CELL ASSOCIATION ATTACK VIA REFERENCE SIGNAL SPOOFING IN MULTI-CELL WIRELESS NETWORKS

A Dissertation by

Shuang Feng

Master of Science, Wichita State University, 2010

Bachelor of Engineering, Southwest University of Science and Technology, China, 2007

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

July 2016

CELL ASSOCIATION ATTACK VIA REFERENCE SIGNAL SPOOFING IN MULTI-CELL WIRELESS NETWORKS

The following faculty members have examined the final copy of this dissertation for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Doctor of Philosophy with a major in Electrical Engineering.

_____
Hyuck M. Kwon, Committee Chair

_____
John Watkins, Committee Member

_____
Preethika Kumar, Committee Member

_____
M. Edwin Sawan, Committee Member

_____
Xiaomi Hu, Committee Member

Accepted for the College of Engineering

_____
Janet Twomey, Associated Dean

Accepted for the Graduate School

_____
Dennis Livesay, Dean

DEDICATION

To my parents and friends

ACKNOWLEDGEMENTS

I would like to express my greatest gratitude to my adviser, Dr. Hyuck M. Kwon, for his many years of thoughtful encouragement and patient guidance. His valuable teaching and inspiration led me to explore the field of wireless communications. Influences from his research attitude, study method, and perseverance will continuously benefit my future career. I also express gratitude to my dissertation committee members, Dr. John Watkins, Dr. M. Edwin Sawan, Dr. Preethika Kumar, and Dr. Xiaomi Hu, whom I thank for their valuable suggestions and instruction.

In addition, I acknowledge my former colleague and friend, Amitav Mukherjee, for his help and suggestions. I also thank my colleagues—YuvArchi Sagar, Jie Yang, Shane Michael Hodges, Kanghee Lee, Hyunggi Kim, Chandana Jayasooriya, Kenny Wong—who provided me with an outstanding academic environment in the wireless commuication laboratory at Wichita State University.

Last, special gratitude goes to my parents for their endless support and unlimited love.

This work was supported in part by the Air Force Summer Faculty Fellowship Program, the Air Force Research Laboratory (AFRL) under Grant FA9453-15-1-0308 and Grant FA9453-16-1-0049. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the AFRL or the U.S. Government.

ABSTRACT

The research in this dissertation involved investigating a novel physical-layer security problem wherein malicious base stations (MBSs) mislead mobile terminals (MTs) into being prematurely handed over to suboptimal target cells, resulting in radio link failure (RLF). The MBSs achieve this by spoofing the common reference signals of legitimate base stations (LBSs), which are used by MTs to measure signal strengths.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
BS	Base Station
CA	Cell Association
CDF	Cumulative Distribution Function
CR	Cognitive Radio
CRS	Cell-Specific Reference Signals
EPS	Evolved Packet System
ERD	Energy Ratio Detector
3GPP	Third-Generation Partnership Project
HCN	Heterogeneous Cellular Network
HetNet	Heterogonous Network
HO	Handover
LBS	Legitimate Base Station
LocDef	Localization-Based Defense
LTE	Long-Term Evolution
MACA	Mobile Assisted Connection Admission
MBS	Malicious Base Station
MS	Mobile Station
MT	Mobile Terminal
PDF	Probability Density Function
PPP	Poisson Point Process
PUE	Primary User Emulation

RLF	Radio Link Failure
SINR	Signal-to-Interference-plus-Noise Ratio
SIR	Signal-to-Interference Ratio

LIST OF SYMBOLS

$\|a\|$	2-Norm of a
$E[\cdot]$	Expectation Operator
I_N	N × N Identity Matrix
$\log_a$	Logarithm of Base a
$\|a\|$	Absolute Value of a
$\mathcal{L}\{f\}(s)$	Laplace Transformation
$M_x(t)$	Moment-Generating Function
$G_\Theta(f)$	Probability-Generating Function
θ	Radio Link Failure Threshold
$\lambda(x)$	Intensