 [75]. 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. [74, 88]). The uninformed player's sufficient statistics and computation of his optimal security strategy still are open problems. Recently,

[74] used realized regret vector as the uninformed player's sufficient statistics to compute its efficient but suboptimal strategy in finite-horizon asymmetric zero-sum repeated games. Furthermore, [75] 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. Moreover, a recent development in [89] extends the approach used in [74] to λ-discounted infinite-horizon zero-sum repeated games with asymmetric information. 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 [61] and Chapters V and IX of [66] 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 [66] 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, [76] 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 research.

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, [71, 72, 73, 74] 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, [90, 91, 92, 93] used a Bayesian approach to devise an uninformed player's strategy based on expected payoff. Furthermore, [76] 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, [94] 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. [67, 68, 69, 70]), and network security (cf. [95, 96]). Among the security games, Security Stackelberg Games (SSGs) (cf. [96, 77]) 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 formulation. The same assumption is followed in network interdiction games [87], 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 [97], similar to our formulation. However, [97] 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 [98], 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. [99, 100]) in which the jammer can tune its transmit power, adapt attack duration and choose to save energy similar to our model. However, there are many fundamental differences between these formulations and our model. For example, [99] 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 [99], the user is aware of the jammer's existence and intelligence, which is in contrast with our model that requires jamming sense. Also, [99] assumes that the user can compute the jammer's Best Response (BR), and fading channel gains of the opponent player are known. Our model makes no such assumptions for its algorithm design and analysis. On the other hand, [100] 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 uninformed player's strategy and opponent's type estimation in an infinite-horizon asymmetric repeated game without "full monitoring". Therefore, I am confident that this research attempts to solve a unique problem at the intersection of *smart jamming* attacks in LTE networks and non-cooperative game theory!

CHAPTER 2

SMART JAMMING IN LTE NETWORKS

Long Term Evolution (LTE) and LTE-Advanced (LTE-A) [3, 4] 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, it is shown 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. A typical *smart jammer* implementation uses USRPs to launch jamming attacks and is shown as a block diagram in Fig. 2.1. Potential *smart jamming* attacks and suggested network countermeasures are briefly presented in this chapter.

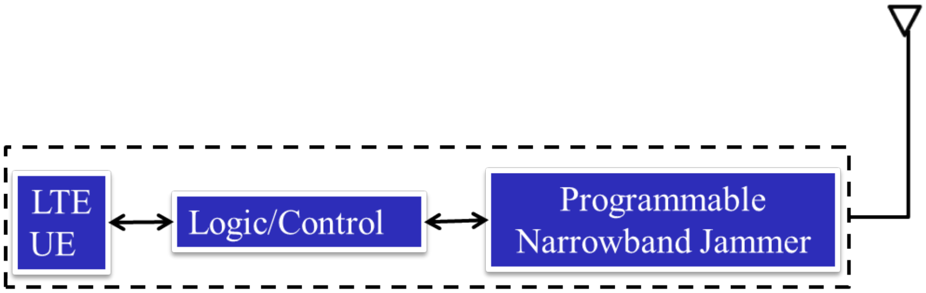

Figure 2.1: A Typical Smart Jammer Implementation

2.1 Potential Smart Jamming Attacks on an LTE Network

A wireless jammer can be classified as any of the following types based on its jamming technique.

- Barrage jammer
- Pulse jammer
- Partial-band jammer
- Single-tone/multi-tone jammer or
- Smart jammer

A *smart jammer* can "learn" the network timing and physical layer parameters to jam it 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 *Denial-of-Service (DOS)* and *loss-of-service* attacks. Moreover, if a UE is unable to receive *Cell-SpecificReferenceSignal(CS-RS)* reliably ($\leq 2\%$) for 5-10 *DiscontinuousReception(DRX)* cycles then it goes *out-of-sync* [4]. 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 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 instances 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*.

Inactive mode 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

[1] See [3] or [4] for the description of various LTE channels.

channels and transmit both in the Uplink and Downlink to achieve its goals. Jamming *Cell-Specific Reference Signal (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. [36]. Jamming Physical Control Format Indicator Channel (PCFICH) may cause loss of *Control Format Indicator (CFI)* in the Downlink. *CFI* indicates the control region associated with Physical Downlink Common Control Channel (PDCCH), which carries all essential control information and grants associated with both the Downlink (DL) and Uplink (UL). A UE may attempt blind CFI decode but it could be too slow resulting in missed grants which might result in *Radio Link Failure (RLF)* or the UE might go *out-of-sync*. Jamming Physical Uplink Control Channel (PUCCH) may cause eNode B to loose track of critical feedback information from UEs. Jamming Physical Broadcast Channel (PBCH) and Physical Random Access Channel (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, it is assumed that a fraction of UEs try to access it at any given resource instant. If the jammer's signal is received at the eNode B along with other legitimate users, it will need to perform contention resolution which may fail because of the jammer presence. Hence, the jammer only needs to make sure that its signal is received with high enough power at the eNode B receiver.

2.2 Suggested Network Countermeasures

LTE air interface is an OFDM-based radio link designed to connect subscriber terminals known as the *User Equipment (UE)* to network interface known as the *eNode B* [3]. A UE has to follow a certain (hence vulnerable) call flow of *control* and *data channels* to send an *attach request*; and/or send/receive data. Although this work is focused on *Frequency*

Division Duplexing (FDD) mode networks; it can be easily extended to *Time Division Duplexing (TDD)* mode as well.

As of today, 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 on a regular basis and launches jamming attacks probabilistically. In the event of incomplete jamming information (jammer's location, jamming waveform, probability of jamming, etc.) available at the network, it is proposed that an LTE network can take the following countermeasures:

1. Normal Mode (*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*)

Normal mode refers to the default day-to-day operation of the network. However, 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 f_c 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. Moreover, SIB 2 parameters' change may prevent PRACH and PUCCH failures caused by jamming. However, this would require very carefully planned reconfiguration at the network side and the cell would not be available during the transition period.

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 [101].

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 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.

CHAPTER 3
LTE NETWORK & SMART JAMMER DYNAMICS

In this Chapter, LTE network and smart jammer dynamics are presented in terms of network and game-theoretic models.

3.1 Network Model

It is assumed 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 the 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. It is also assumed that the 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.

3.1.1 Channel Model

All transmit signals go though large-scale path loss which is modeled using *Simplified Path Loss Model* [101] represented by (3.1).

$$P_r(dBm) = P_t(dBm) + K(dB) - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) \tag{3.1}$$

where P_r is the received power, P_t is the transmitted power, $K(dB) = 20\log_{10}\left(\frac{\lambda}{4\pi d_0}\right)$ is a constant, γ is the *path loss exponent* with typical values from 2.7 - 3.5 for urban microcells, d is the distance between transmitter and receiver, and d_0 is the outdoor reference distance for antenna far field. The small-scale multipath fading is modeled as *Rayleigh-faded exponentially distributed* channel gains for simple **Narrowband Model**; whereas it is modeled

Table 3.1: Power Delay Profile of EVA Channel Model

Tap No.	Excess Tap Delay (ns)	Relative Power (dB)
1	0	0.0
2	30	-1.5
3	150	-1.4
4	310	-3.6
5	370	-0.6
6	710	-9.1
7	1090	-7.0
8	1730	-12.0
9	2510	-16.9

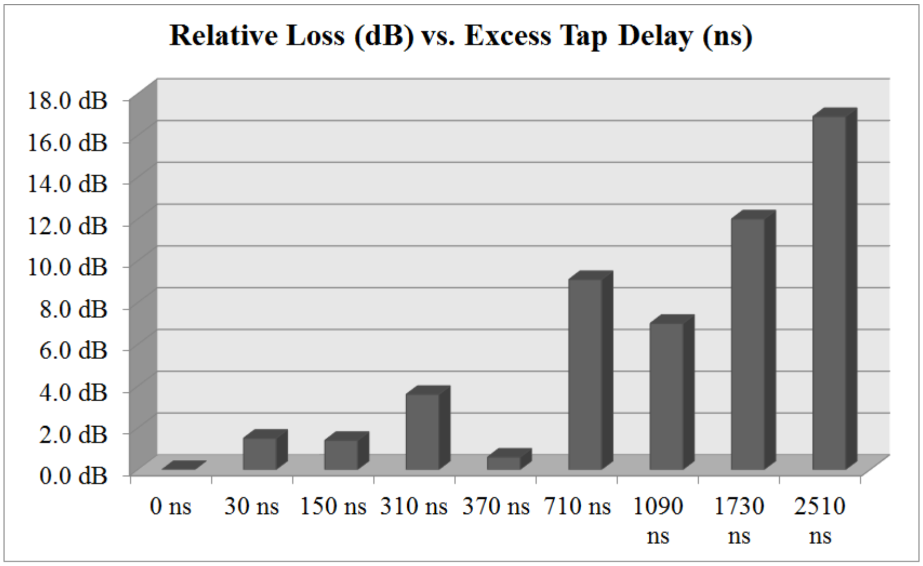

Figure 3.1: 3GPP’s Extended Vehicular A (EVA) Wideband Channel Model

as per *3GPP/ITU’s Extended Vehicular A (EVA)* channel model (cf. [3, 4]) for **Wideband Model** with *maximum Doppler frequency of 70 Hz* (which corresponds to maximum speed of 35 km/h at 2140 MHz). The power delay profile of 3GPP’s *EVA* channel model is given in Table 3.1 and plotted in Fig. 3.1.

3.1.2 SINR Model

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

$$\Gamma[k] = \frac{P_0[k]|h|^2 K(\frac{R_0}{d_0})^{-\gamma}}{\sigma^2 + P_j[k]|g|^2 K(\frac{R_j}{d_0})^{-\gamma}} \tag{3.2}$$

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 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 SINR model presented above. Therefore, any residual ICI can be lumped together in σ^2 for the scope of this research. It is further assumed that σ^2 is the same at all receivers.

The SINR in (3.2) 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 $(\frac{C}{J})$.

$$\Gamma[k] = \frac{(\frac{C}{J})|h|^2 K(\frac{R_0}{d_0})^{-\gamma}}{(\frac{\sigma^2}{P_j[k]}) + |g|^2 K(\frac{R_j}{d_0})^{-\gamma}} \tag{3.3}$$

However, (3.2) or (3.3) 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, (3.2) or (3.3) can be used to model their SINR accurately. But, (3.2) or (3.3) cannot be used to model the SINR of LTE's wideband data channels like PDSCH and PUSCH.

3.1.3 SINR Estimation

SINR estimation is done in the frequency domain by estimating noise and interference power in frequency domain as suggested in [102]. The received time-domain symbols can be expressed in frequency-domain as follows:

$$Y_i[k] = H_i[k]X_i[k] + G_i[k]J_i[k] + W_i[k] \tag{3.4}$$

where H_i, and G_i represent channel frequency responses for desired transmitter and jammer's signals; X_i, and J_i represent desired transmitted signal and jamming waveform; and W_i represent DFT of i.i.d. AWGN noise at the receiver. The instantaneous noise and interference power $\hat{E}_m[k]$ is estimated for each OFDM subcarrier by finding the difference between each received (noisy) sample and the best hypothesis of noiseless received signal, as shown in (3.5) below.

$$\hat{E}_m[k] = |Y_m[k] - \hat{X}_m[k]\hat{H}_m[k]|^2 \tag{3.5}$$

where $\hat{X}_m[k]$ and $\hat{H}_m[k]$ are the best hypotheses of desired symbol and channel estimate for the *k*th subcarrier of the *m*th OFDM symbol. Thus, (3.5) can be used to estimate the SINR of a link in LTE network by computing the quantity $\frac{\hat{X}_m[k]}{\hat{E}_m[k]}$.

3.1.4 Throughput & Multiuser Scheduling Model

It is widely known that fading channel's capacity can be modeled as a fraction of AWGN channel capacity [101]. Since LTE data channels operate close to *Shannon Capacity* at high data rates and *smart jamming* does not target data channels, mth user's DL PDSCH throughput $\mathcal{R}_m(k, l)$ in kth Resource Block during lth subframe can be approximated as *Shannon's AWGN Channel Capacity* as shown in (3.6).

$$\mathcal{R}_m(k, l) = \mathbb{W}_{\text{RB}}\ log_2[1 + \Gamma_m^{\text{PDSCH}}(k, l)] \tag{3.6}$$

where $\mathbb{W}_{\text{RB}}$ is the bandwidth of a single RB i.e. 180 kHz.

A UE's throughput in a subframe would be the sum of its assigned RBs' throughput. It is assumed 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, well-known closed form expression for QPSK Symbol Error Rate (SER) performance in Rayleigh fading [101], is used to convert desired BLER performance threshold into required average SINR, i.e. $\overline{P_s} = \left(1 - \sqrt{\frac{\overline{\Gamma_s}/2}{1+\overline{\Gamma_s}/2}}\right)$ (where $\overline{P_s}$ = average QPSK symbol error probability in Rayleigh fading, and $\overline{\Gamma_s}$ = average 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, a combination of the Union Bound for coded PSK symbol error probability [103], i.e. $P_M < 2^k \binom{2d_{min}-1}{d_{min}} \left(\frac{1}{4R_c\overline{\Gamma_b}}\right)^{d_{min}}$ (where P_M = coded M-PSK symbol error prob., $M = 2^k$, R_c = code rate, d_{min} = minimum distance of channel code and $\overline{\Gamma_b}$ = avg. SNR per bit), channel code's *free distance* d_{free} derived from 3GPP *LTE* specifications [3], and equally likely symbol error probability across entire block of a particular signal is used to convert desired BLER performance into required average SINR.

It is modeled that eNode B uses Proportional Fair Scheduling (PFS) [104] algorithm to allocate resources to its users that survive jamming attacks. PFS provides a good balance in multiuser scheduling between eNode B throughput performance and fairness among users. User m is allocated in Resource Block k during lth subframe if the ratio of his achievable instantaneous data rate and long-term average throughput in (3.7) is the highest among all the users in the network. The long-term average throughput of user m, $\overline{\mathcal{R}}_m(l)$ during subframe l is computed using the recursive equation (3.8).

$$\hat{m}_k = \underset{m'=1,\ldots,N}{\arg\max} \left\{ \frac{\mathcal{R}_{m'}(k,l)}{\overline{\mathcal{R}}_{m'}(l)} \right\} \tag{3.7}$$

$$\overline{\mathcal{R}}_m(l) = \left(1 - \frac{1}{t_c}\right) \overline{\mathcal{R}}_m(l-1) + \frac{1}{t_c} \sum_{k=1}^{K} \mathcal{R}_m(k,l) \mathcal{I}(\hat{m}_k = m) \tag{3.8}$$

where t_c represents fairness time window, and $\mathcal{I}$ is an indicator function.

3.1.5 Network Dynamics

An LTE network can be abstracted as a highly nonlinear dynamical system that can be represented by (3.9).

$$\chi^{+} = f(\chi, \theta, a^{0}, a^{j}, \omega) \tag{3.9}$$

where $\chi \in \mathbb{R}^{M \times N}$ represents the state of the network (not to be confused with the game-theoretic state of nature) with each row corresponding to the user $m \in M$, including N 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 game-theoretic 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 both players (jammer cannot access network users' states 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*.

3.2 Game-Theoretic Model

The network dynamics (interaction between the LTE network and the smart jammer) are modeled as an **infinite-horizon** [1] **two-player general sum Bayesian game $\mathcal{G}$ with asym-**

[1] Infinite-horizon model is used when the players believe that the game will continue for an additional stage after each stage, i.e., there is a non-zero probability associated with game continuation at the end of each stage [62]

metric information, cf. [62, 61, 63]. The game $\mathcal{G}$ is described by

- $\mathcal{N}$ = {eNode B, jammer}, the set of players,
- Θ, the set of states of nature (jammer types),
- $p_0 \in \Delta(\Theta)$, the common prior probability distribution on Θ, where $\Delta(\Theta)$ represents the set of all probability distributions over Θ,
- $\mathcal{A}_0$ and $\mathcal{A}_j$, the set of pure actions of the eNode B, and the *smart jammer*, respectively as described in Chapter 2, and $a^0 \in \mathcal{A}_0$ and $a^j \in \mathcal{A}_j$ represent corresponding elements in these sets,
- $\mathcal{H}$, a set of sequences such that each $h \in \mathcal{H}$ is a history of observations,
- $\mathcal{I}_i$, the information partition of player i and
- $\mathcal{U}_i \colon \Theta \times \mathcal{A}_0 \times \mathcal{A}_j \to \mathbb{R}$, the utility function of player i.

3.2.1 Jammer Types

The state of nature, i.e. 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**

The type *Normal* refers to the state when there is no jammer present in the network, i.e. the network is operating in its default conventional mode. 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. It is to be noted here that the type *Normal* should not be confused with the jammer being *inactive*, where latter merely represents an action that might be played by the *smart jammer*.

3.2.2 Strategies

A *pure strategy* of a player is a mapping from each non-terminal history to a pure action and a *mixed strategy* is defined as a probability measure Δ over the set of its pure strategies. Whereas, a *behavioral strategy* specifies a probability measure Δ over its available actions at each point when an action needs to be taken [62]. Both the network and the jammer are modeled as as *rational* and *strategic* players with the exception of *evolved jammer type estimation algorithm* when the jammer is modeled as *"myopic" (non-strategic)*, i.e., the jammer would play a myopic best response [2] 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, such as [97]. Also, this assumption makes perfect sense in the assumed model as the jammer wants to either "cheat" the network or inflict maximum damage to it in the shortest possible time without getting caught.

3.2.3 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 on the states of nature, i.e. $p_0 \in \Delta(\Theta)$. This results in a **game with asymmetric information**, with lack of information on the network side, making **eNode B the uninformed player**.

[2] The *best response* (BR) is the strategy (or strategies) that produces the most favorable outcome for a player given other players' strategies [60].

3.2.4 Observable Signals

Unlike the formulation described in classic game-theoretic literature like Chapter 6 of [61] etc., players can only observe their own payoffs but not opponent's actions due to inherent randomization and inaccessibility of information in the network. This means that the "full monitoring" [3] assumption cannot be realistically made in the modeled dynamics. The eNode B's 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 with certainty. All of these impediments make adversary type and actions' estimation very difficult for eNode B, further complicated by inherent randomization in the links caused by channel variations, UEs' locations and mobility, PFS scheduling etc..

The *Cheater*'s observable signals include its own downlink SNRs, resource block(s) 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 on a regular basis.

[3] All players can observe the previous actions of their opponents after each stage [61].

3.2.5 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 in (3.10).

$$\mathcal{U}_i = \sum_{l=1}^{L} \alpha^l \mathbb{E}_\omega [g_i^l(\theta, a_i, a_{-i})] - \mathcal{C}_i(a_i) \tag{3.10}$$

where α^l represents weight of the l^{th} KPI normalized with respect to the baseline jamming-free scenario, $\mathbb{E}_\omega$ represents the spatio-temporal expectation with respect to the randomness caused by ω described in (3.9), g^l represents the l^{th} normalized KPI as a function of the jammer type θ, action of the *i*th player a_i, and action of the player other than the *i*th player a_{-i}, and $\mathcal{C}_i$ represents fixed cost of *i*th player as a function of his 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 with the exception of the preliminary narrowband model results presented in Chapter 4 and [8]. For eNode B, KPIs include throughput/UE, number of *Connected Mode* UEs, CS-RS, PUCCH, PCFICH SINRs, PRACH failure rate, and transmit duty cycle τ_{eNB}. For *Cheater*, KPIs include its own throughput and transmit duty cycle τ_{c}. For *Saboteur*, KPIs include the negative of the eNode B throughput/UE, the negative of number of *Connected Mode* UEs and its own transmit duty cycle τ_{s}. 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 transmit 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 transmit 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, explored in Chapter 4, due to the asymmetry of objectives and KPIs among different players. The general-sum game is converted to more tractable **zero-sum** formulation in Chapter 5.

3.2.6 Game Play

At the beginning of the game, nature flips a coin and selects $\theta \in \Theta$ (type of adversary) according to $p_0 \in \Delta(\Theta)$, which remains fixed for the rest of the game. It is assumed that $p_0^\theta > 0, \forall \theta \in \Theta$, without loss of generality. The jammer is informed about its selected type but eNode B is not. This leads to a **game with asymmetric information**, with **eNode B being the uninformed player**, and *smart jammer* being the informed player. Although eNode B is unaware of the jammer type, it's history would evolve with time in a *repeated game* by repeated interaction with the jammer that could affect its belief about true state of nature, i.e. θ.

CHAPTER 4

GENERAL-SUM GAME ALGORITHMS

The *smart jamming* problem in LTE/LTE-A networks has been modeled in Chapter 3 as an infinite-horizon general-sum (non-zero-sum) repeated Bayesian game with asymmetric information (cf. [8, 10, 12]) 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. [61, 63, 64, 65, 66]), with the network and the jammer being the uninformed and informed player, respectively. To the best of my knowledge, there does not exist any efficient and optimal formulations for the uninformed (or informed) player's strategy computation in infinite-horizon repeated general-sum games with asymmetric information and partial monitoring. Hence, heuristic algorithms are devised for strategy computation and type estimation that do not require any feedback from the network users nor do they rely on a specific distribution (e.g., Gaussian) of test statistic and are implemented without any notion of "full monitoring" (i.e., players cannot observe opponent's actions). The LTE network can combat *smart jamming* attacks autonomously by employing the repeated game algorithms presented in this chapter (cf. [8, 10]). However, these network strategy algorithms are contingent upon a specific jammer type. Hence, state estimation algorithms (cf. [8, 12]) are also presented in this chapter to estimate the jammer type, which are based on non-parametric estimation and threat mechanisms in repeated games.

4.1 Narrowband Strategy Algorithms

4.1.1 Single-Shot Game

In the *single-shot game*, a *smart jammer* infringes on regular network communication by playing pure or mixed strategy over the jamming actions mentioned in Chapter 2. Since jammer is power and resource limited, it tries to jam as few control channels as possible while maximizing its utility. The eNode B counteracts as a result of jammer's infraction and plays a pure or mixed strategy over countermeasures described in Chapter 2. 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 in which every player's set of actions is finite, has at least one mixed strategy *Nash Equilibrium (NE)* [1] [62].

Single-Shot Game Simulation Results

The following simulation parameters are used for MATLAB simulations based on their anticipated significance:

- $\alpha^{\text{UE}} = 80,$
- $\alpha^{\text{Tput}} = 50,$
- $\alpha^{\text{RS}} = 10,$
- $\alpha^{\text{PUCCH}} = 8,$
- $\alpha^{\text{RACH}} = -25,$
- $\alpha^{\tau} = -25,$
- $\mathcal{C}_{\text{eNB}}^{RS} = 20,$

[1] No single player can obtain a higher utility by deviating unilaterally from a NE by choosing a different strategy other than the one used at that particular NE [62].

- $\mathcal{C}_{\text{eNB}}^{\text{throttle}} = 0$,
- $\mathcal{C}_{\text{eNB}}^{\text{f Change}} = 50$,
- $\mathcal{C}_{\text{eNB}}^{\text{t Change}} = 80$,
- $\text{BLER}_{\text{threshold}} = 10\%$,
- $C/J =$ 20 dB,
- $p_j = 0.7$,
- path loss exponent $\gamma = 3.5$,
- LTE carrier frequency $f_c =$ 2140 MHz, and
- UE arrival rate $\lambda = 8$ UEs/Km^2,

where C/J, and p_j denote *Carrier-to-Jammer power ratio* and *probability of jamming* respectively. The utility results obtained from the 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 $\mathcal{U}_{0,c}$ utility matrix representing eNode B vs. Cheater simulation results is given as follows:

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

Similarly, $\mathcal{U}_{0,s}$ utility matrix representing eNode B vs. Saboteur simulation results is given as follows:

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

In the case of **Cheater**, the single-shot 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 the case of **Saboteur**, the game has a **mixed strategy NE** with expected payoff of **(-81.32,0.68)**. This mixed strategy NE corresponds to assigning probability distribution of $[0.04, 0.05, 0, 0, 0.91]^T$ and $[0.67, 0.28, 0, 0, 0.05]^T$ 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 as evident from its very low utility values. It is to be noted here that the best possible utility value for eNode B is zero as compared to its baseline jamming-free scenario. Also, some network actions are strictly dominated against a particular type of adversary, e.g., *'Change f_c'* and *'Timing Change'* against *Cheater*. Hence, the network strategy depends on the adversary action as well as its type. Similar trends are observed at other values of C/J and p_j.

4.1.2 Infinite-horizon Repeated Bayesian Game with Asymmetric Information

Single-shot games are less appealing from convergence and implementation point of view. On the other hand, *repeated games* can potentially provide further opportunities for improving network utility by learning and utilizing game dynamics. Hence, in this chapter, a *repeated Bayesian game* [62] is used to model the game dynamics. Also, *repeated game* *algorithms* are presented for the network and the adversaries. All measurements and actions required by the strategy computation and state estimation algorithms are within the capabilities of both the network and the adversaries without changing LTE specifications significantly. In other words, they are practically implementable in current LTE networks with minor changes. It is assumed that a certain probability of occurrence is associated with each adversary, and 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 research.

eNode B's Jammer Type Estimation Algorithm

Based on the single-shot game simulation results, the network's *Best Response (BR)* depends on the type of adversary it faces. Hence, it is important for the network to determine the jammer type, if detected. A repeated game algorithm is presented in Fig. 4.1 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_c'* for few consecutive frames respectively.

The baseline statistics are defined in terms of observed samples collected during initial jamming-free observations and decisions are made based on level (threshold) crossing of ongoing observations against baseline statistics. For example, the eNode B's baseline CS-RS and PUCCH SNR statistics are defined as: $\nu^{\text{RS}}_{\text{baseline}} = \mu^{\text{RS}}_{\text{initial}} - \sigma^{\text{RS}}_{\text{initial}}$, and $\nu^{\text{PUCCH}}_{\text{baseline}} = \mu^{\text{PUCCH}}_{\text{initial}} - \sigma^{\text{PUCCH}}_{\text{initial}}$, where ν represents the baseline statistic, μ represents mean and σ represents standard deviation. Jamming sense decision is made by the eNode B if the ongoing sliding window SNR observations fall below certain thresholds, i.e., when $\mu^{\text{RS}}_{\text{obs}} < 1.135\ \nu^{\text{RS}}_{\text{baseline}}$ or $\mu^{\text{PUCCH}}_{\text{obs}} < 0.85\ \nu^{\text{PUCCH}}_{\text{baseline}}$. Jamming sense decision results in the declaration of 'Jammer Present' with a probability $1 - p_{\text{false}}$ as shown in the Fig. 4.1. Sim-

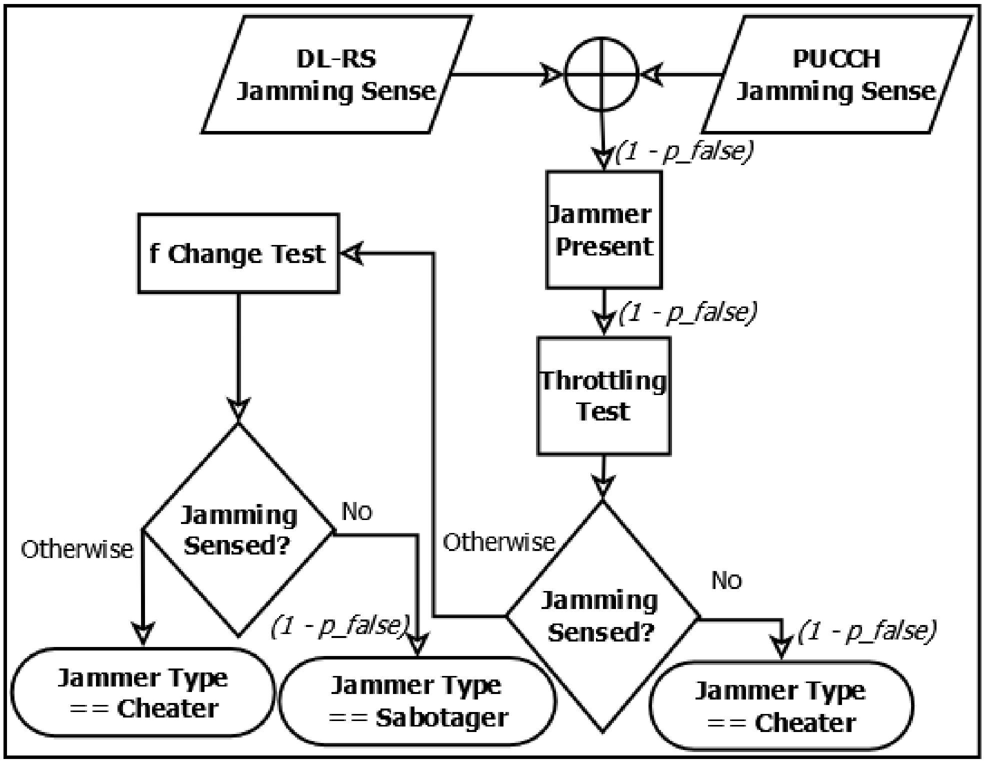

Figure 4.1: eNode B's *Narrowband* Jammer Type Estimation Algorithm

ilar manipulations are done for Cheater and other eNode B baseline and decision statistics. Obviously, all of the coefficients used in the statistics' definition are configurable. The jammer type estimation algorithm's true estimation probability $p(\hat{\theta}|\theta)$ for $\frac{C}{J} = 20\text{dB}, p_j = 0.7$, and $p_{false} = 0.10$ is given below in the form of a matrix. Other configuration parameters include initial jamming-free observations window length = 40 subframes, eNode B's observations sliding window length = 10 subframes, Cheater's observations sliding window length = 10 subframes, 'throttling' test duration = 30 subframes, and 'f Change' test duration = 20 subframes.

$$p(\hat{\theta}|\theta) = \begin{bmatrix} 0.06 & 0.16 & 0.78 \\ 0.07 & 0.37 & 0.56 \\ 0.09 & 0.09 & 0.82 \end{bmatrix}$$

Ideally, the above matrix should be diagonal. But, at a high value of $\frac{C}{J} = 20$ dB, jamming effects are too subtle to sense so SNR values are not much affected by jamming and hence, a lot of false alarms are detected. On the other hand, with the above-mentioned configuration parameter values, the algorithm gets biased towards *Saboteur*, i.e. it tends to declare its presence (and often erroneously) much more often. However, the algorithm can be tweaked for a certain performance (detection) level since there are many degrees of freedom built into it, provided that enough data is available for tweaking. Furthermore, the jammer type estimation algorithm converges in 96 subframes on average.

Repeated Game Learning and Strategy Algorithms

After jammer type determination, eNode B uses the algorithm presented in Fig. 4.2 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 that action is played. It is to be noted here that the eNode B merely forms an estimate of jammer type which may or may not represent the true state. Also the presented actions' algorithm forms beliefs about network state and adversary's actions based on its observations and may not always be true as well. This phenomenon is typical for a stochastic environment with incomplete information.

Similarly, jammer personalities, i.e. *Cheater* and *Saboteur* devise their own corresponding strategy for the repeated game. Their strategies are presented in Figs. 4.3 and 4.4, respectively. Similar to eNode B, adversaries are also unaware of network state (not to be confused with system state, i.e., state of nature) 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 the dark by the network. Therefore, *Saboteur* keeps re-synchronizing itself with the network on regular intervals denoted by $period_J$ in Fig. 4.4. On the other hand, *Cheater* might be able to estimate network actions more accurately and can act ac-

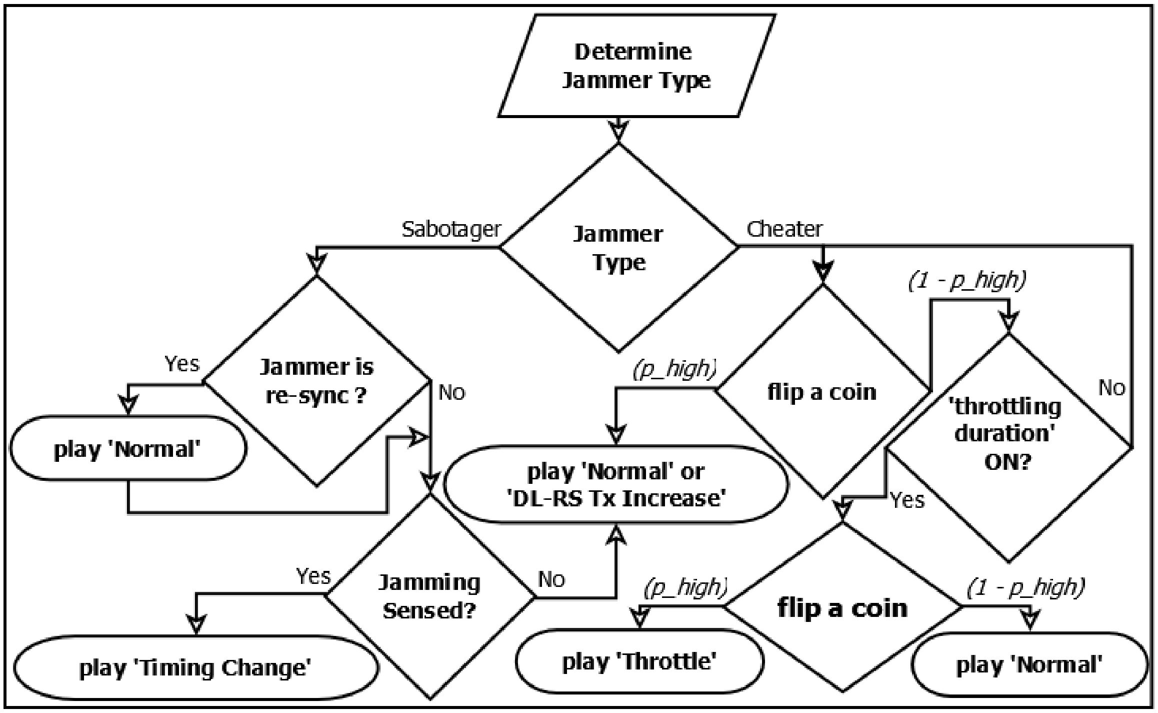

Figure 4.2: eNode B's *Narrowband* Repeated Game Strategy Algorithm

cordingly. It forms its own baseline during the observatory *(inactive)* period so that future network behavior can be interpreted in terms of eNode B actions. In addition, jammer uses a probability distribution over frames to jam the network randomly in order to escape detection by the network.

Repeated Game Simulation Results

The same weighting parameters are used for repeated game as single-shot game with following frequency of different jammer personalities occurrence: $f_c = 9.33\%$, and $f_s = 5.67\%$ for *Cheater* and *Saboteur* respectively. As a result, the following ***repeated game utility*** values are obtained from the simulation: $\mathcal{U}_{\text{eNB}}^{\text{repeated}} = \mathbf{-23.2}$, $\mathcal{U}_{c}^{\text{repeated}} = 466.2$, and $\mathcal{U}_{s}^{\text{repeated}} = -511.3$. The corresponding ***single-shot utility*** at NE would be $\mathcal{U}_{\text{eNB}}^{\text{single}} = (-523)f_c + (-81.3)f_s = -53.4$. Evidently, eNode B enjoys 57% relative improvement in its utility when using *narrowband repeated game strategy algorithm* as compared to playing *best response* in its single-shot scenario.

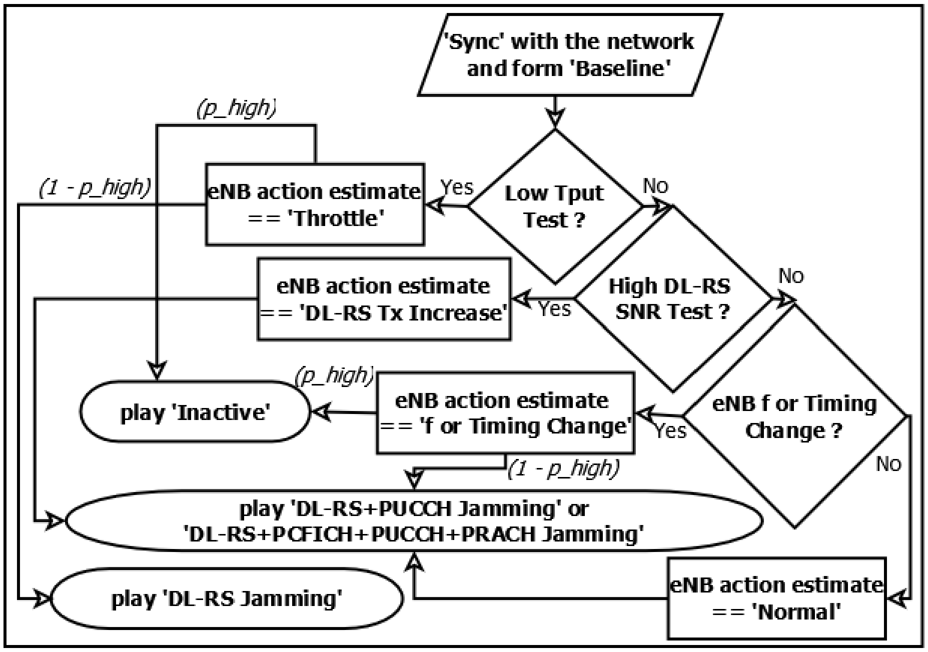
'Sync' with the network and form 'Baseline'
Low Tput Test ?
Yes
No
eNB action estimate == 'Throttle'
(p_high)
(1 - p_high)
High DL-RS SNR Test ?
Yes
No
eNB action estimate == 'DL-RS Tx Increase'
eNB f or Timing Change ?
Yes
No
eNB action estimate == 'f or Timing Change'
(p_high)
(1 - p_high)
play 'Inactive'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

Figure 4.3: Cheater's *Narrowband* Repeated Game Strategy Algorithm

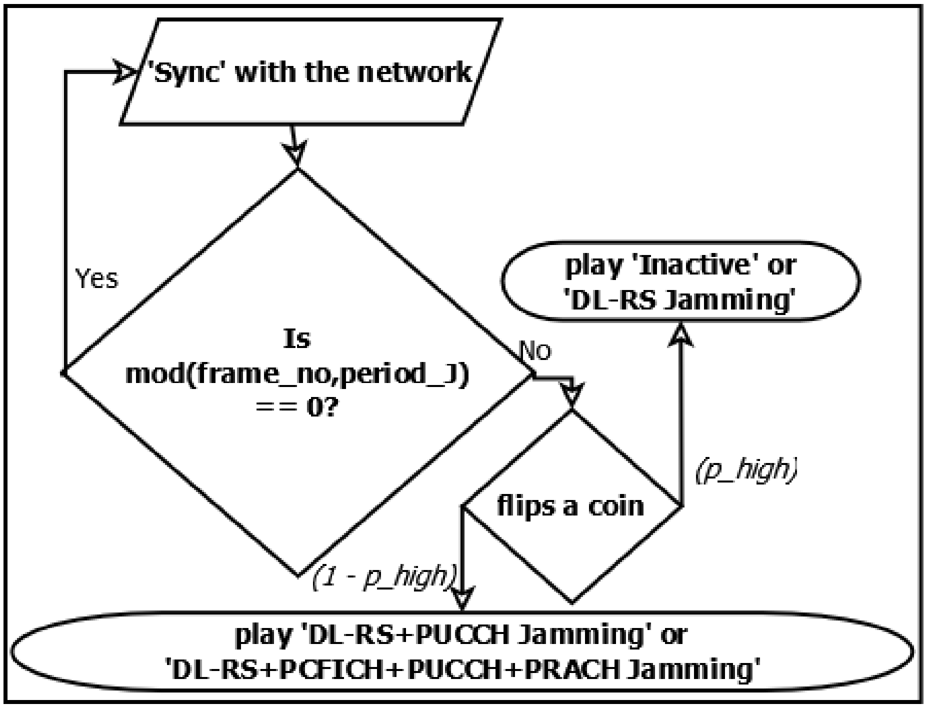
'Sync' with the network
Yes
Is mod(frame_no,period_J) == 0?
No
play 'Inactive' or 'DL-RS Jamming'
(p_high)
flips a coin
(1 - p_high)
play 'DL-RS+PUCCH Jamming' or 'DL-RS+PCFICH+PUCCH+PRACH Jamming'

Figure 4.4: Saboteur's *Narrowband* Repeated Game Strategy Algorithm

Brief Discussion on Simulation Results

Based on the simulation results, it becomes clear that the network can improve its utility significantly by using the presented narrowband algorithms in case of a jamming attack. In a single-shot game, network may not have enough information and leverage against adversary, whereas it can learn jammer type and use threats against it in a repeated game. Similarly, *Cheater* can also improve its utility as a consequence of repeated game formulation. Although the *jammer type estimation algorithm* is not completely characterized, it can be tweaked for various jammer types based on their expected behavior. It is to be noted here that the simulation results are probabilistic in nature and only long-term averages are reported here.

4.1.3 Summary

It is shown 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 *narrowband repeated game type estimation, and repeated game learning and strategy algorithms* are used by the network, it can recover most of its performance loss and may even force an adversary to retract.

4.2 *Evolved* Jammer Type Estimation Algorithm for Wideband Model

In this section, the *evolved* jammer type estimation algorithm is presented for the wideband model and its performance is characterized.

4.2.1 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 as frequently as desired (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 immediate feedback is possible from the UEs who suffer RLF either due to channel variations or possible jamming attack. During 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. The network can be divided into multiple regions and the near-cell UEs' RSSI can be used as a test statistics but it's not robust enough because of unknown jammer location.

Hence, the *"number of Connected mode UEs"* is used 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. Furthermore, non-parametric statistical hypothesis tests are used for jamming sense, 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 can be 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* [105] is used for jamming detection. It does not require the assumption of any specific distribution (e.g., Gaussian) and the only required assumption is that the underlying distribution must be symmetric about its median.

4.2.2 Threat Mechanisms

The following threat mechanisms are constructed for various jammer types.

'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. However, it cannot be extended indefinitely due to lack of credibility in infinite-horizon when it harms the network as well.

'Change f_c + SIB 2' - Interference Avoidance

eNode B "relocates" its center frequency f_c 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 alleviate PRACH and PUCCH failures. This mechanism acts like a credible threat to Saboteur since Saboteur cares deeply about sabotaging the LTE network and cannot observe frequency reconfiguration messages. The aforementioned interference avoidance scheme alleviates jamming of control channels until Saboteur re-synchronizes with the network.

4.2.3 *Evolved* Jammer Type Estimation Algorithm for eNode B

The devised algorithm is shown in Fig. 4.5. 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 presented in next section, 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.

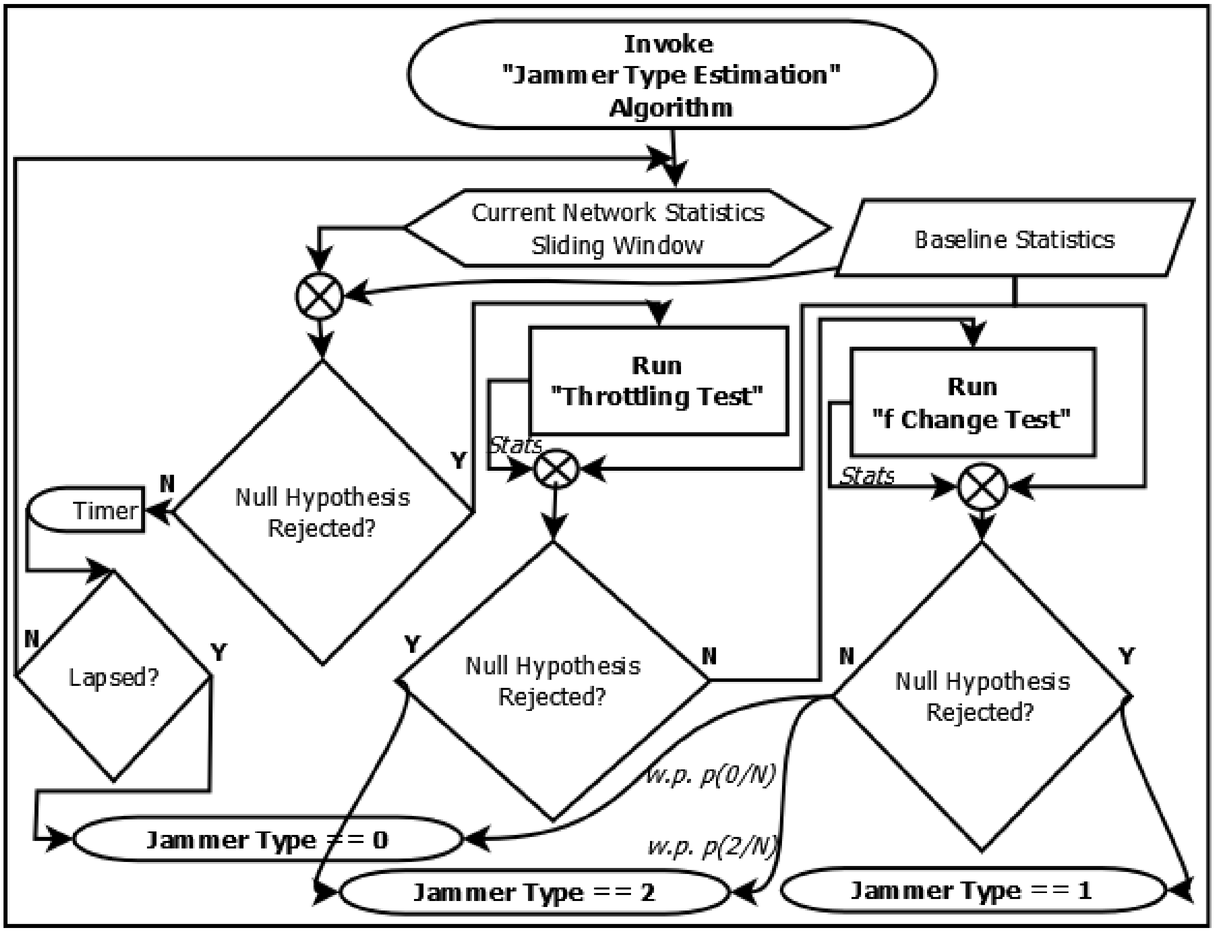

Figure 4.5: eNode B’s *Evolved* Jammer Type Estimation Algorithm

Initial Jamming Sense

The devised 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 the 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.

‘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”*.

‘Change f_c + SIB 2’ 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.

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. The assumption of myopic player is not unprecedented and has been used before, such as [97]. 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 plays best response to them according to single-shot formulation. For example, in case of *‘throttling’* and *‘f Change’*, Cheater plays *‘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 0.75 and *‘Jam CS-RS + PUCCH’* with probability 0.25.

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 0.60 and *’Inactive’* with probability 0.40.

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.

4.2.4 Simulation Results

The devised 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

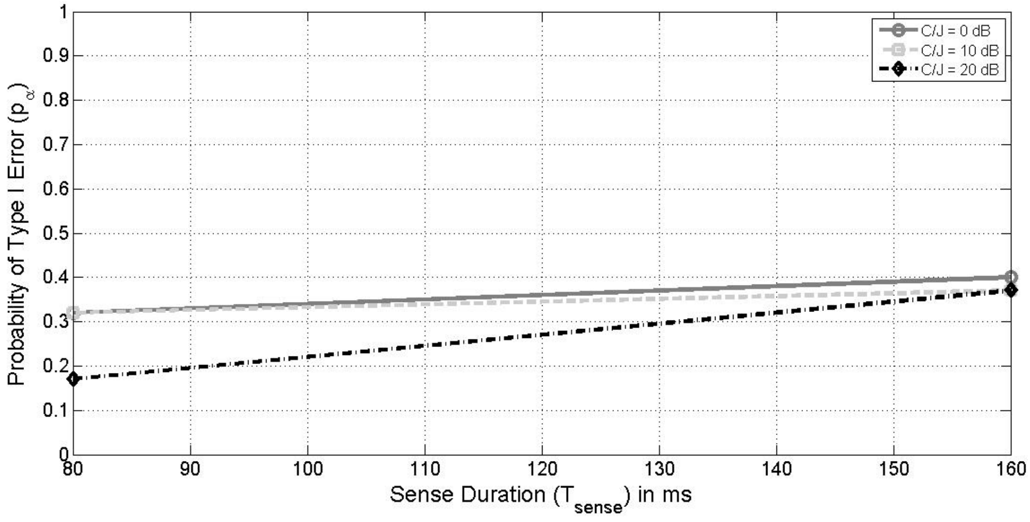

Figure 4.6: False Alarm (type I error) Probability vs. Jamming Sense Duration T_{sense}

$\frac{C}{J}$ and probability of jamming p_j as well. Since, this section is focused on characterizing the devised 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 devised 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. 4.6 and Fig. 4.7, 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 ($\theta = 2$) missed detection error probability is generally lower than that of Cheater ($\theta = 1$) especially at higher 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. 4.8 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

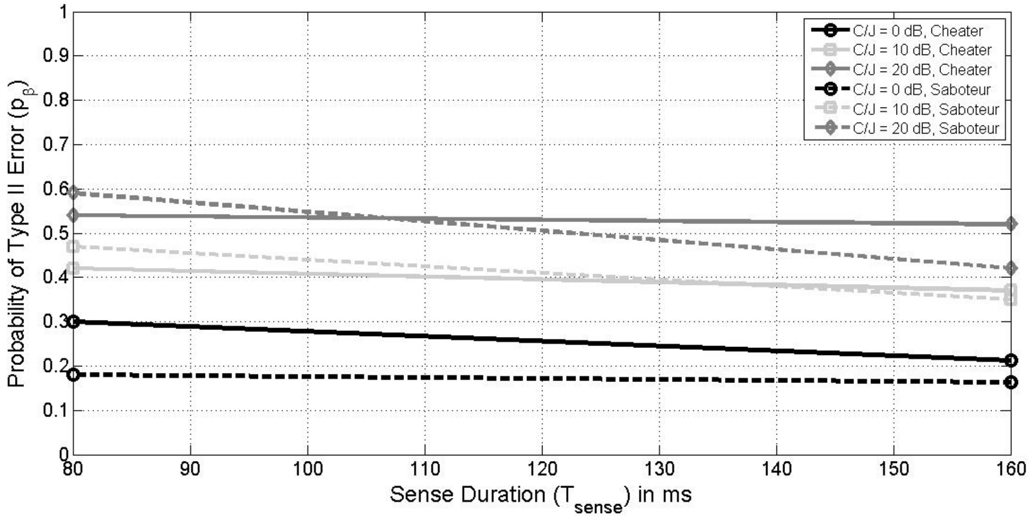

Figure 4.7: Missed Detection (type II error) Prob. vs. Jamming Sense Duration T_{sense}

missed detection probability decreases with increasing p_j. However, higher Type II error probability (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 devised algorithm's true estimation probability $p(\hat{\theta} = k|\theta = k)$, $k = \{0, 1, 2\}$ is plotted against C/J in Fig. 4.9 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) as well as misclassification errors. Normal state's ($\theta = 0$) 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 C/J). Also, Saboteur's ($\theta = 2$) true estimation probability decreases more rapidly than that of the Cheater ($\theta = 1$) due to relatively higher misclassification errors $p(\hat{\theta} = 1|\theta = 2)$ at lower jamming powers (higher 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

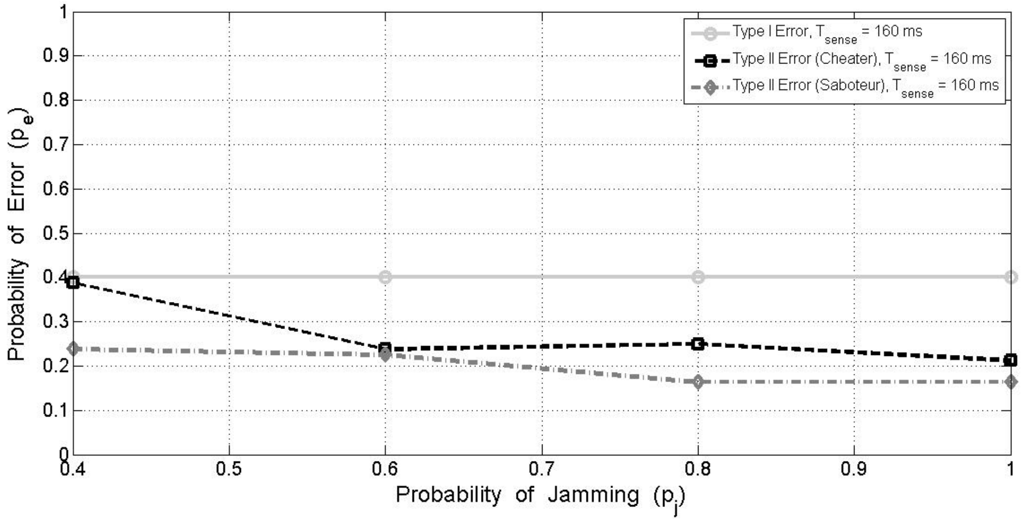

Figure 4.8: Probability of Error (p_e) vs. Probability of Jamming (p_j) for $C/J = 0$ dB

observed to be 0.66 and 0.61 for T_{sense} = 80 ms and 160 ms, respectively.

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.

4.2.5 Performance Analysis

Although the devised 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 C/J. Furthermore, *Normal* state's ($\theta = 0$) true estimation performance does not degrade with decreasing jamming power (increasing C/J), and that of states 1 (Cheater) and 2 (Saboteur) degrade gracefully with increasing C/J.

The algorithm provides several parameters to tweak its performance and trade-off dif-

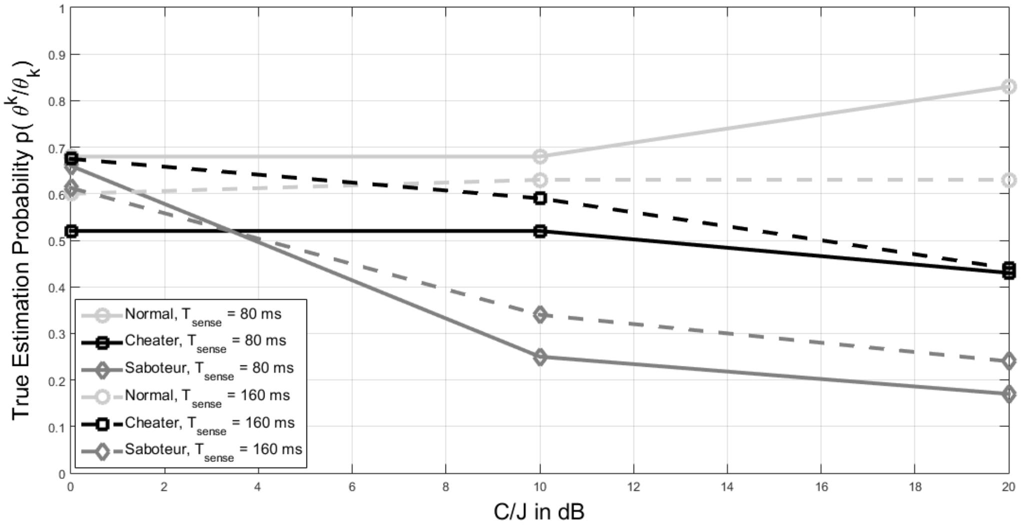

Figure 4.9: True Estimation Probability $p(\hat{\theta} = k/\theta = k)$ vs. C/J for $p_j = 1.0$

ferent 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.

4.2.6 Summary

In this section, a *threat-based jammer type estimation algorithm* is presented 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 algorithm provides several parameters to tweak its estimation performance and trade-off error probabilities (e.g. false alarm and missed detection errors). Furthermore, the 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 presented algorithm provides a practical yet robust way to estimate jammer type without requiring any feedback from the network users nor making any unrealistic assumptions.

4.3 *Evolved* Strategy Algorithms for Wideband Model

4.3.1 Single-Shot Game for Wideband Model

In a *single-shot game*, the eNode B and adversary choose their pure action $a^i \in \mathcal{A}_i$ or mixed $\Delta(\mathcal{A}_i)$ strategies once and for all at the beginning of the game $\mathcal{G}$. The simulations results are presented in the form of *normal-form utility matrices* with the network and the adversary being the *row* and *column* player respectively. Following weights are chosen for utility computation based on relative significance of their corresponding *KPIs*:

- $\alpha^{\text{UE}} = 100,$
- $\alpha^{\text{Tput}} = 50,$
- $\alpha^{\text{RS}} = 3,$
- $\alpha^{\text{PCFICH}} = 2,$
- $\alpha^{\text{PUCCH}} = 2,$
- $\alpha^{\text{RACH}} = -25,$
- $\alpha^{\tau} = -10,$
- $\mathcal{C}_{\text{eNB}}^{\text{f Change}} = 5,$

- $\mathcal{C}_{\text{eNB}}^{\text{t Change}} = 10$
- $\text{BLER}_{\text{threshold}} = 10\%$,
- LTE carrier frequency $f_c = 2140$ MHz,
- path loss exponent $\gamma = 3.5$,
- UE arrival rate $\lambda = 8\ \text{UEs/km}^2$,
- $C/J = 20$ dB and
- $p_j = 0.7$,

where C/J, and p_j denote *carrier-to-jammer power ratio* and *probability of jamming* respectively. The $\mathcal{U}_{0,c}^{\text{evolved}}$ *(eNB vs. Cheater)* utility matrix is:

$$\mathcal{U}_{0,c}^{\text{evolved}} = \begin{bmatrix} 0,0 & 7,-70 & -9,5 & -5,59 & -9,-20 \\ -1,47 & -1,5 & -11,58 & \textbf{-3.5,87.5} & -10,-21 \\ -764,-535 & -761,-544 & -781,-546 & -765,-545 & -781,-553 \\ -32,-89 & -37,-55 & -39,31 & -35,-6 & -49,-21 \\ -10,0 & -3,-70 & -19,5 & -15,59 & -19,-20 \end{bmatrix}$$

Similarly, $\mathcal{U}_{0,s}^{\text{evolved}}$ *(eNB vs. Saboteur)* utility matrix is:

$$\mathcal{U}_{0,s}^{\text{evolved}} = \begin{bmatrix} 0,0 & 10,-17 & -12,10 & -7,-5 & -9,3 \\ -1,7 & 7,-4 & -18,24 & -6,5 & -5,4 \\ -764,765 & -758,752 & -778,775 & -765,755 & -777,768 \\ -32,22 & -35,21 & -28,7 & -32,16 & -31,9 \\ -10,0 & -14,-1 & -5,-14 & -6,-10 & -5,-16 \end{bmatrix}$$

As per celebrated *Nash existence theorem*, every finite strategic game has a mixed strategy *Nash Equilibrium (NE)* that captures a steady state of the game [62]. In case of **Cheater**, game has a single **pure strategy NE** (marked above) with an expected payoff of **(-3.5, 87.5)**. Whereas, in case of **Saboteur**, game has a **mixed strategy NE** with expected payoff of **(-7, 0)** with corresponding probability distribution of $[0.585, 0, 0, 0, 0.415]^T$ and $[0.408, 0, 0.592, 0, 0]$ assigned to the network and Saboteur actions respectively. Evidently, **similar to the narrowband model, the network's utility is severely compromised in case of a jamming attack**. Also, some eNode B actions are strictly dominated against a particular type of adversary, e.g., *'Change f_c'* and *'Timing Change'* against *Cheater*. Hence, the **network strategy depends on adversary action as well as its type as observed in the narrowband model**. Similar trends are observed at other values of C/J and p_j.

4.3.2 Infinite-horizon Repeated Bayesian Game with Asymmetric Information

Repeated games model long-term interaction among players and aim to explain "real life" phenomena like cooperation, threats, revenge and signals (cf. [61, 62]). The strength of our algorithms comes from practicality of suggested actions; and learning and utilizing game dynamics in the *repeated game*.

Initial Stage

During the *initial stage*, both players play their *default* actions and observe signals correlated to jamming-free scenario in order to collect *"baseline statistics"*. eNode B and *Cheater* compute thresholds γ_{signal} based on these *"baseline statistics"* to be used in later stages.

eNode B's Jamming Sense Algorithm

eNode B uses *sliding-window based moving-average filter* for signals observed during the game. It uses these *filter's* outputs for determining if it is under attack or not. The algorithm can be described as follows:

```
    if $(\mu_{\mathrm{RS}}^{\mathrm{eNB}} \leq \gamma_{\mathrm{RS}}^{\mathrm{eNB}}) \parallel (\mu_{\mathrm{PUCCH}}^{\mathrm{eNB}} \leq \gamma_{\mathrm{PUCCH}}^{\mathrm{eNB}})$
set $flag_{\mathrm{sense}} = 1$ w.p. $(1 - p_{\mathrm{false}})$
otherwise $flag_{\mathrm{sense}} = 0$
end
abort if not sensed within $(n_1 \times l_{\mathrm{win}}), n_1 \in \mathbb{Z}^+$
```

where μ_{k}, γ_{k} and l_{win} represent observations' average, threshold for the kth signal and window length.

eNode B's Adversary Type Estimation Algorithm for Wideband Model

eNode B's *best response (BR)* depends on both the adversary type and its actions. If eNode B senses a jamming attack twice within $n_2 \times l_{win}, n_2 \in \mathbb{Z}^+$, it invokes its *Adversary Type Estimation Algorithm* presented in the previous section ([12]). It uses a combination of threat mechanism and interference-avoidance tests to make the determination.

eNode B's Evolved Repeated Game Strategy Algorithm for Wideband Model

After determining adversary type, eNode B uses the algorithm shown in Fig. 4.10 to strategize for infinite-horizon repeated game. This algorithm is different from the one presented for narrowband model [8] since network's *best response* has changed and *threat* is not used due to lack of credibility for infinite-horizon.

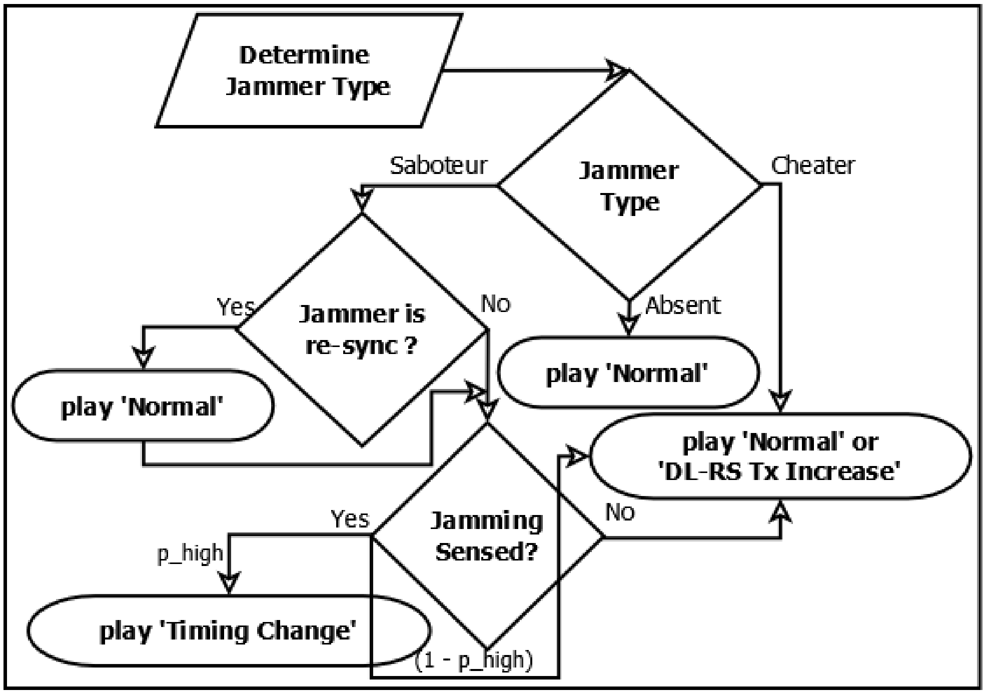

Figure 4.10: eNode B's *Evolved* Repeated Game Strategy Algorithm

Jammer's Repeated Game Strategy Algorithms

Cheater and *Saboteur* also devise their repeated game strategies shown in Figs. 4.11 and 4.12 respectively. These algorithms are also based on playing *best response* and *semi-best response* and are different from narrowband algorithms [8]. *Cheater* observes signals correlated to eNode B's actions and tries to estimate them assuming a quasi-stationary distribution of opponent's actions. *Saboteur* lacks the resources for observations and employs an *open-loop* strategy.

Repeated Game's Steady-State Simulation Results

The presented *evolved Repeated Game Strategy Algorithms* show significant improvement in eNode B utility provided that *adversary type* is correctly estimated. When **Cheater** is present in the network, the algorithm results in $\mathcal{U}_{\mathbf{eNB}}^{\mathbf{repeated}} = \mathbf{-2.34}$ and $\mathcal{U}_{\mathbf{c}}^{\mathbf{repeated}} = \mathbf{-1.25}$ as compared to $\mathcal{U}_{\mathbf{eNB}}^{\mathbf{single}} = \mathbf{-3.5}$ and $\mathcal{U}_{\mathbf{c}}^{\mathbf{single}} = \mathbf{87.5}$ in its single-shot version. This translates to 33% relative improvement in eNode B's utility and 101% relative decline in Cheater's

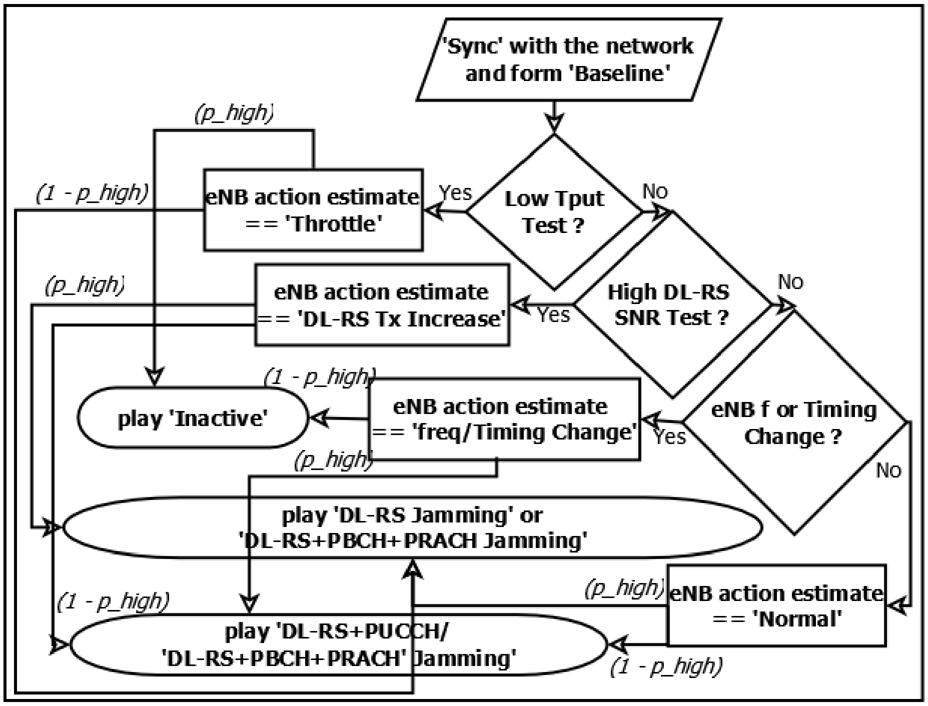
'Sync' with the network and form 'Baseline'
Low Tput Test ?
Yes
No
eNB action estimate == 'Throttle'
(p_high)
(1 - p_high)
High DL-RS SNR Test ?
Yes
No
eNB action estimate == 'DL-RS Tx Increase'
(p_high)
eNB f or Timing Change ?
Yes
No
eNB action estimate == 'freq/Timing Change'
(1 - p_high)
(p_high)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

Figure 4.11: Cheater's *Evolved* Repeated Game Strategy Algorithm

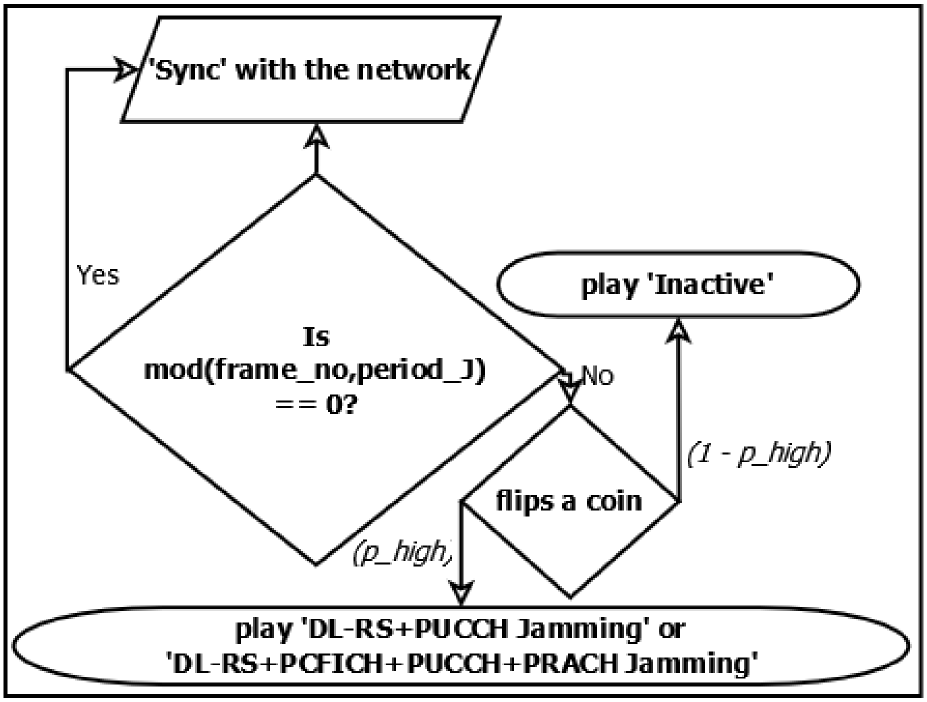
'Sync' with the network
Yes
Is mod(frame_no,period_J) == 0?
No
play 'Inactive'
flips a coin
(1 - p_high)
(p_high)
play 'DL-RS+PUCCH Jamming' or 'DL-RS+PCFICH+PUCCH+PRACH Jamming'

Figure 4.12: Saboteur's *Evolved* Repeated Game Strategy Algorithm

utility as compared to single-shot version.

Similarly, when **Saboteur** is present in the network, the evolved algorithms result in $\mathcal{U}_{\mathbf{eNB}}^{\mathbf{repeated}} = -\mathbf{2.74}$ and $\mathcal{U}_{\mathbf{s}}^{\mathbf{repeated}} = -\mathbf{2.40}$ as compared to $\mathcal{U}_{\mathbf{eNB}}^{\mathbf{single}} = -\mathbf{7}$ and $\mathcal{U}_{\mathbf{s}}^{\mathbf{single}} = \mathbf{0}$ in its single-shot counterpart. This translates to 61% relative improvement in eNode B's utility and theoretically ∞ relative decline in Saboteur's utility. Hence, in both the cases not only does eNode B enjoy a substantial improvement in its utility but also the jammer suffers remarkable loss in his utility, forcing him to retract.

4.3.3 Summary

This section studies the LTE/LTE-A networks' performance under wideband multipath fading conditions and it is shown that LTE networks are indeed vulnerable to *denial-of-service (DOS)* and *loss of service* attacks from *smart jammers* even if the jammers are power and bandwidth-limited. The jammer can launch network-wide *smart jamming* attacks resulting in significant performance loss for the network. It is further shown that the presented *evolved Repeated Game Learning and Strategy Algorithms* can help the network recover substantial part of network performance loss and may even force an adversary to retract.

4.4 Practical Implementation Challenges

Although implementing the devised algorithm on an experimental test bed is out of scope for this research, 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 this 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, I am confident that the algorithm would perform well if implemented on a realistic eNode B.

CHAPTER 5
ZERO-SUM GAME FORMULATION & STRATEGY ALGORITHMS

5.1 Rationale

The main purpose of this research is to employ game-theoretic and communication theory tools to construct realistic techniques to help LTE/LTE-A networks combat *smart jamming* attacks. Although previous work in Chapter 4 is focused on infinite-horizon general-sum (non-zero sum) repeated games without "full monitoring" [1] to reflect realistic operating environment; there does not exist any suitable game-theoretic formulations, to the best of my knowledge, that can be used for computation of the uninformed player's strategies in infinite-horizon repeated games with asymmetric information. Hence, all of the algorithms presented in Chapter 4 are based on heuristics, learning and threat mechanisms in repeated games and knowledge of LTE network and *smart jammer* dynamics. This problem gets further complicated for general-sum (non-zero-sum) games with imperfect monitoring, which is still an open problem [76]. This is the motivation for transforming previous model of LTE vs. *smart jammer* interaction into a zero-sum setting. Zero-sum formulations have been studied extensively in the game-theoretic literature concerning asymmetric information repeated games, such as, Chapter 5 of [61], Chapter 4 of [63], Chapters 2 - 4 of [64], and Chapter 2 of [65]. But, almost all of the formulations deal with the informed player with "full monitoring". In this chapter, it is attempted to solve LTE vs. smart jammer interaction as a strictly competitive **infinite-horizon zero-sum repeated Bayesian game with asymmetric information,** [106] by using LP formulation for both players' strategy computation developed by Li and Shamma in their recent work [89]. The informed player's security strategy (optimal strategy in the worst-case scenario) only depends on the his-

[1] It requires that all players are capable of observing previous actions of their opponents with certainty after each stage [61].

tory of his own actions and is independent of the other player's actions. The informed player models the uninformed player as a Bayesian player, making Bayesian updates with an evolving belief state. However, in order to solve the infinite-horizon game efficiently, fixed-sized sufficient statistics are needed for both players that do not not grow with the horizon. The evolving belief state serves as a sufficient statistics for the informed player in a λ-discounted asymmetric repeated game. On the other hand, the uninformed player's security strategy does not depend on the history of his own actions, but rather depends on the history of the informed player's actions. However, the uninformed player does not have access to the informed player's belief state and needs to find different fixed-sized sufficient statistics. Fortunately, the uninformed player's security strategy in the dual game depends only on a fixed-sized sufficient statistics that is fully available to him. Furthermore, the uninformed player's security strategy in the dual game, with initial worst-case vector regret, also serves as his security strategy in the primal game. Therefore, initial worst-case regret of security strategy and its anti-discounted update (which is the same size as the cardinality of system state) is used as the fixed-sized sufficient statistics for the uninformed player. Although the above-mentioned sufficient statistics are fixed-sized for both players in an infinite-horizon game, optimal security strategy computation in λ-discounted asymmetric game are still hard to compute because of non-convexity [107]. Consequently, approximated security strategies with guaranteed performance are computed for both players, but they require "full monitoring". Hence, the uninformed player's simplistic "expected" strategy formulation is also explored in this chapter that does not require any "full monitoring".

5.2 Zero-Sum Game Formulation

The eNode B vs. *smart jammer* game described in the Chapter 3 is converted to zero-sum (strictly competitive) setting so that repeated game strategy algorithms presented in [89] can be employed. Following the convention used in game-theoretic literature including [89], the informed player, i.e., the **smart jammer** is played as the **maximizer (row player)**, whereas the uninformed player, i.e., the **eNode B** is played as the **minimizer (column player)**. Furthermore, player's utility functions are modified to reflect zero-sum setting, i.e., one player's gain is exactly the other player's loss as described by (5.1).

$$\mathcal{U}_0 = -\mathcal{U}_j \tag{5.1}$$

When the system state is *Cheater*, the zero-sum utility function is simplified to (5.2) below.

$$\mathcal{U}_j^c = -\alpha^{\mathcal{N}_c}\mathbb{E}_w[\mathcal{N}_c^{\text{norm}}] + \alpha^{\mathcal{R}_c}\mathbb{E}_w[\delta(\mathcal{R}_c^{\text{norm}})] \tag{5.2}$$

where $\mathcal{N}_c^{\text{norm}}$ represents normalized average number of Connected mode UEs in the network when *Cheater* is present, $\alpha^{\mathcal{N}_c}$ represents its corresponding weight, $\delta(\mathcal{R}_c^{\text{norm}})$ represents change in *Cheater*'s normalized average throughput from baseline scenario, $\alpha^{\mathcal{R}_c}$ represents its corresponding weight and $\mathbb{E}_w$ represents expectation with respect to randomness caused by w as mentioned in (3.10).

The *Cheater* tries to maximize (5.2) in order to reduce the number of Connected mode UEs in the network while increasing its throughput from the baseline scenario. The eNode B, on the other hand, tries to minimize (5.2) to do the opposite, hence, creating a zero-sum game. Similarly, the zero-sum utility function for the system state *Saboteur* is simplified to (5.3).

$$\mathcal{U}_j^s = -\alpha^{\mathcal{N}_s}\mathbb{E}_w[\mathcal{N}_s^{\text{norm}}] - \alpha^{\mathcal{R}_{\text{eNB}}}\mathbb{E}_w[\mathcal{R}_{\text{eNB}}^{\text{norm}}] \tag{5.3}$$

where $\mathcal{N}_s^{\text{norm}}$ represents normalized average number of Connected mode UEs in the network when *Saboteur* is is present, $\alpha^{\mathcal{N}_s}$ represents its corresponding weight, $\mathcal{R}_{\text{eNB}}^{\text{norm}}$ represents eNode B's normalized average throughput/UE, $\alpha^{\mathcal{R}_{\text{eNB}}}$ represents its corresponding weight and $\mathbb{E}_w$ again represents expectation with respect to randomness caused by w as mentioned above.

The *Saboteur* tries to maximize the opposite (negative of) eNode B utility defined in terms of average number of Connected mode users and average throughput/UE, hence, defining the zero-sum game.

It is to be noted here that there are no “unilateral” fixed costs associated with either player in order to convert the game to zero-sum. This means that the game would be played as zero-sum at the expense of some fidelity loss associated with players’ modeling, such as, their duty cycles and implicit cost associated with eNode B actions *’f Change’* and *’Timing Change’*. Furthermore, the LTE network model was simplified to include Rayleigh fading at each subcarrier similar to the **narrowband model** defined in Chapter 3 in order to simplify network dynamics and reduce convergence time, while preserving realistic network dynamics.

5.3 Single-Shot Game

A two-player zero-sum game is defined by vector spaces Σ and $\mathcal{T}$ of row player and column player strategies respectively, and a utility function $\mathcal{U}^{\theta} : \Sigma \times \mathcal{T} \to \mathbb{R}$ for given state of nature $\theta \in \Theta$. The row player (the **maximizer**) chooses his strategy $\sigma \in \Sigma$, the column player (the **minimizer**) chooses his strategy $\tau \in \mathcal{T}$, and the corresponding utility function is $\mathcal{U}^{\theta}(\sigma, \tau)$. For a given prior p_0, the payoff function in a **game with lack of information on one side** can be written as $\mathcal{U}(p_0, \sigma, \tau) = \sum_{\theta \in \Theta} p_0^{\theta} \, \mathcal{U}^{\theta}(\sigma(\theta), \tau)$. The **maxmin** value $\underline{v}$ for the row player (the **informed player**) for given state θ is defined as [64]:

$$\underline{v}(p_0) = \sup_{\sigma \in \Sigma(\theta)} \inf_{\tau \in \mathcal{T}} \mathcal{U}(p_0, \sigma, \tau) \tag{5.4}$$

Similarly, the **minmax** value $\overline{v}$ for the column player (the **uninformed player**) is defined as:

$$\overline{v}(p_0) = \inf_{\tau \in \mathcal{T}} \sup_{\sigma \in \Sigma(\theta)} \mathcal{U}(p_0, \sigma, \tau) \tag{5.5}$$

It is widely known that $\underline{v} \leq \overline{v}$ is always true. However, when $\underline{v} = \overline{v}$ is satisfied, then the game is said to have a **value** v. The legendary *von Neumann's* celebrated **Minmax Theorem** states that any matrix game has a value v in mixed strategies and the players have optimal strategies [64], i.e., the *minmax solution* of a zero-sum game is the same as the *Nash equilibrium*.

$$v = \max_{x \in \Delta(\mathcal{A}_j)} \min_{y \in \Delta(\mathcal{A}_0)} xAy = \min_{y \in \Delta(\mathcal{A}_0)} \max_{x \in \Delta(\mathcal{A}_j)} xAy \tag{5.6}$$

where x is row player's mixed strategy, y is column player's mixed strategy, A is $\mathcal{A}_j \times \mathcal{A}_0$ utility matrix, and $\Delta(\mathcal{A})$ represents the simplex on $\mathcal{A}$. Thus, both players play their **security strategies** in a zero-sum game to guarantee the best outcome under the worst conditions, due to the game's strictly competitive nature.

The complete-information single-shot game results for a given jammer type θ are presented in this section as a reference when eNode B knows what game is being played. Following parameter values are used for both single-shot and repeated game simulations in addition to the ones used in Chapter 4: $\frac{C}{J} = 0\text{dB}, p_j = 1.0, \alpha^{\mathcal{N}_c} = 4, \alpha^{\mathcal{R}_c} = 5, \alpha^{\mathcal{N}_s} = 5, \alpha^{\mathcal{R}_{\text{eNB}}} = 4$. The single-shot game's simulation results for zero-sum game of **Cheater vs. eNode B** are presented below.

$$\mathcal{U}_j^c = \begin{bmatrix} -1.0000 & -1.0239 & -2.2464 & -1.3840 & -1.0000 \\ -0.9642 & -1.0029 & -2.2130 & -1.3398 & -0.9642 \\ -0.8016 & -0.8239 & \mathbf{-2.0553} & -1.1366 & -0.8016 \\ -0.9714 & -1.0078 & -2.2212 & -1.3525 & -0.9714 \\ -0.8181 & -0.8399 & -2.0716 & -1.1610 & -0.8181 \end{bmatrix}$$

The game has a single **pure strategy Nash Equilibrium**, (a^{j*}, a^{0*}) = *('Jam CS-RS + PUCCH', 'Throttling')*, with the game value $v = -2.0553$, satisfying the following equation.

$$\mathcal{U}_j^c(a^{j*}, a^{0*}) = \min_{a^0 \in \mathcal{A}_0} \mathcal{U}_j^c(a^{j*}, a^0) = \max_{a^j \in \mathcal{A}_j} \mathcal{U}_j^c(a^j, a^{0*}) \tag{5.7}$$

Similarly, the complete-information single-shot game's simulation results for zero-sum game of **Saboteur vs. eNode B** are presented below.

$$\mathcal{U}_j^s = \begin{bmatrix} -1.0000 & -0.9933 & -0.5635 & -0.9128 & -1.0000 \\ -0.9879 & -0.9805 & -0.5446 & -0.9022 & -0.9898 \\ -0.9905 & -0.9805 & -0.4578 & -0.8849 & -0.9867 \\ -0.9900 & -0.9827 & -0.5498 & -0.9050 & -0.9919 \\ -0.9895 & -0.9800 & -0.4666 & -0.8880 & -0.9875 \end{bmatrix}$$

For complete information case when the network is aware of the jammer type, the game does not have any pure strategy Nash Equilibrium. If the players are allowed to use mixed strategies, i.e. a probability distribution over a player's action set, then there exists a **mixed strategy Nash Equilibrium** (x^*, y^*), where $x^* = [0\; 0.51\; 0\; 0\; 0.49]^T \in \Delta(\mathcal{A}_j)$, and $y^* = [0.59\; 0\; 0\; 0\; 0.41] \in \Delta(\mathcal{A}_0)$ with the game value $v = -0.9887$, satisfying the following equation. This mixed strategy probability distribution loosely translates to playing *('Jam CS-RS', 'Jam CS-RS + PCFICH + PUCCH + PRACH')* and *('Normal', 'Timing Change')* equally likely by the jammer and the eNode B, respectively.

$$E_{x^*,y^*}(\mathcal{U}_j^s(a^j, a^0)) = \min_{y \in \Delta(\mathcal{A}_0)} E_{x^*,y}(\mathcal{U}_j^s(a^j, a^0)) = \max_{x \in \Delta(\mathcal{A}_j)} E_{x,y^*}(\mathcal{U}_j^s(a^j, a^0)) \tag{5.8}$$

where $E_{x,y}(\mathcal{U}_j^s(a^j, a^0)) = x^T \mathcal{U}_j^s y$ is the expected value of the single-stage utility given mixed strategies x and y. Given the utility matrix, linear program is used to compute the Nash Equilibirum [62] with x^* and y^*, and the game value v.

However, in asymmetric information case, eNode B only knows the probability distribution p_0 over jammer's types which is public information, while the jammer knows exactly his own type. Knowing its own type, the jammer can use different strategy for different states θ. Therefore, in the asymmetric game, jammer's mixed strategy x is a mapping from Θ to $\Delta(\mathcal{A}_j)$. The single-shot asymmetric game still has a mixed strategy Nash Equilibrium (x^*, y^*), where $x^* \in \Delta(\mathcal{A}_j)^{|\Theta|}$ and $y^* \in \Delta(\mathcal{A}_0)$ satisfying the following equation.

$$E_{p_0,x^*,y^*}(\mathcal{U}_j^\theta(a^j, a^0)) = \min_{y \in \Delta(\mathcal{A}_0)} E_{p_0,x^*,y}(\mathcal{U}_j^\theta(a^j, a^0)) = \max_{x \in \Delta(\mathcal{A}_j)^{|\Theta|}} E_{p_0,x,y^*}(\mathcal{U}_j^\theta(a^j, a^0))$$

where $E_{p_0,x,y}\left[\mathcal{U}_j^\theta(a^j, a^0)\right] = \sum_{\theta \in \Theta} p_0^\theta {x^\theta}^T \mathcal{U}_j^\theta y$ is the expected value of single-stage utility given initial probability p_0 and mixed strategies x and y. The Nash Equilibrium for the asymmetric information game can be computed by solving an LP by setting the time horizon to single stage [108].

5.4 Infinite-Horizon Asymmetric Repeated Game Strategy Algorithms

The repetition of a zero-sum game in its basic form does not warrant further study as the players can play their optimal security strategies i.i.d. at each stage to guarantee optimal game value [64]. However, in our case, the system has multiple states and the game is played with the lack of information on one side. Therefore, the repeated game needs to be studied further. Li et al. showed that the security strategies for both the players in finite-horizon asymmetric information repeated zero-sum games depend only one the informed player's history actions [74]. For the infinite-horizon games, this would imply utilizing large amount of memories to record the history actions. It is, therefore, necessary for the players to find fixed-size sufficient statistics for decision making in λ-discounted infinite-horizon games, but it is still nontrivial to compute optimal security strategies even with fixed-size sufficient statistics due to non-convexity. Therefore, Li & Shamma provided approximated security strategies with guaranteed performance to solve infinite-horizon games

[89].

The λ-discounted game $\Gamma_\lambda(p_0)$ is defined as a two-player zero-sum asymmetric information repeated game with prior probability distribution p_0, informed player's space of behavioral strategies Σ, uninformed player's space of behavioral strategies $\mathcal{T}$, and payoff function $\mathcal{U}_\lambda(p_0, \sigma, \tau)$, where $\sigma \in \Sigma$ and $\tau \in \mathcal{T}$. The λ-discounted payoff function for the discounted game $\Gamma_\lambda(p_0)$ for some $\lambda \in (0, 1)$ is defined in (5.9).

$$\mathcal{U}_\lambda(p_0, \sigma, \tau) = \mathbb{E}_{p_0,\sigma,\tau}\left[\sum_{t=1}^{\infty} \lambda(1-\lambda)^{t-1}\mathcal{U}(\theta, a_t^j, a_t^0)\right] \tag{5.9}$$

where $\mathcal{U}(\theta, a_t^j, a_t^0)$ represents the payoff given state θ, jammer's action $a_t^j \in \mathcal{A}_j$, and eNode B action $a_t^0 \in \mathcal{A}_0$ at time t.

Similarly, the average payoff function $\overline{\mathcal{U}}_T(p_0, \sigma, \tau)$ for the T-stage finite-horizon repeated game $\Gamma_T(p_0)$ with prior probability p_0, and behavioral strategy spaces Σ and $\mathcal{T}$ is defined as follows:

$$\overline{\mathcal{U}}_T(p_0, \sigma, \tau) = \mathbb{E}_{p_0,\sigma,\tau}\left[\frac{1}{T}\sum_{t=1}^{T}\mathcal{U}(\theta, a_t^j, a_t^0)\right] \tag{5.10}$$

which leads to the average payoff formulation $\overline{\mathcal{U}}_\infty(p_0, \sigma, \tau)$ in (5.11) for the infinite-horizon non-discounted game $\Gamma_\infty(p_0)$. Since, in our case, the stage payoff $\mathcal{U}(\theta, a_t^j, a_t^0), \forall t \in \{0, 1, 2, ...\}$ is bounded for all possible combinations of states and pairs of actions, and $\Theta, \mathcal{A}_0$ and $\mathcal{A}_j$ are finite sets, the limit exists in (5.11), and hence, can be used as a legitimate utility function.

$$\overline{\mathcal{U}}_\infty(p_0, \sigma, \tau) = \lim_{T\to\infty} \overline{\mathcal{U}}_T(p_0, \sigma, \tau) \tag{5.11}$$

5.4.1 The Informed Player's Approximated Security Strategy Algorithm

It is shown in [89] that the game value $V_\lambda(p)$ in $\Gamma_\lambda(p)$ satisfies the following recursive equation.

$$V_\lambda(p) = \max_{x\in\Delta(\mathcal{A}_j)^{|\Theta|}} \min_{y\in\Delta(\mathcal{A}_0)} \left[\lambda \sum_{\theta\in\Theta} p^\theta {x^\theta}^T \mathcal{U}^\theta y + (1-\lambda)\mathbf{T}_{p,x}(V_\lambda)\right] \tag{5.12}$$

where x^θ represents jammer's behavioral strategy given state θ, y represents eNode B's behavioral strategy, and $\mathbf{T}_{p,x}(V_\lambda) = \sum_{a^j\in\mathcal{A}_j} \bar{x}_{p,x}(a^j)V_\lambda(\pi(p,x,a^j))$ with π representing the belief update equation shown in (5.13).

It is shown that the informed player has a security strategy in $\Gamma_\lambda(p)$ that is independent of the uninformed player's history action sequence $H^{\mathcal{A}_0}$ and depends only on the belief state p_t at stage t. Thus, the informed player only needs to record his sufficient statistics (belief state) $p_t \in \Delta(\Theta)$, i.e., the posterior probability over the system state $\theta\in\Theta$ at stage t to play the game. The belief state p_{t+1} at stage $t+1$ can be computed recursively as a function of p_t, the informed player's $H^{\mathcal{A}_0}$-independent strategy x_t^θ, and the informed player's realized action a_t^j based on the Bayesian law as shown in (5.13).

$$p_{t+1}^\theta(h_{t+1}^j) = \pi(p_t, x_t, a_t^j) = \frac{p_t^\theta(h_t^j)x_t^\theta(a_t^j)}{\bar{x}_{p_t,x_t}(a_t^j)} \tag{5.13}$$

with $p_1 = p$ in the game $\Gamma_\lambda(p)$ and $\bar{x}_{p_t,x_t}(a_t^j) = \sum_{\theta\in\Theta} p_t^\theta(h_t^j)x_t^\theta(a_t^j)$ represents weighted average of x_t.

Furthermore, (5.12) shows that a Bellman-like equation can be used to compute informed player's security strategy. However, the game value $V_\lambda(p)$ and hence the informed player's corresponding optimal security strategy σ^* computation is non-convex [107]. Hence, the game value $V_\lambda(p)$ is approximated to $V_{\lambda,T}(p)$, i.e. the corresponding game value for a λ-discounted T-stage asymmetric repeated game, which is played only for T stages. The game value $V_{\lambda,T+1}(p)$ satisfies the following recursive equation (5.14).

$$V_{\lambda,T+1}(p) = \max_{x\in\Delta(\mathcal{A}_j)^{|\Theta|}} \min_{y\in\Delta(\mathcal{A}_0)} \left[\lambda\sum_{\theta\in\Theta} p^\theta {x^\theta}^T \mathcal{U}^\theta y + (1-\lambda)\mathbf{T}_{p,x}(V_{\lambda,T})\right] \tag{5.14}$$

with $V_{\lambda,0}(p) \equiv 0$.

It is also shown that given $\lambda \in (0,1)$, the approximated game value $V_{\lambda,T+1}$ converges to optimal game value V_λ exponentially fast with rate $1-\lambda$. The informed player's stationary security strategy $\bar{\sigma}_{\lambda,T} : \Theta \times \Delta(\Theta) \to \Delta(\mathcal{A}_j)$, computed based on the approximated game value $V_{\lambda,T}$ in the game $\Gamma_\lambda(p)$, satisfies the following recursive equation (5.15).

$$\bar{\sigma}_{\lambda,T}(:,p) = \operatorname*{arg\,max}_{x\in\Delta(\mathcal{A}_j)^{|\Theta|}} \min_{y\in\Delta(\mathcal{A}_0)} \left[\lambda\sum_{\theta\in\Theta} p^\theta {x^\theta}^T \mathcal{U}^\theta y + (1-\lambda)\mathbf{T}_{p,x}(V_{\lambda,T})\right] \tag{5.15}$$

where $\bar{\sigma}_{\lambda,T}(:,p)$ is an $|\mathcal{A}_j| \times |\Theta|$ matrix whose θ th column is $\bar{\sigma}_{\lambda,T}(\theta,p)$.

Moreover, Li & Shamma constructed a linear program to compute the approximated game value $V_{\lambda,T+1}(p)$ and corresponding approximated security strategy $\bar{\sigma}_{\lambda,T}(\theta,p)$, which depends only on the belief state p_t and the system state $\theta \in \Theta$. It is shown that $V_{\lambda,T+1}(p)$ satisfies the following linear program in (5.16) - (5.20) in the λ-discounted zero-sum asymmetric game $\Gamma_\lambda(p)$:

$$V_{\lambda,T+1}(p) = \max_{q,l\in Q,L} \left[\sum_{t=1}^{T+1} \sum_{h_t^j\in\mathcal{H}_t^j} \lambda(1-\lambda)^{t-1} l_{h_t^j}\right] \tag{5.16}$$

$$s.t. \sum_{\theta \in \Theta, a^j \in \mathcal{A}_j} q_{t+1}\left(\theta, (h_t^j, a^j)\right) \mathcal{U}_{a^j,:}^{\theta} \geq l_{h_t^j} \mathbf{1}^T,$$

$$\forall t = 1, 2, ..., T+1, h_t^j \in \mathcal{H}_t^j \tag{5.17}$$

$$q_1(h_1^j; \theta) = 1, \forall \theta \in \Theta, \tag{5.18}$$

$$\sum_{a_t^j \in \mathcal{A}_j} q_{t+1}((h_t^j, a_t^j); \theta) = q_t(h_t^j; \theta),$$

$$\forall \theta \in \Theta, h_t^j \in \mathcal{H}_t^j, \forall t = 1, \ldots, T, \tag{5.19}$$

$$q_t(h_t^j; \theta) \geq 0, \forall \theta \in \Theta, h_t^j \in \mathcal{H}_t^j,$$

$$\forall t = 2, \ldots, T+1, \tag{5.20}$$

where $q \in Q$ is a set of all properly dimensioned real vectors, L is a properly dimensioned real space, and (h_t^j, a_t^j) corresponds to a concatenation.

The above linear program can be used to solve the approximated security strategy for the informed player as follows:

$$\bar{\sigma}_{\lambda,T}^{a^j}(\theta, p) = q_2^*(a^j, \theta), \forall a^j \in \mathcal{A}_j \tag{5.21}$$

where q_2^* is the optimal solution of the linear program in (5.16) - (5.20). Interested reader is encouraged to see [89] for further details.

The Informed Player's Approximated Security Strategy Algorithm

Th LP-based algorithm for the informed player to compute his approximated security strategy and update belief state in λ-discounted asymmetric repeated game is presented as follows [89]:

1. Initialization:

    (a) Read payoff matrices $\mathcal{U}$, prior probability p_0, and system state θ.

    (b) Set receding horizon length T.

    (c) Let $t = 1$, and $p_1 = p_0$.

2. Compute the informed player's approximated security strategy $\bar{\sigma}_{\lambda,T}$ based on (5.21) with $p = p_t$.

3. Choose an action $a^j \in \mathcal{A}_j$ according to the probability $\bar{\sigma}_{\lambda,T}(\theta, p_t)$, and announce it publicly.

4. Update the belief state p_{t+1} according to (5.13).

5. Update $t = t + 1$ and go to step 2.

5.4.2 The Uninformed Player's Approximated Security Strategy Algorithm

The uninformed player does not have access to the informed player's strategy or belief state p_t, therefore, p_t cannot serve as his sufficient statistics. Given the λ-discounted asymmetric repeated primal game $\Gamma_\lambda(p)$, its dual game $\widetilde{\Gamma}_\lambda(w)$ is defined with respect to p, where $w \in \mathbb{R}^{|\Theta|}$ is called the initial regret. The dual game is played the same way as the primal game with the exception that the system state is chosen by the informed player instead of nature. In the dual game, the uninformed player is still not informed of the system state. The informed player's payoff (or equivalently the uninformed player's penalty) in the dual game $\widetilde{\Gamma}_\lambda(w)$, when it uses p to choose system state is defined in (5.22).

$$\widetilde{\mathcal{U}}_\lambda(w, p, \sigma, \tau) = \mathbb{E}_{p,\sigma,\tau}\left[w^\theta + \sum_{t=1}^{\infty} \lambda(1-\lambda)^{t-1}\mathcal{U}(\theta, a_t^j, a_t^0) \right] \tag{5.22}$$

The game value $\widetilde{V}_\lambda(w)$ of the dual game $\widetilde{\Gamma}_\lambda(w)$ satisfies the following equation (5.23).

$$\widetilde{V}_\lambda(w) = \min_{\tau \in \mathcal{T}} \max_{p \in \Delta(\Theta), \sigma \in \Sigma} \widetilde{\mathcal{U}}_\lambda(w, p, \sigma, \tau) = \max_{p \in \Delta(\Theta), \sigma \in \Sigma} \min_{\tau \in \mathcal{T}} \widetilde{\mathcal{U}}_\lambda(w, p, \sigma, \tau) \tag{5.23}$$

Moreover, the game value $\widetilde{V}_\lambda(w)$ of the dual game and the game value $V_\lambda(p)$ of the primal game are related in the following way.

$$\widetilde{V}_\lambda(w) = \max_{p\in\Delta(\Theta)} \left\{V_\lambda(p) + p^T w\right\} \tag{5.24}$$

$$V_\lambda(p) = \min_{w\in\mathbb{R}^{|\Theta|}} \left\{\widetilde{V}_\lambda(w) - p^T w\right\} \tag{5.25}$$

The regret $\mu_t^\theta(h_t^j)$ in state θ is defined as the difference between the expected realized utility so far and the security level of eNode B's security strategy, given state θ, i.e.

$$\mu_t^\theta(h_t^j) = -\mu^{\theta *} + E_{\bar{\tau}}\left(\sum_{s=1}^{t-1} \lambda(1-\lambda)^{s-1}\mathcal{U}^j(a_s^j, a_s^0)|\theta, h_t^j\right) \tag{5.26}$$

$$\mu^{\theta *} = \max_{\sigma(\theta)\in\Sigma(\theta)} E_{\sigma(\theta),\tau^*}\left(\sum_{s=1}^{\infty} \lambda(1-\lambda)^{s-1}\mathcal{U}^j(a_s^j, a_s^0)|\theta\right) \tag{5.27}$$

where τ^* is the eNode B's security strategy, $\sigma(\theta)$ indicates jammer's behavior strategy given $\theta\in\Theta$, and $\Sigma(\theta)$ is the corresponding set including all $\sigma(\theta)$.

The anti-discounted regret $w_t^\theta(h_t^j)$ at stage t with respect to the state θ given the informed player's history action sequence $(h_t^{\mathcal{A}_j})$ is defined as follows in (5.28).

$$w_t^\theta(h_t^j) = \frac{\mu_t^\theta(h_t^j)}{(1-\lambda)^{t-1}}, \forall\theta\in\Theta \tag{5.28}$$

The anti-discounted regret $w_t^\theta(h_t^j)$ can be recursively computed as follows in (5.29) with $w_1 = w$.

$$w_{t+1}^\theta(h_t^j, a_t^j) = \frac{w_t^\theta(h_t^j) + \lambda\, \mathcal{U}^\theta(a_t^j, :)\bar{\tau}(h_t^j)}{1-\lambda}, \forall\theta\in\Theta \tag{5.29}$$

It is shown in [64] that the security strategies of the uninformed player in both primal and dual games depend only on the informed player's history actions and that the optimal security strategy w^* of the uninformed player in the dual game $\widetilde{\Gamma}_\lambda(w^*)$ is also his optimal security strategy in the primal game $\Gamma_\lambda(p)$. Mathematically speaking, w^* is the optimal solution of the problem on the right hand side of (5.25) and logically, it is the uninformed player's worst case regret of his security strategy.

It is shown in [89] that anti-discounted regret w_t is the sufficient statistics for the uninformed player in the dual game, i.e., the uninformed player can fully rely on w^* and its anti-discounted update w_t to compute his security strategy. However, computing w^* is difficult because it relies on the uninformed player's optimal security level μ^* and game value in the primal game, which are non-convex [107]. Furthermore, computation of the uninformed player's security strategy in the dual game is also non-trivial because of non-convexity. Therefore, [89] proposed using approximated security level $\mu^{\theta\star}$ for approximating w^* for a T-stage truncated version $\Gamma_{\lambda,T}(p)$ of the primal game that is defined as follows.

$$\mu^\theta_{\lambda,T}(\bar{\tau}^*) = -\max_{\bar{\sigma}(\theta)\in\bar{\Sigma}(\theta)} \mathbb{E}_{p,\bar{\sigma},\bar{\tau}^*}\left[\sum_{t=1}^{T} \lambda(1-\lambda)^{t-1}\mathcal{U}(\theta, a^j_t, a^0_t)|\theta\right] \tag{5.30}$$

In $\Gamma_{\lambda,T}(p)$, the conditional expected total payoff $\mathcal{U}_{\lambda,T}(\bar{\tau};\theta,h^j_{T+1})$ given uninformed player's strategy $\bar{\tau}\in\bar{\mathcal{T}}$, system state $\theta\in\Theta$, and informed player's history action sequence $h^j_{T+1}\in\mathcal{H}^j_{T+1}$ is defined in (5.31).

$$\mathcal{U}_{\lambda,T}(\bar{\tau};\theta,h^j_{T+1}) = \mathbb{E}_{\bar{\tau}}\left[\sum_{t=1}^{T} \lambda(1-\lambda)^{t-1}\mathcal{U}(\theta, a^j_t, a^0_t)|\theta, h^j_{T+1}\right] \tag{5.31}$$

which satisfies the following:

$$\mathcal{U}_{\lambda,T}(\bar{\tau};\theta,h^j_{T+1}) = \sum_{t=1}^{T} \lambda(1-\lambda)^{t-1}\mathcal{U}^\theta(a^j_t,:)y_{h^j_t} \tag{5.32}$$

Li & Shamma constructed the following linear program to compute the approximated game value $V_{\lambda,T}(p)$, i.e. the approximated security level $\mu^{\theta\star}$ in a λ-discounted asymmetric repeated game $\Gamma_\lambda(p)$:

$$V_{\lambda,T}(p) = \min_{y\in Y, l\in\mathbb{R}^{|\Theta|}} \sum_{\theta\in\Theta} p^\theta l^\theta \tag{5.33}$$

$$s.t. \sum_{t=1}^{T} \lambda(1-\lambda)^{t-1} \mathcal{U}^\theta(a_t^j, :) y_{h_T^j} \leq l^\theta, \forall\theta\in\Theta,$$

$$\forall h_T^j \in \mathcal{H}_T^j, a_t^j \in \mathcal{A}_j, \tag{5.34}$$

$$\mathbf{1}^T y_{h_t^j} = 1, \forall h_t^j \in \mathcal{H}_t^j, \forall t = 1, ..., T, \tag{5.35}$$

$$y_{h_t^j} \geq \mathbf{0}, \forall h_t^j \in \mathcal{H}_t^j, \forall t = 1, ..., T \tag{5.36}$$

where Y is properly-dimensioned real space, and $\mathcal{U}_\lambda(y;\theta,:)$ is a $|\mathcal{H}_{T+1}^j|$ dimensional column vector whose element $\mathcal{U}_\lambda(y;\theta,h_{T+1}^{\mathcal{A}_j})$ is a linear function of y satisfying the equation (5.32). The approximated anti-discounted regret is $w^* = -\mu^{\theta\star} = -l^*$, where l^* is the optimal solution to the LP problem.

The eNode B has a stationary security strategy that only depends on the anti-discounted regret w_t [89]. Define eNode B's stationary behavior strategy as $\bar{\tau} : \mathbb{R}^{|\theta|} \to \Delta(\mathcal{A}_0)$. Computing the stationary security strategy of eNode B is non-convex [89]. Therefore, an approximated stationary security strategy $\bar{\tau}(w)$ of eNode B is proposed in [89], which can be computed by solving the following LP problem for $\widetilde{V}_{\lambda,T+1}(w)$ in the zero-sum λ-discounted $T+1$-stage dual game $\widetilde{\Gamma}_{\lambda,T+1}(w)$

$$\widetilde{V}_{\lambda,T+1}(w) = \min_{y\in Y, l\in\mathbb{R}^{|\Theta|}, L\in\mathbb{R}} L \tag{5.37}$$

$$s.t.\ w + l \leq L\mathbf{1}, \tag{5.38}$$

$$s.t.\ \sum_{t=1}^{T+1} \lambda(1-\lambda)^{t-1} \mathcal{U}^{\theta}(a^j, :) y_{h^j_{T+1}} \leq l^{\theta}, \forall \theta \in \Theta,$$
$$\forall h^j_{T+1} \in \mathcal{H}^j_{T+1}, a^j \in \mathcal{A}_j, \tag{5.39}$$

$$\mathbf{1}^T y_{h^j_t} = 1, \forall h^j_t \in \mathcal{H}^j_t, \forall t = 1, ..., T+1, \tag{5.40}$$

$$y_{h^j_t} \geq \mathbf{0}, \forall h^j_t \in \mathcal{H}^j_t, \forall t = 1, ..., T+1 \tag{5.41}$$

where Y is properly-dimensioned real space, and $\mathcal{U}_{\lambda,T+1}(y; \theta, :)$ is a $|\mathcal{H}^j_{T+2}|$ dimensional column vector whose element $\mathcal{U}_{\lambda,T+1}(y; \theta, h^{\mathcal{A}_j}_{T+2})$ is a linear function of y satisfying the equation (5.32). The uninformed player's approximated security strategy $\bar{\tau}_{\lambda,T}(w)$ is $y^*_{h^j_1}$, when the anti-discounted regret at stage t is $w_t = w$.

Li & Shamma further showed that the truncated game value $\widetilde{V}_{\lambda,T}$ converges to $\widetilde{V}_{\lambda}$ exponentially fast with respect to the time horizon T with convergence rate $1-\lambda$. Curious reader is encouraged to see [89] for further details.

The Uninformed Player's Approximated Security Strategy Algorithm

Th LP-based algorithm for the uninformed player to compute his approximated security strategy in λ-discounted asymmetric repeated game $\Gamma_{\lambda}(p_0)$ is presented as follows [89]:

1. Initialization:

   (a) Read payoff matrices $\mathcal{U}$, and prior probability p_0.

(b) Set receding horizon length T.

(c) Solve the LP problem (5.33) - (5.36) with $p = p_0$ and let $\mu^* = l^*$.

(d) Let $t = 1$ and $w_1 = -\mu^*$.

2. Solve the LP problem (5.37) - (5.41) with $w = w_t$, and the uninformed player's approximated security strategy $\bar{\tau}(w_t) = y^*_{h_1^j}$.

3. Choose an action $a^0 \in \mathcal{A}_0$ according to the probability $\bar{\tau}_{\lambda,T}(w_t)$, and announce it publicly.

4. Read the informed player's action, and update the anti-discounted regret w_{t+1} according to (5.29).

5. Update $t = t + 1$ and go to Step 2.

5.4.3 The Uninformed Player's Expected Security Strategy Algorithm

The "Expected Strategy" algorithm for the eNode B is defined as a simplex Δ over its complete-information single-shot game security strategies σ_1 with the same probability as prior p_0. In other words, the eNode B would play the complete-information single-shot security strategies $\sigma_1|\theta = 1$ and $\sigma_1|\theta = 2$ with the probabilities p_0^1 and p_0^2 respectively. Since, the prior is common knowledge, it alleviates eNode B from "learning" and "full monitoring" in a repeated game. Thus, the eNode B essentially plays a single-shot strategy in a repeated game but without the requirement of "full monitoring", which may not be such a bad idea if the jammer plays "non-revealing" strategies. Furthermore, the network does not need to observe jammer's action with certainty that leads to more practical implementations. Both discounted and average payoff formulations can be used with this algorithm.

In this chapter, the approximated security strategy and expected security strategy algorithms described above would be used to design strategies for both the *smart jammer* and the LTE network. Both discounted and average cost formulations would be used in infinite-horizon asymmetric information games.

5.5 Performance Analysis of Repeated Game Strategy Algorithms

The zero-sum game-theoretic algorithms presented earlier in this chapter are used to devise "approximated" strategy formulation for the network both in the average cost and discounted cost sense. Although, average cost formulation was not developed by [89], probably due to convergence and boundedness issues associated with generalized average cost, utility functions used in this research are bounded and hence convergence may not pose a serious problem. However, "approximated" algorithms require "full monitoring", i.e. the network has to observe jammer's action at every stage with certainty. Therefore, "expected" formulation is also employed in which the network being the uninformed player simply plays its single-shot *best response (BR)* in an expected sense, i.e. it would play single-shot BR with the same probability distribution as the prior probability of jammer occurrence, which is common knowledge. This enables the network to alleviate "full monitoring" requirement, i.e. the network does not have to observe jammer's action with certainty and leads to more practical implementation.

The performance of both "approximated" and "expected" algorithms for both discounted and average cost formulations is characterized in the following sections. However, not all of the simulation results can be shared here for the sake of time and space constraints. The following parameters in addition to the single-shot case were used for repeated game simulation: discount facot $\lambda = 0.70$ and receding horizon length $T = 4$.

5.5.1 eNode B vs. Cheater

Jammer Strategy

When the *Cheater* is in the network, it always uses his "approximated" algorithm to devise repeated game strategy against the network. Also, being the informed player, there is no ambiguity about the system state so *Cheater* can decide to reveal his superior information as much as it suits him. The Cheater's steady state belief state p_t and repeated game strategy vs. prior probability are shown in Fig. 5.1 and Fig. 5.2 respectively, where p^1 and p^2 represent updated belief (probability) about the states $\theta = 1$ and $\theta = 2$ respectively and a_j^k represents *kth* pure action of the Cheater. It is interesting to note that the Cheater always plays the same security (pure) strategy that he uses for single-shot game, independent of the prior probability. It is also interesting to know that Cheater's strategies are **non-revealing** [2], even at relatively low prior probability of his occurrence when $p_0^1 \geq 0.25$. This means that the network does not "learn" anything new about the jammer type from jammer's repeated actions even in the case of "full-monitoring" when $p_0^1 \geq 0.25$ and Cheater takes full advantage of his superior information. At relatively low prior probability of Cheater's occurrence ($p_0^1 < 0.25$), the jammer reveals very little information in the first stage when the belief state gets updated to $p_0 = [0.25\ 0.75]^T$, but it remains the same after that. This puts the network at a disadvantageous position in the game if the network plays as a Bayesian player, even when it can observe jammer's actions perfectly at every stage.

eNode B Strategies

The eNode B's steady state "approximated" and "expected" security strategies vs. prior probability p_0^1 are plotted in Fig. 5.3, and Fig. 5.4, respectively, where a_0^k represents *kth* pure action of the eNode B. The network's strategies (both "expected" and "approximated") evolve with varying prior probability levels as it is the uninformed player. The "approximated" strategy relies on full monitoring and switches to a different strategy at $p_0^1 \geq 0.35$, when it starts playing *'Throttling'* (its security strategy against Cheater in complete-information single-shot game) in addition to playing *'Change f_c'*. On the other hand, the "expected" algorithm does not rely on full monitoring and hence uses an expec-

[2] The informed player is said to play non-revealing at stage n when the posterior probabilities in (5.13) do not change at that stage if his mixed move at stage n is independent of the state $\theta \in \Theta$ for all values of θ for which $p_n^\theta > 0$. In case when full monitoring is assumed, not revealing the information is equivalent to not using that information, [66].

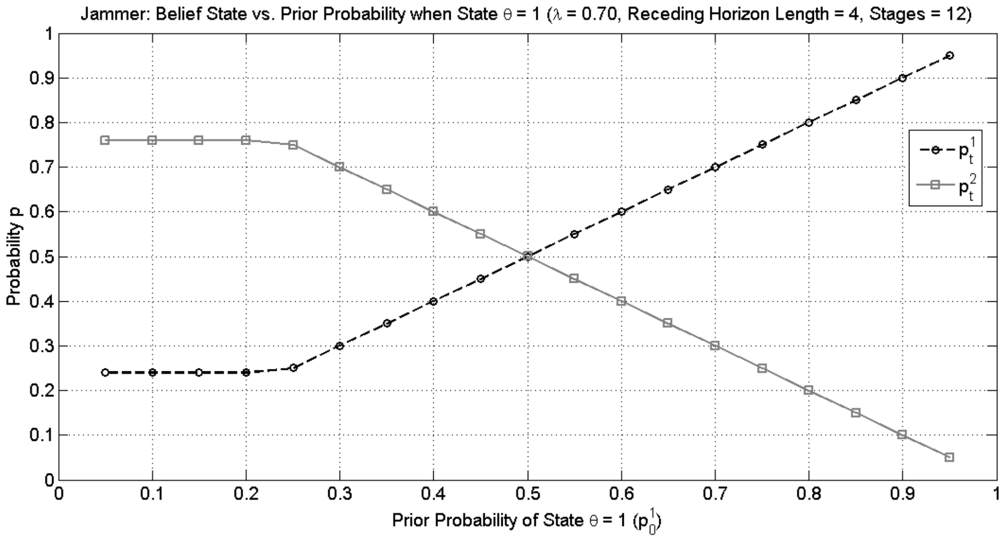

Figure 5.1: Cheater's Steady State Belief State vs. Prior p_0^1

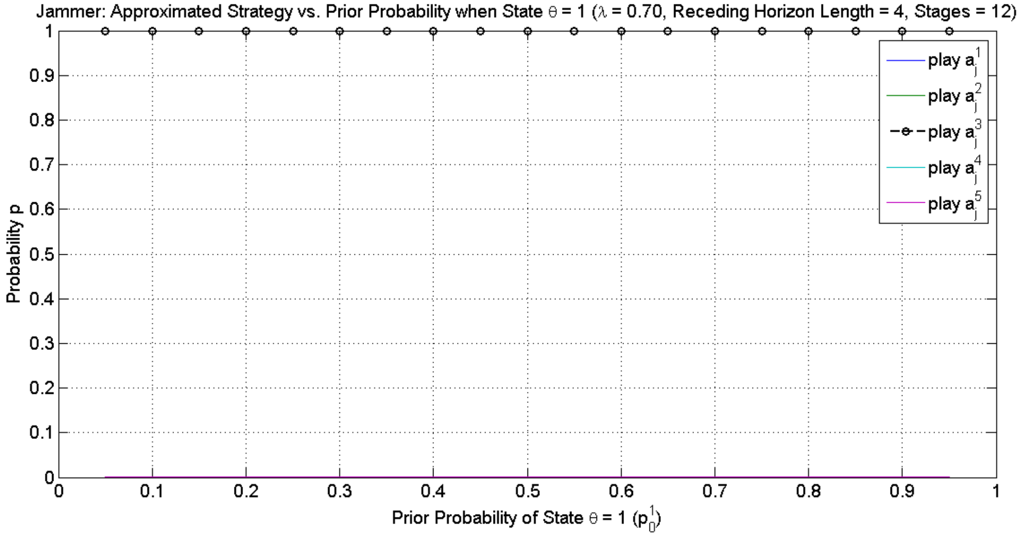

Figure 5.2: Cheater's Steady State Approximated Strategy vs. Prior p_0^1

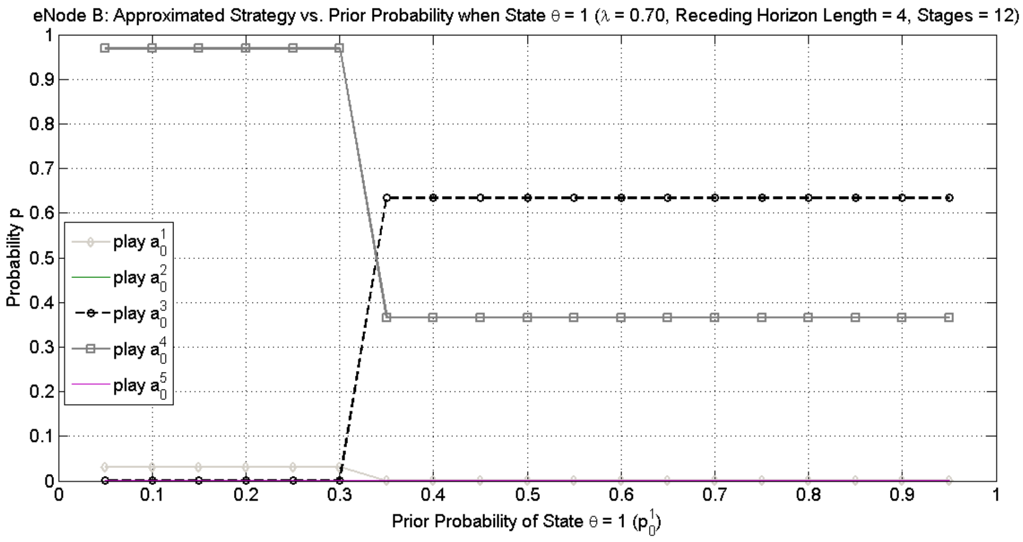

Figure 5.3: eNode B's Steady State Approximated Strategy against Cheater vs. Prior p_0^1

tation of its single-shot strategies involving playing mixed strategy over *'Normal', 'Throttling'* and *'Change Timing'*. The "expected" strategy is pre-computed based on the prior probability and does not change as the game proceeds, whereas the "approximated" algorithm converges in around 12 stages. The "expected" strategy algorithm may work well enough for the network as the jammer's strategies are mostly non-revealing and "approximated" algorithm requires "full-monitoring".

eNode B's Utilities

The eNode B's "approximated" and "expected" λ-discounted and average utility values are plotted in Fig. 5.5 at different prior probability p_0^1 levels. The "approximated" security strategy algorithm with discounted cost performs almost optimally when $p_0^1 \geq 0.35$, whereas the "expected" algorithm with discounted cost performs poorly as compared to its counterpart "approximated" algorithm with the exception of low prior values. The "approximated" algorithm uses full-monitoring and repeated game LP formulation to compute its strategy and hence performs much better than its counterpart. On the other hand, the "expected" algorithm only relies on the prior probability and does not observe jammer's actions, hence, ends up underperforming even when the jammer uses its single-shot security

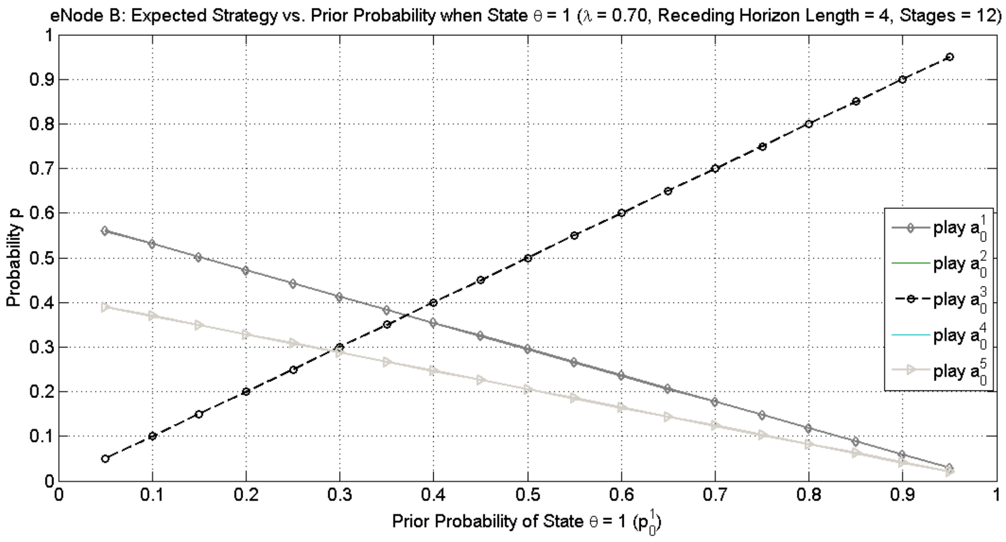

Figure 5.4: eNode B's Expected Strategy vs. Prior p_0^1

strategy.

The average utility value does not reach the optimal complete-information single-shot level for both "approximated" and "expected" formulations. However, "approximated" average cost formulation trails the discounted cost at high prior values and even performs better at low prior events when discounted cost formulation breaks down. The "expected" strategy formulation with average cost performs linearly better with increasing prior p_0^1 values, similar to discounted cost case. Hence, both discounted and average cost solutions perform very similar for a particular algorithm, i.e. the cost selection does not change the inherent behavior of the underlying algorithm. Both cost formulations perform essentially the same for "expected" strategy algorithm. However, in case of "approximated" algorithm, discounted cost mostly performs better than average cost, primarily because the algorithm is developed for discounted case.

When prior probability for Cheater's occurrence is low (i.e., $p_0^1 < 0.35$), all of the formulations discussed above fail to even come close to the complete-information single-shot value. This happens due to the fact that it is rather unlikely for the Cheater to be present in the network at such low prior value and eNode B strategy algorithms are not robust enough to address this unlikely event.

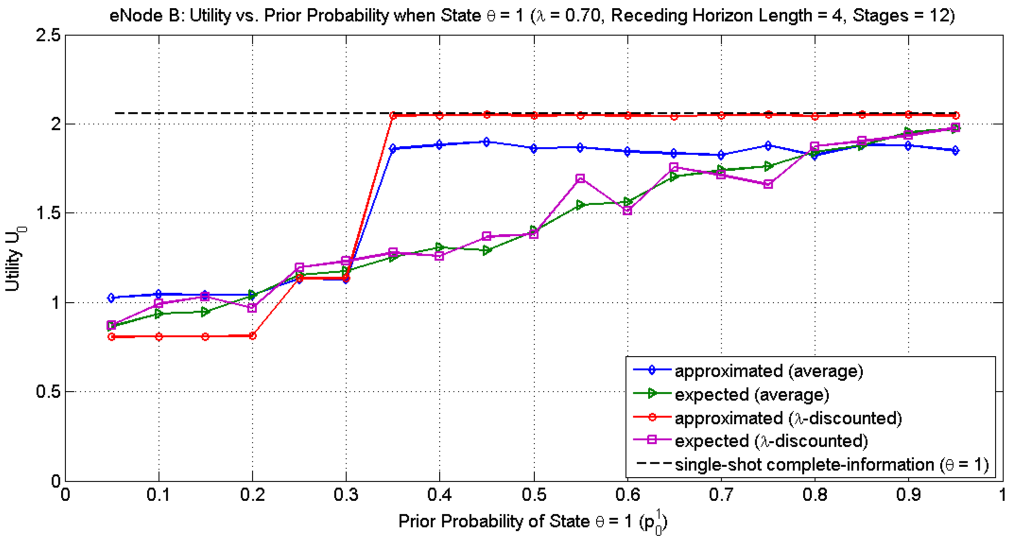

Figure 5.5: eNode B's Utility against Cheater vs. Prior p_0^1

5.5.2 eNode B vs. Saboteur

Jammer Strategy

Similar to the eNode B vs. Cheater game, Saboteur's steady state belief states p_t and "approximated security" strategies vs. prior probability of his occurrence p_0^2 are shown in Fig. 5.6 and Fig. 5.7, respectively. It is very interesting to note that being the informed player, Saboteur plays **non-revealing** and **"misleading"** strategies even at prior probability values as high as $p_0^2 = 0.85$ (and sometimes up to $p_0^2 = 0.80$). It plays its state $\theta = 1$ (Cheater) dominant security strategy while actually being a type $\theta = 2$ (Saboteur) jammer. At very high prior probability values of $0.75 \leq p_0^2 \leq 0.85$, jammer further tricks the network by revealing misinformation which causes the belief state to show higher probability of Cheater's presence than the prior. However, at prior probability levels of $p_0^2 \geq 0.90$, a little information about the Saboteur's ($\theta = 2$) presence is revealed by playing its single-shot game security strategy (play *'Jam CS-RS + PUCCH'* and *'Jam CS-RS + PUCCH + PCFICH + PRACH'* with almost the same probability) for the correct jammer type. Hence, the jammer uses its superior information to its complete advantage even when full monitoring is allowed. This is a good example of the strength of superior information and how

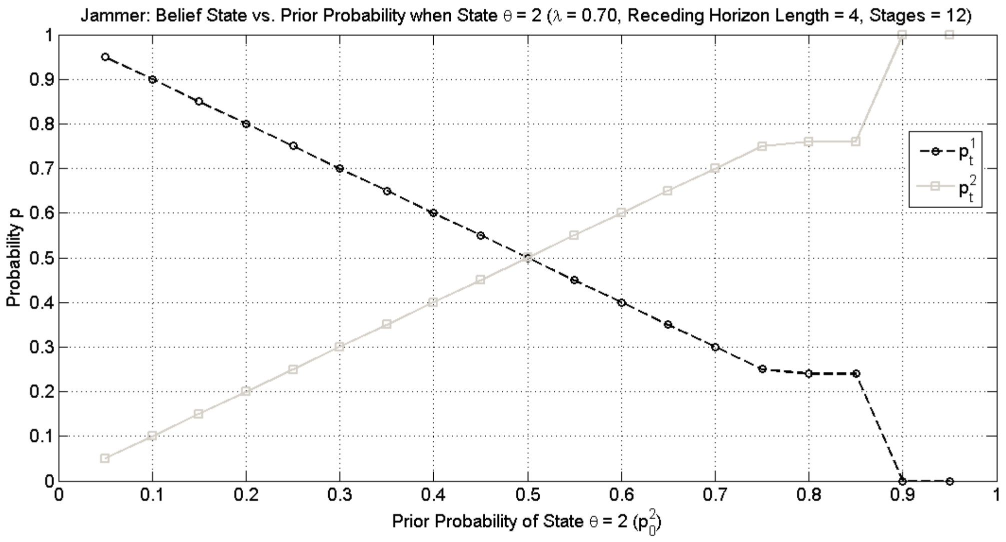

Figure 5.6: Saboteur's Steady State Belief State vs. Prior p_0^2

it can be exploited in asymmetric games against an adversary.

eNode B Strategies

Similar to the repeated game against Cheater, the eNode B adapts its repeated game strategy against Saboteur as the game proceeds. From the simulations, eNode B's strategy seems to converge in 12 stages. The "expected" strategy is shown in Fig. 5.8 and is deployed similar to the game against Cheater. Since, "expected" strategy algorithm is oblivious to the actual jammer type and does not use full monitoring, its mixed strategy does not depend on the system state θ and is played solely based on the prior probability value.

On the other hand, the "approximated" security strategy algorithm relies on the repeated game and full monitoring to adapt its strategy. The network's steady state "approximated" strategy vs. prior probability p_0^2 is plotted in Fig. 5.9. As mentioned above, the jammer plays completely non-revealing and misleading strategies for $p_0^2 \leq 0.85$ and hence, eNode B gets tricked into believing that it is playing against Cheater, where in fact it is playing against the Saboteur. This leads the network to play the same strategy that it played against Cheater with relatively high probability of Cheater's occurrence. It gets further tricked by the jammer into believing the incorrect jammer type when the jammer keeps playing its

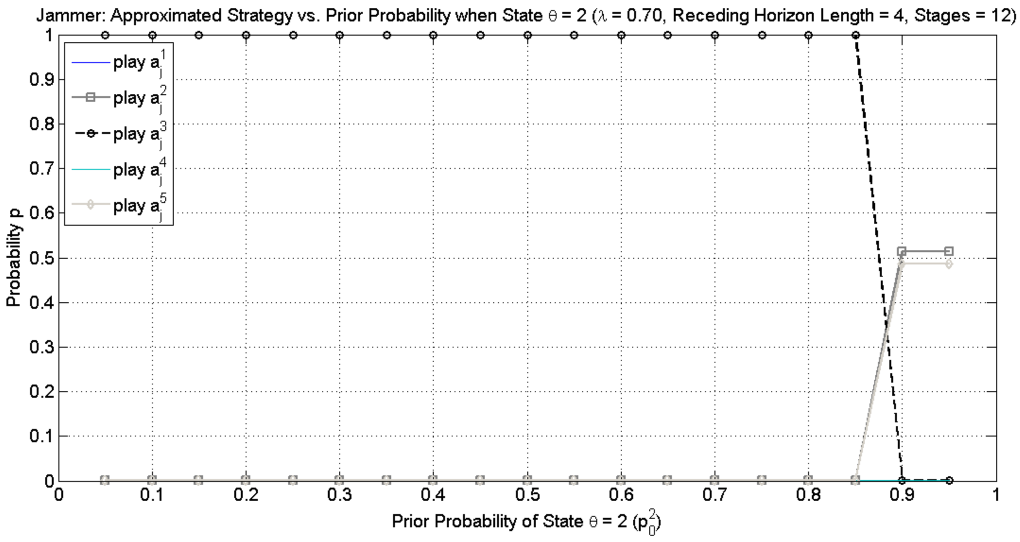

Figure 5.7: Saboteur's Steady State Approximated Strategy vs. Prior p_0^2

"trick strategy" even at very high levels of prior probability. At that time, the network switches to more aggressive interference avoidance scheme of *'Change f_c'* with very high probability. The network gets the correct information only when the jammer switches its strategy at $p_0^2 \geq 0.90$ and then the network adapts its defense strategy accordingly. It is curious to see how the network gets tricked by the jammer even with full monitoring because it lacks information about the system state.

eNode B's Utilities

The network's λ-discounted and average utility values for both "approximated" and "expected" security strategy algorithms are plotted against prior probability values p_0^2 in Fig. 5.10. The jammer strategies are mostly non-revealing and hence, eNode B does not seem to "learn" much about the jammer type from its repeated interaction. Therefore, the "approximated" security strategy formulation with discounted cost performs very poorly until $p_0^2 < 0.70$. At $p_0^2 = 0.70$, the eNode B switches its strategy to playing *'Change f_c'* and catches up to the optimal value at $p_0^2 \geq 0.80$. Obviously, the jammer also uses full monitoring and is forced to come out and play revealing strategy at $p_0^2 \geq 0.90$.

On the other hand, "expected" strategy algorithm with discounted cost seems to per-

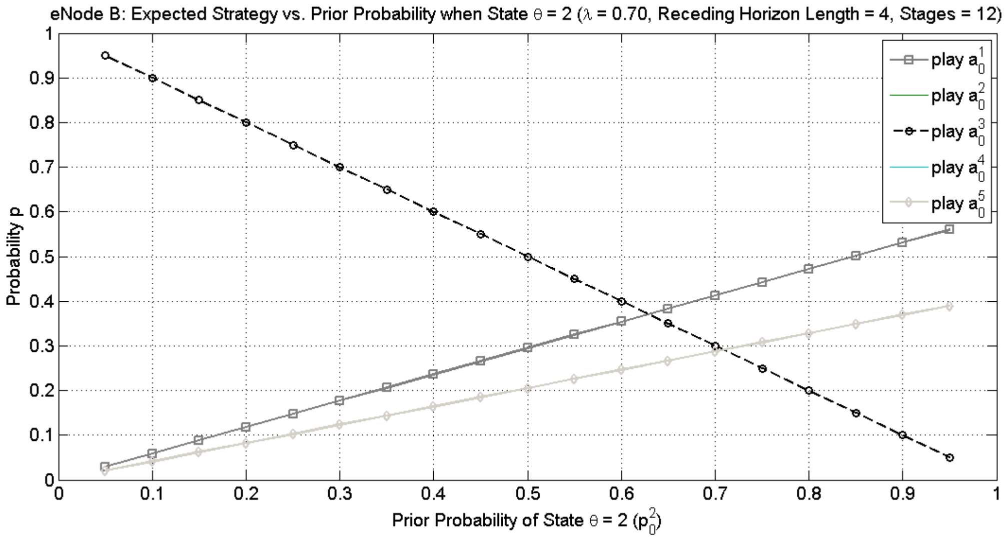

Figure 5.8: eNode B's Expected Strategy vs. Prior p_0^2

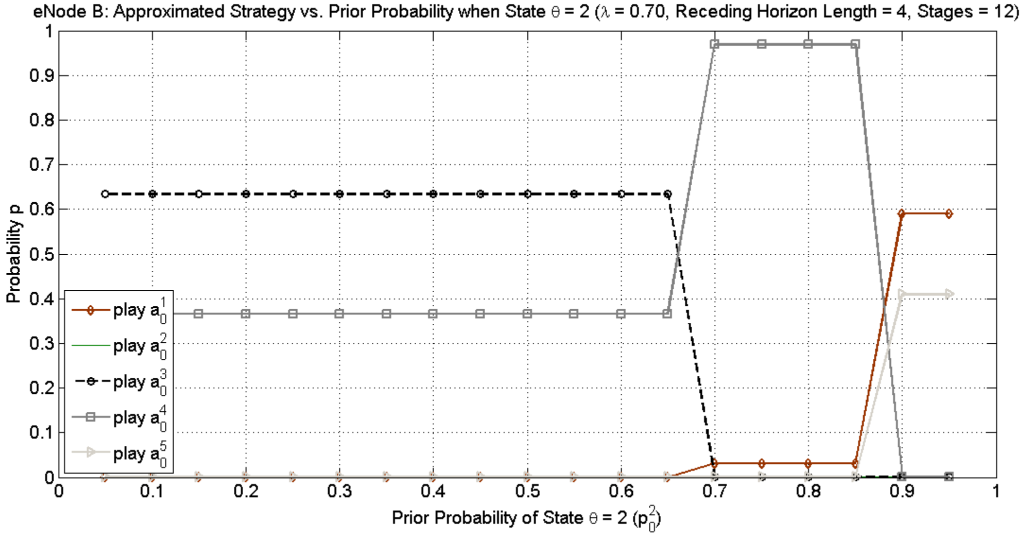

Figure 5.9: eNode B's Steady State Approximated Strategy against Saboteur vs. Prior p_0^2

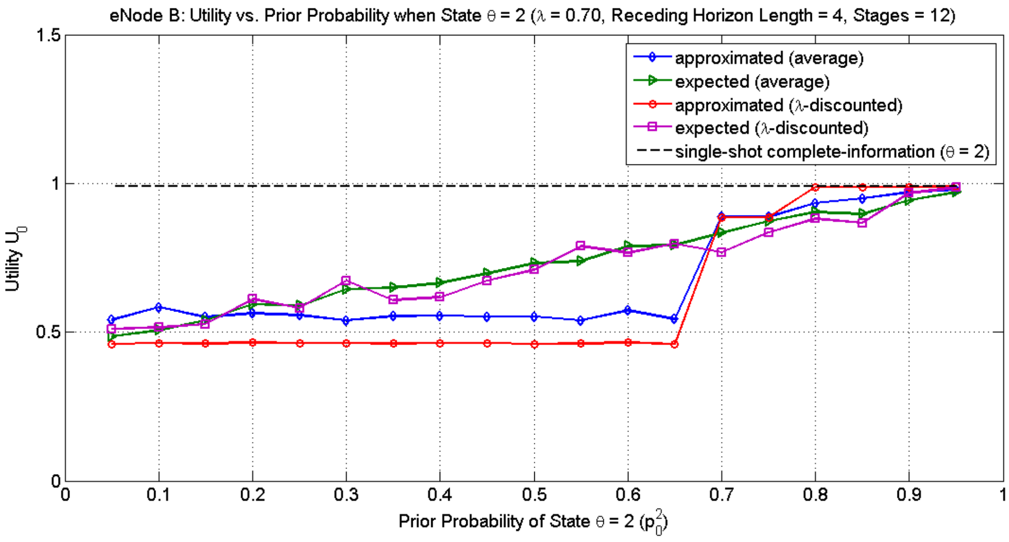

Figure 5.10: eNode B's Utility against Saboteur vs. Prior p_0^2

form better than the "approximated" security strategy as it does not get tricked by the jammer's non-revealing strategies due to its oblivion. It appears that the "expected" strategy algorithm outperforms its counterpart when $p_0^1 \leq 0.30$ (or equivalently, $p_0^2 \geq 0.70$) given that the Cheater is present in the network and $p_0^2 < 0.70$ (or equivalently, $p_0^1 > 0.30$) when Saboteur is present in the network. Thus, it performs better in low prior probability regions, when eNode B does not expect a certain jammer type in the network.

Similar to eNode B vs. Cheater case, "expected" strategy formulation with both average and discounted costs performs very close to each other. Also, "approximated" formulation with average cost follows the same behavior as discounted cost formulation, and performs better at low prior values, similar to eNode B vs. Cheater scenario.

Nevertheless, it becomes clear that the network is at a very disadvantageous position in the game against the *smart jammer* due to its lack of information and can be easily misled by the jammer. Furthermore, the "approximated" and "expected" strategy algorithms work in a complementary sense in favor of the network, and the choice of cost formulation does not affect the algorithm's behavior.

5.6 Summary

In this chapter, the eNode B and the *smart jammer* dynamics are modeled as a strictly competitive zero-sum repeated game for tractability purposes, while preserving all the important elements of infinite-horizon interaction between players and lack of information on the network side. The solution of a complete-information single-shot game is based on very familiar security strategies that lead to a Nash equilibrium. However, tractable optimal strategy formulations do not exist in game-theoretic literature, especially for the uninformed player in infinite-horizon repeated games. Therefore, LP formulations from a recent work [89] are used for "approximated" security strategy algorithms to compute repeated game strategies for both players efficiently. In addition, simplistic "expected" security strategy algorithm is also used for the network that does not require "full monitoring".

This chapter also presents and discusses performance characterization of above-mentioned algorithms. Two different cost formulations namely λ-discounted and average cost are used for both algorithms. It turns out that the jammer is able to play non-revealing strategies most of the time, which implies that the network is unable to learn any new information about the jammer type in repeated games even with full monitoring. Hence, at low prior values, the eNode B performs worse (or equivalently, the smart jammer performs better) in repeated games as compared to hypothetical complete-information single-shot game. In the game against Cheater, the "approximated" security strategy algorithm is able to strategize against the jammer rather quickly and achieves its optimal utility because the jammer plays its single-shot game security strategy in repeated game. However, this advantage goes away in the game against the Saboteur, when the jammer plays non-revealing and misleading strategies for a wide range of prior probabilities. Nevertheless, the network's algorithm eventually catches up and forces the jammer to reveal its true type. In both the cases, average cost performs a little worse than discounted cost at high prior values when "approximated" algorithm catches up to the optimal utility and vice versa at low prior values when discounted cost performs worse.

The "expected" strategy algorithm performs equally well (or sometimes better) as its counterpart "approximated" security strategy algorithm in a complementary fashion at low prior probability values against the Cheater and for a wide range of prior probability values against the Saboteur. This is because it does not get duped by the "misinformation" spread by the jammer due to lack of full monitoring, which plays at its advantage against Saboteur. Both average and discounted cost formulations perform equally well for the "expected" algorithm. However, the "expected" algorithm never reaches the optimal complete-information single-shot value. Nevertheless, the biggest advantage of simplistic "expected" strategy algorithm comes from the fact that it does not require "full monitoring" and hence, can be easily deployed in practical networks. Furthermore, choice of the cost formulation does not seem to make much difference in both algorithms' behavior as anticipated.

It is to be noted here that the zero-sum formulations presented in this chapter only deal with the situation when the jammer is present in the network. Hence, first the network needs to perform jamming sense (presented in Chapter 4) under normal conditions to decide if it is under attack or not. If the network senses jamming attack then it can use algorithms presented in this chapter to counteract jamming attacks.

CHAPTER 6
CONCLUSION

6.1 The Last Word

It is shown that LTE/LTE-A networks are indeed vulnerable to *denial-of-service (DOS)* and *loss-of-service* attacks from *smart jammers* who can "learn" network timing and control channel configuration in order to launch *smart jamming* attacks, without even "hacking" the network or sending an *attach* request. The eNode B and the *smart jammer* dynamics are modeled as an *infinite-horizon repeated Bayesian game with asymmetric information*, with the jammer being the informed player with multiple types, and the network being the uninformed player. The *smart jammer* has two different types, namely *Cheater* and *Saboteur*, which determine the system state hidden from the network. Several potential jamming attacks and network countermeasures are proposed, all of which could be implemented using current technology without changing 3GPP specifications. Furthermore, high-fidelity models are developed for the network subcomponents, from channel model to multiuser scheduling, while keeping the overall network dynamics tractable. It is shown that the network suffers huge performance loss in case of a *smart jamming* attack. It is also shown that the network's *best response* not only depends on the jammer's actions but also on its type. Several heuristic and repeated game learning strategy algorithms are presented for the jammer and the network for *general-sum asymmetric repeated games*, which do not rely on the assumption of "full monitoring" (i.e., players cannot observe opponent's actions with certainty), nor do they require any exogeneous information. In addition, jammer type estimation algorithms are presented for the network that use threat mechanism, repeated game learning and non-parametric estimation to estimate jammer's type. These algorithms perform remarkably well under realistic modeling and observational constraints. All of the presented algorithms have been designed with practical constraints in mind so that they are tractable and can be implemented in real networks. It is shown that the network can recover some of its performance loss and may even force an adversary to retract if aforementioned algorithms are employed. Moreover, approximated and expected strategy algorithms are presented for the network and the *smart jammer* for *zero-sum asymmetric repeated games* that can be used to compute suboptimal yet efficient strategies for the players. Although there has been considerable amount of work done on protecting LTE/LTE-A networks from *smart jamming* attacks, this work is far from complete!

6.2 Future Research Directions

The *smart jamming* problem is not limited to LTE/LTE-A networks by any means. The similar concept can be applied to almost any wireless network. This problem is potentially widespread across all the wireless networks especially the ones with protocols and “features”, such as, WWAN cellular networks, WLANs, IoT, vehicle-to-vehicle networks or even some military networks. The most unsettling part is that these *smart jammers* can be easily conceived with the help of an SDR like USRP. This problem is bound to get worse with emerging 5G technologies and Internet of Things (IoT) when everything is going to be connected to the Internet everywhere all the time!

The research work presented in this thesis can be extended in multiple directions. First of all, it needs to consider more involved and sophisticated real-world cellular network deployments, such as multicell configurations, heterogeneous networks, multi-layered and multi-mode networks, device-to-device networks, proliferation of small cells, evolution to 5G and IoT, and more. Second, more sophisticated yet tractable game-theoretic formulations are needed to address this *smart jamming* problem, e.g., repeated Stackelberg games in which the network is the leader and the uninformed player. Third, more sophisticated and original techniques are needed for network countermeasures that can be deployed within real (not realistic) constraints, without sacrificing too much network efficiency and availability or creating more security vulnerabilities. Finally, all of these models and techniques need to be combined together in a coherent and systematic fashion to provide a holistic solution for the *smart jamming* problem!

This research has a huge potential for technological advancements and could have greater impact on our lives and society. It must be pursued further, not for the sole purpose of academic research, but also for the sake of solving a real-world high stake challenge that engineers face from time to time! Without these challenges, the world would be a dull place!!!

Appendices

APPENDIX A
A BRIEF OVERVIEW OF THE LTE AIR INTERFACE

The LTE air interface is an OFDM-based radio link designed to connect subscriber terminals known as *User Equipment (UE)* to the network interface known as *eNode B* [3]. 3GPP specifies LTE air interface in two duplexing modes, namely *Frequency Division Duplexing (FDD)* and *Time Division Duplexing (TDD)*, depending on how the spectrum is allocated/used. Although there are many similarities between the two duplexing modes; this section is focused on FDD mode.

The LTE air interface can be divided into *Downlink (DL)* and *Uplink (UL)* depending on the direction of data transfer, each configured into 10-ms long frames, occupying bandwidths of up to 20 MHz. Each frame is subdivided into ten 1-ms long subframes, which in turn is divided into two slots. Each slot contains seven OFDM symbols when normal *Cyclic Prefix (CP)* is used. This DL frame structure is shown in Fig. A.1 for FDD mode [3]. In the frequency domain, an LTE cell can be configured into various flexible bandwidths ranging from 1.4 MHz - 20 MHz, with subcarrier spacing of 15 KHz for most of the channels. LTE's radio resources are assigned in terms of time-frequency resources. Its DL resource grid is shown in Fig. A.2 [1], indicating *Resource Elements (REs)* and *Resource Blocks (RBs)* [3].

A.1 Mapping of Control Channels

The LTE air interface is composed of *control* and *data channels*, described in Table A.1 and A.2 corresponding to critical DL and UL channels respectively [3]. The *control channels* are mapped to specific time and frequency resources known as *Resource Elements (RE)* and are transmitted according to a pre-defined schedule (periodicity) as per 3GPP specifications

[1] Graphics Source: https://www.slideshare.net/

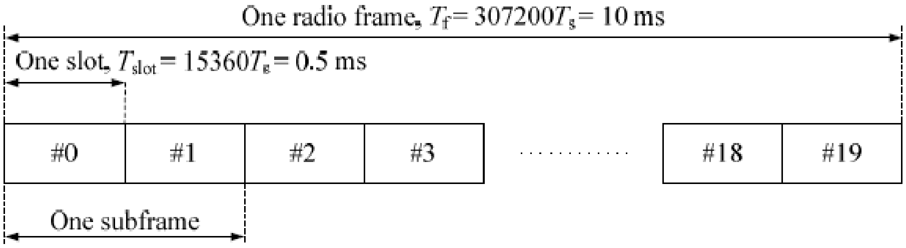
One radio frame, $T_f = 307200T_s = 10$ ms
One slot, $T_{slot} = 15360T_s = 0.5$ ms
#0
#1
#2
#3
#18
#19
One subframe

Figure A.1: 3GPP's LTE DL Frame Structure for FDD Deployments (Type I)

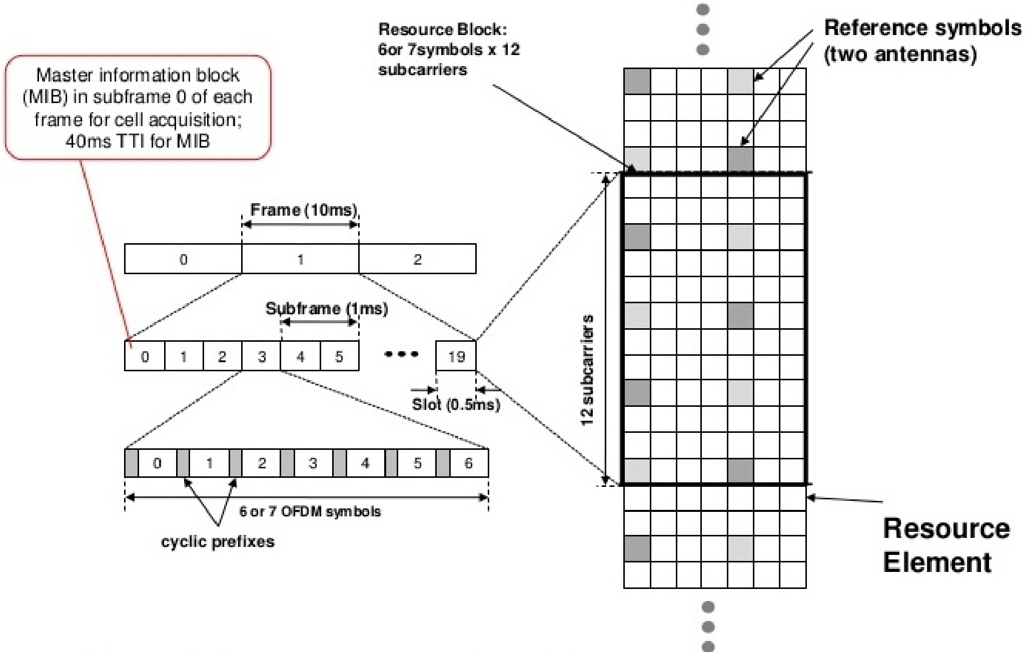
Master information block (MIB) in subframe 0 of each frame for cell acquisition; 40ms TTI for MIB
Resource Block: 6or 7symbols x 12 subcarriers
Reference symbols (two antennas)
Frame (10ms)
0
1
2
Subframe (1ms)
0
1
2
3
4
5
19
Slot (0.5ms)
12 subcarriers
0
1
2
3
4
5
6
6 or 7 OFDM symbols
cyclic prefixes
Resource Element

Figure A.2: 3GPP's LTE DL Resource Grid

[3]. For example:

- PSS & SSS (the sync signals) are transmitted in the last two OFDM symbols of the first slot of the first and sixth subframe of every frame. They are mapped to six *Resource Blocks (RBs)* (1.08 MHz) in the middle of the occupied bandwidth, irrespective of the overall system bandwidth.

- PBCH is transmitted in the first four OFDM symbols of the second slot of the first subframe of every frame. It is mapped to six central RBs, similar to PSS and SSS.

- CS-RS (the pilot symbols) symbols are transmitted every first and third last OFDM symbol of each slot from antenna ports 0 and 1. In frequency domain, they are spaced six subcarriers apart.

- PCFICH is transmitted in the first OFDM symbol of every subframe. It is mapped to sixteen Resource Elements (REs) that span the entire system bandwidth depending on the Cell ID.

- PDCCH is transmitted in 1-4 OFDM symbols of every subframe. PDCCH region is indicated by PCFICH in the first OFDM symbol. In frequency domain, a PDCCH instance is mapped to 1-8 *Control Channel Elements (CCEs)* (36 REs/CCE) depending on the *Downlink Control Information (DCI)* format.

- PUCCH is always mapped to the outside edges of the system bandwidth with frequency hopping in every slot.

- PRACH preamble is mapped to a bandwidth corresponding to six consecutive RBs, whose starting frequency is specified in SIB2. There is no frequency hopping for PRACH.

Table A.1: LTE DL: Critical PHY Channels

Channel	**Acronym**	**Used for**
Synchronization Channel	SCH	Time/frequency synchronization during initial system acquisition; OFDM symbol, slot, subframe, half-frame and radio-frame boundary ID; Cell ID. Two signals: Primary (PSS) and Secondary (SSS)
Physical Broadcast Channel	PBCH	Master Information Block
Physical Downlink Shared Channel	PDSCH	DL data transmission for different users; Upper layer signaling; System Information Blocks (SIBs)
Physical Downlink Control Channel	PDCCH	Resource allocation information for DL and UL; UL power control commands.
Cell-Specific Reference Signal	CS-RS	Initial cell acquisition; Cell-specific reference signal for coherent demodulation of DL channels; DL signal strength measurements for scheduling and handovers
Physical Control Format Indicator Channel	PCFICH	Control format indicator for each DL subframe (PHY-only channel)
Physical Hybrid Indicator Channel		Hybrid ACK/NAK for UL data transmission

Table A.2: LTE UL: Critical PHY Channels

Channel	**Acronym**	**Used for**
Physical Random Access Channel	PRACH	Sending new UL data, control information or ACK/NAK; or Handing over from current serving cell to a target cell in “RRC Connected” but not“UL synchronized” state; or Transition from “RRC Idle” to “RRC Connected” state; or Recovering from RL failure; or Sending a Scheduling Request (SR) occasionally
Physical Uplink Control Channel	PUCCH	UL Control Information (UCI) such as Hybrid ARQ ACK/NAK, CQI, RE. Not transmitted simultaneously with PUSCH
Physical Uplink Shared Channel	PUSCH	UL data transmission from different users, upper layer signaling, and UCI

A.2 UE Acquisition and Data Transfer Procedures

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 during the following events [3, 4]:

- 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.
- Receiving a notification that SI has changed.

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. This *attach request* can only be sent after going through a certain sequence of physical and control channels as discussed below. When a UE powers on or finds coverage after being *OOS*, it goes through the following procedure:

1. Decodes PSS/SSS (sync signals) to get *System Frame Number (SFN)*/subframe boundaries.
2. Decodes PBCH to get *Master Information Block (MIB)* (Bandwidth, SFN, PHICH-config).
3. Decodes PDSCH to get *System Information Block (SIB) 1* (cell suitability, PLMN, cell access info, scheduling of other SIBs).

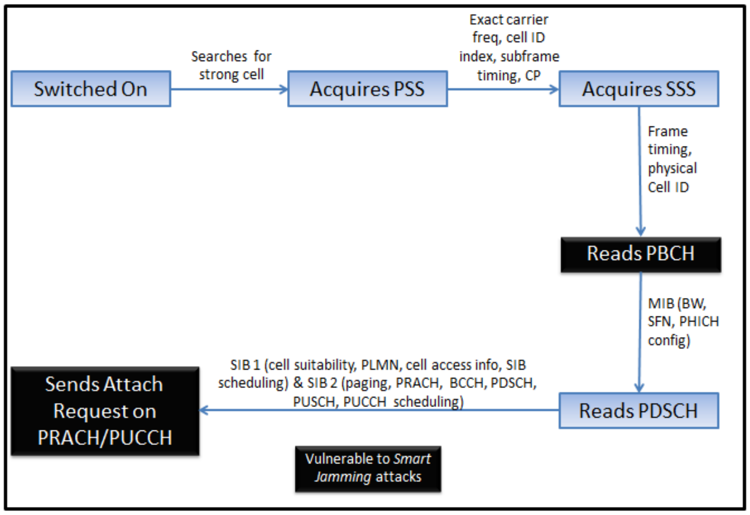
Switched On
Searches for strong cell
Acquires PSS
Exact carrier freq, cell ID index, subframe timing, CP
Acquires SSS
Frame timing, physical Cell ID
Reads PBCH
MIB (BW, SFN, PHICH config)
Reads PDSCH
SIB 1 (cell suitability, PLMN, cell access info, SIB scheduling) & SIB 2 (paging, PRACH, BCCH, PDSCH, PUSCH, PUCCH scheduling)
Sends Attach Request on PRACH/PUCCH
Vulnerable to Smart Jamming attacks

Figure A.3: The LTE UE Attach Procedure

4. Decodes PDSCH to get *SIB 2* (paging, PRACH, BCCH, PDSCH, PUSCH, PUCCH scheduling).

At this point the UE sends an *attach request* on PRACH/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), *SIB 9* (home eNode B info), *SIB 10-11* (ETWS notification), *SIB 12* (CMAS notification) and *SIB 13* (MBMS control info) ([3, 4]). This procedure is shown in Fig. A.3 below [3].

Similarly, 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. In *RRC Connected* state, the UE follows a certain call flow when receiving and/or sending data in the DL and UL, respectively. This data transfer call flow sequence is given below and also shown in Fig. A.4 [3, 4].

- DL data transfer:

  1. UE decodes PCFICH to get *Physical Downlink Control Channel (PDCCH)-*

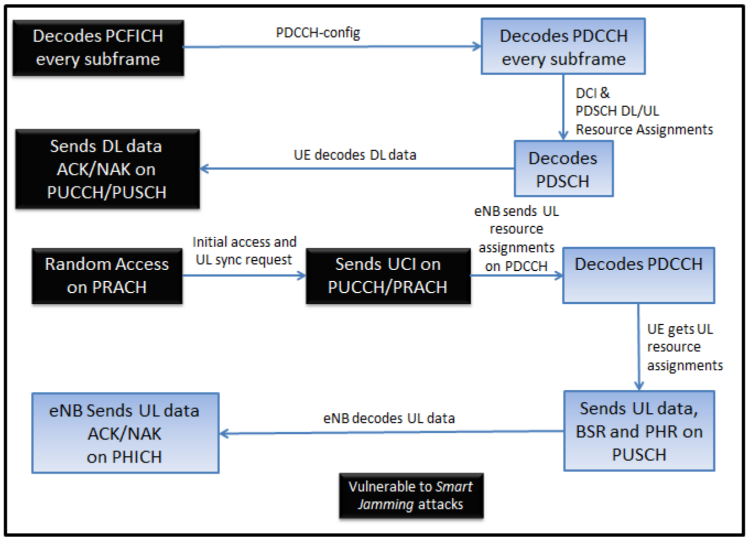
Decodes PCFICH every subframe
PDCCH-config
Decodes PDCCH every subframe
DCI & PDSCH DL/UL Resource Assignments
Sends DL data ACK/NAK on PUCCH/PUSCH
UE decodes DL data
Decodes PDSCH
eNB sends UL resource assignments on PDCCH
Random Access on PRACH
Initial access and UL sync request
Sends UCI on PUCCH/PRACH
Decodes PDCCH
UE gets UL resource assignments
eNB Sends UL data ACK/NAK on PHICH
eNB decodes UL data
Sends UL data, BSR and PHR on PUSCH
Vulnerable to *Smart Jamming* attacks

Figure A.4: LTE DL and UL Data Transfer Call Flow

config.

2. UE decodes PDCCH to get *DL Control Information (DCI)* and resource assignments in PDSCH.
3. UE decodes PDSCH to get DL data and sends ACK/NAK on PUCCH/PUSCH.

- UL data transfer:

  1. UE sends initial access and UL sync requests on PRACH.
  2. UE sends *UL Control Information (UCI)* on PUCCH/PRACH to eNode B scheduler.
  3. eNode B sends UL resource assignments on PDCCH in response.
  4. UE sends UL data, *Buffer Status Report (BSR)* and *Power Headroom (PHR)* on *Physical Uplink Shared Channel (PUSCH)*.
  5. eNode B completes data transfer by sending ACK/NAK on *Physical Hybrid ARQ Indicator Channel (PHICH)*.

REFERENCES

[1] *The mobile economy 2017*, Online. Available: *https://www.gsmaintelligence.com/*, GSMA Intelligence, 2017.

[2] *GSA: Evolution to LTE report - january 2017*, Online. Available: *http://gsacom.com/*, The Global Mobile Suppliers Association (GSA), 2017.

[3] *Technical specifications; LTE (Evolved UTRA) and LTE-Advanced radio technology series (Rel 14)*, Online. Available: *http://www.3gpp.org/ftp/Specs/latest/Rel-14/*, The 3rd Generation Partnership Project (3GPP), 2017.

[4] S. Sesia, I. Toufik, and M. Baker, Eds., *LTE - the UMTS long term evolution: From theory to practice*, second. West Sussex, UK: Wiley, 2011.

[5] J. H. Reed, *Comments of Wireless @ Virginia Tech in the matter of NTIA development of the nationwide interoperable public safety broadband network*, Wireless @ Virginia Tech, Blacksburg, VA, 2012.

[6] M. Lichtman, J. Reed, T. Clancy, and M. Norton, “Vulnerability of LTE to hostile interference,” in *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, 2013, pp. 285–288.

[7] R. P. Jover, J. Lackey, and A. Raghavan, “Enhancing the security of LTE networks against jamming attacks,” *EURASIP Journal on Information Security*, vol. 2014, no. 7, pp. 1–14, 2014.

[8] F. Aziz, J. Shamma, and G. Stüber, “Resilience of LTE networks against smart jamming attacks,” in *Global Communications Conference (GLOBECOM), 2014 IEEE*, 2014, pp. 734–739.

[9] C. Shahriar, M. La Pan, M. Lichtman, T. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. Reed, “PHY-layer resiliency in OFDM communications: A tutorial,” *Communications Surveys Tutorials, IEEE*, vol. 17, no. 1, pp. 292–314, 2015.

[10] F. Aziz, J. Shamma, and G. Stüber, “Resilience of LTE networks against smart jamming attacks: Wideband model,” in *Personal, Indoor, and Mobile Radio Communication (PIMRC), 2015 IEEE 26th Annual International Symposium on*, 2015, pp. 1534–1538.

[11] 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 Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[12] F. Aziz, J. Shamma, and G. Stüber, "Jammer type estimation in LTE with a smart jammer repeated game," *Vehicular Technology, IEEE Transactions on*, 2017, IEEE early access article.

[13] R. Blom, P. de Bruin, J. Eman, M. Folke, H. Hannu, M. N`aslund, M. Stålnacke, and P. Synnergren, "Public safety communication using commercial cellular technology," in *Next Generation Mobile Applications, Services and Technologies (NGMAST), 2008 The Second International Conference on*, 2008, pp. 291–296.

[14] M. Simić, "Feasibility of Long Term Evolution (LTE) as technology for public safety," in *Telecommunications Forum (TELFOR), 2012 20th*, 2012, pp. 158–161.

[15] T. Doumi, M. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, "LTE for public safety networks," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 106–112, 2013.

[16] A. Paulson and T. Schwengler, "A review of public safety communications, from LMR to voice over LTE (VoLTE)," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, 2013, pp. 3513–3517.

[17] R. Ferrús, O. Sallent, G. Baldini, and L. Goratti, "LTE: The technology driver for future public safety communications," *Communications Magazine, IEEE*, vol. 51, no. 10, pp. 154–161, 2013.

[18] R. Ferrús and O. Sallent, "Extending the LTE/LTE-A business case: Mission- and business-critical mobile broadband communications," *Vehicular Technology Magazine, IEEE*, vol. 9, no. 3, pp. 47–55, 2014.

[19] C. Hochgraf, R. Tripathi, and S. Herzberg, "Smart grid charger for electric vehicles using existing cellular networks and SMS text messages," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 167–172.

[20] P. Parikh, M. Kanabar, and T. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, pp. 1–7.

[21] Q. Zou and L. Qin, "Integrated communications in smart distribution grid," in *Power System Technology (POWERCON), 2010 International Conference on*, 2010, pp. 1–6.

[22] Z. Feng, L. Jianming, H. dan, and Z. Yuexia, “Study on the application of advanced broadband wireless mobile communication technology in smart grid,” in *Power System Technology (POWERCON), 2010 International Conference on*, 2010, pp. 1–6.

[23] M. Ibrahim and M. Salama, “Smart distribution system volt/VAR control using distributed intelligence and wireless communication,” *Generation, Transmission Distribution, IET*, vol. 9, no. 4, pp. 307–318, 2015.

[24] E. Thompson. (2012). Army examines feasibility of integrating 4G LTE with tactical network. Online. Available: *http://www.army.mil/article/87875/*, US Army RDECOM CERDEC Public Affairs.

[25] G. Crowe. (2013). Navy’s ship-to-ship communications go 4G. Online. Available: *https://gcn.com/*, GCN Magazine.

[26] K. Jain. (2015). These top 7 brutal cyber attacks prove ‘no one is immune to hacking’. Online. Available: *http://thehackernews.com/2015/09/top-cyber-attacks-1.html*, The Hacker News.

[27] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: A tutorial,” *Wireless Communications, IEEE*, vol. 18, no. 2, pp. 66–74, 2011.

[28] C. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal, The*, vol. 28, no. 4, pp. 656–715, 1949.

[29] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

[30] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless information-theoretic security,” *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515 –2534, 2008.

[31] W. Trappe, “The challenges facing physical layer security,” *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 16–20, 2015.

[32] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, ACM, 2005, pp. 46–57.

[33] Z. Lu, X. Lu, W. Wang, and C. Wang, “Review and evaluation of security threats on the communication networks in the smart grid,” in *Military Communications Conference (MILCOM), 2010 IEEE*, 2010, pp. 1830–1835.

[34] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A survey on security aspects for LTE and LTE-A networks,” *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 283–302, 2014.

[35] Y. Park and T. Park, “A survey of security threats on 4G networks,” in *Globecom Workshops, 2007 IEEE*, 2007, pp. 1–6.

[36] C. Patel, G. Stüber, and T. Pratt, “Analysis of OFDM/MC-CDMA under channel estimation and jamming,” in *Wireless Communications and Networking Conference (WCNC), 2004 IEEE*, vol. 2, 2004, 954–958 Vol.2.

[37] T. Clancy, “Efficient OFDM denial: Pilot jamming and pilot nulling,” in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1–5.

[38] C. Mueller-Smith and W. Trappe, “Efficient OFDM denial in the absence of channel information,” in *Military Communications Conference (MILCOM), 2013 IEEE*, 2013, pp. 89–94.

[39] M. J. Husso, “Performance analysis of a WiMAX system under jamming,” Master’s thesis, Department of ELectrical and Communications Engineering, Helsinki University of Technology, 2006.

[40] M. Petracca, M. Vari, F. Vatalaro, and G. Lubello, “Performance evaluation of GSM robustness against smart jamming attacks,” in *Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on*, 2012, pp. 1–6.

[41] A. Hussain, N. Saqib, U. Qamar, M. Zia, and H. Mahmood, “Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks,” *Communications and Networks, Journal of*, vol. 16, no. 4, pp. 397–406, 2014.

[42] J. Andrews, W. Choi, and R. Heath, “Overcoming interference in spatial multiplexing MIMO cellular networks,” *Wireless Communications, IEEE*, vol. 14, no. 6, pp. 95–104, 2007.

[43] K. Yang, “Interference management in LTE wireless networks [industry perspectives],” *Wireless Communications, IEEE*, vol. 19, no. 3, pp. 8–9, 2012.

[44] H. Burchardt and H. Haas, “Multicell cooperation: Evolution of coordination and cooperation in large-scale networks,” *Wireless Communications, IEEE*, vol. 20, no. 1, pp. 19–26, 2013.

[45] B. Soret, H. Wang, K. Pedersen, and C. Rosa, “Multicell cooperation for LTE-Advanced heterogeneous network scenarios,” *Wireless Communications, IEEE*, vol. 20, no. 1, pp. 27–34, 2013.

[46] O. El Ayach, S. Peters, and J. Heath R.W., “The practical challenges of interference alignment,” *Wireless Communications, IEEE*, vol. 20, no. 1, pp. 35–42, 2013.

[47] Y. Chen, F. He, J. Yan, X. Chen, and Y. Gu, “A smart tracking-based jamming scheme for signals with periodic synchronization sequences,” in *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, 2011, pp. 1–5.

[48] S. Zorn, M. Gardill, R. Rose, A. Goetz, R. Weigel, and A. Koelpin, “A smart jamming system for UMTS/WCDMA cellular phone networks for search and rescue applications,” in *Microwave Symposium Digest (MTT), 2012 IEEE MTT-S International*, 2012, pp. 1–3.

[49] W. Shen, P. Ning, X. He, and H. Dai, “Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time,” in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 174–188.

[50] A. Yener and S. Ulukus, “Wireless physical-layer security: Lessons learned from information theory,” *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[51] A. Asterjadhi, R. Kumar, T. La Porta, and M. Zorzi, “Broadcasting in multi channel wireless networks in the presence of adversaries,” in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on*, 2011, pp. 377–385.

[52] M. Strasser, C. Pöpper, S. Čapkun, and M. Čagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, 2008, pp. 64–78.

[53] L. Qing, L. Fen, and Z. Yangshi, “An enhanced anti-jamming capability method for frequency hopping synchronization system,” in *Intelligent Information Technology Application Workshops, 2008 (IITAW ’08). International Symposium on*, 2008, pp. 236–238.

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

[55] X.-Y. Meng, R. Tao, and L.-N. Jia, “An intelligent anti-jamming frequency hopping system,” in *Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on*, 2010, pp. 1053–1056.

[56] D. Thuente and M. Acharya, “Intelligent jamming in wireless networks with applications to 802.11b and other networks,” in *Proc. 25th IEEE Communications So-*

ciety Military Communications Conference (MILCOM06), Washington, DC, 2006, pp. 1–7.

[57] B. Lo and I. Akyildiz, "Multiagent jamming-resilient control channel game for cognitive radio ad hoc networks," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 1821–1826.

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

[59] T. Clancy, M. Norton, and M. Lichtman, "Security challenges with LTE-Advanced systems and military spectrum," in *Military Communications Conference (MILCOM), 2013 IEEE*, 2013, pp. 375–381.

[60] D. Fudenberg and J. Tirole, *Game theory*. Cambridge, Massachusetts: MIT press, 1991.

[61] R. J. Aumann and S. Hart, Eds., *Handbook of game theory with economic applications*. Amsterdam, The Netherlands: North Holland, 1992, vol. 1.

[62] M. J. Osborne and A. Rubinstein, *A course in game theory*. Cambridge, Massachusetts: MIT press, 1994.

[63] R. J. Aumann, M. Maschler, and R. E. Stearns, *Repeated games with incomplete information*. Cambridge, Massachusetts: The MIT press, 1995.

[64] S. Sorin, *A first course on zero-sum repeated games*. Berlin Heidelberg: Springer-Verlag, 2002.

[65] H. P. Young and S. Zamir, Eds., *Handbook of game theory with economic applications*. Amsterdam, The Netherlands: North Holland, 2014, vol. 4.

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

[67] A. B. MacKenzie and L. A. DaSilva, *Game theory for wireless engineers*. San Rafael, California: Morgan & Claypool Publishers, 2006.

[68] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: A tutorial," Tech. Rep., 2006.

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

[70] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungnes, *Game theory in wireless and communication networks: Theory, models, and applications*. New York, New York: Cambridge University Press, 2012.

[71] M. Jones and J. Shamma, “Policy improvement for repeated zero-sum games with asymmetric information,” in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, 2012, pp. 7752–7757.

[72] L. Li and J. Shamma, “Lp formulation of asymmetric zero-sum stochastic games,” in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, IEEE, 2014, pp. 1930–1935.

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

[74] L. Li, E. Feron, and J. S. Shamma, “Finite stage asymmetric repeated games: Both players’ viewpoints,” in *Decision and Control (CDC), 2016 IEEE 55th Conference on*, IEEE, 2016, pp. 5310–5315.

[75] V. S. Kamble, “Games with vector payoffs: A dynamic programming approach,” PhD thesis, University of California, Berkeley, 2015.

[76] X. He, H. Dai, P. Ning, and R. Dutta, “Dynamic ids configuration in the presence of intruder type uncertainty,” in *Global Communications Conference (GLOBECOM), 2015 IEEE*, IEEE, 2015, pp. 1–6.

[77] H. Von Stackelberg, *The theory of the market economy*. Oxford University Press, 1952.

[78] M. Bloem, T. Alpcan, and T. Başar, “A Stackelberg game for power control and channel allocation in cognitive radio networks,” in *Proceedings of the 2nd international conference on Performance evaluation methodologies and tools*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2007.

[79] S. Guruacharya, D. Niyato, E. Hossain, and D. I. Kim, “Hierarchical competition in femtocell-based cellular networks,” in *Global Telecommunications Conference (GLOBECOM), 2010 IEEE*, 2010, pp. 1–5.

[80] V. Conitzer and T. Sandholm, “Computing the optimal strategy to commit to,” in *Proceedings of the 7th ACM conference on Electronic commerce*, ACM, 2006, pp. 82–90.

[81] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, “Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness.,” *J. Artif. Intell. Res.(JAIR)*, vol. 41, pp. 297–327, 2011.

[82] Y. Vorobeychik and S. Singh, “Computing Stackelberg equilibria in discounted stochastic games (corrected version),” 2013.

[83] Y. Vorobeychik, B. An, M. Tambe, and S. Singh, “Computing solutions in infinite-horizon discounted adversarial patrolling games,” in *Proc. 24th International Conference on Automated Planning and Scheduling (ICAPS 2014)(June 2014)*, 2014.

[84] H. Xu, Z. Rabinovich, S. Dughmi, and M. Tambe, “Exploring information asymmetry in two-stage security games,” in *AAAI Conference on Artificial Intelligence (AAAI)*, 2015.

[85] M.-F. Balcan, A. Blum, N. Haghtalab, and A. D. Procaccia, “Commitment without regrets: Online learning in Stackelberg security games,” in *16th ACM Conference on Economics and Computation (EC’15)*, ACM, 2015.

[86] J. Zheng and D. Castanon, “Stochastic dynamic network interdiction games,” in *American Control Conference (ACC), 2012*, 2012, pp. 1838–1844.

[87] ——, “Dynamic network interdiction games with imperfect information and deception,” in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, 2012, pp. 7758–7763.

[88] B. De Meyer, “Repeated games and partial differential equations,” *Mathematics of Operations Research*, vol. 21, no. 1, pp. 209–236, 1996.

[89] L. Li and J. Shamma, “Efficient strategy computation in zero-sum asymmetric repeated games,” submitted for publication in IEEE Transactions on Automatic Control, *arXiv preprint arXiv:1703.01952*, 2017.

[90] A. Garnaev, M. Baykal-Gürsoy, and H. Poor, “Incorporating attack-type uncertainty into network protection,” *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 8, pp. 1278–1287, 2014.

[91] A. Garnaev and W. Trappe, “Optimal scanning bandwidth strategy incorporating uncertainty about adversary’s characteristics,” *arXiv preprint arXiv:1502.04676*, 2015.

[92] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, “Security games with unknown adversarial strategies,” *IEEE transactions on cybernetics*, vol. 46, no. 10, pp. 2291–2299, 2016.

[93] A. Garnaev and W. Trappe, "A bandwidth monitoring strategy under uncertainty of the adversarys activity," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 837–849, 2016.

[94] 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.

[95] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[96] M. Tambe, *Security and game theory: Algorithms, deployed systems, lessons learned*. Cambridge University Press, 2011.

[97] J. Marecki, G. Tesauro, and R. Segal, "Playing repeated Stackelberg games with unknown opponents," in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, International Foundation for Autonomous Agents and Multiagent Systems, 2012, pp. 821–828.

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

[99] 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," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, 2015.

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

[101] A. Goldsmith, *Wireless communications*. New York, New York: Cambridge University Press, 2005.

[102] H. Arslan and S. Reddy, "Noise power and SNR estimation for OFDM based wireless communication systems," in *Proc. of 3rd IASTED International Conference on Wireless and Optical Communications (WOC), Banff, Alberta, Canada*, 2003.

[103] J. G. Proakis, *Digital communications*, fourth. New York, New York: McGraw-Hill, 2000.

[104] P. Viswanath, D. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1277–1294, 2002.

[105] R. V. Hogg, J. McKean, and A. T. Craig, *Introduction to mathematical statistics.* seventh. Essex, UK: Pearson, 2012.

[106] F. Aziz, L. Li, J. Shamma, and G. Stüber, "Player's strategies in LTE vs. smart jammer infinite-horizon asymmetric repeated game," *Wireless Communications, IEEE Transactions on*, 2017, submitted for publication.

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

[108] J.-P. Ponssard and S. Sorin, "The LP formulation of finite zero-sum games with incomplete information," *International Journal of Game Theory*, vol. 9, no. 2, pp. 99–105, 1980.

VITA

Farhan M. Aziz was born and raised in one of the largest and most vibrant cities of the world - Karachi, Pakistan. He is currently 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; modeling the network and the *smart jammer* dynamics under realistic constraints; and devising autonomous algorithms to combat *smart jamming* attacks. 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) and Automatic Link Establishment (ALE) algorithms and techniques for military and national interest radios; and writing project proposals for utilizing DSA/ALE technology for communication in various tactical and strategic scenarios providing spectrum agility and link range extension. Aziz received a Bachelor of Engineering (B.E.) degree in Electrical Engineering from the NED University of Engineering & Technology, Karachi, Pakistan in 1999, where he secured second merit position. He also received 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 and during Summer of 2013, 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, dealing with the 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.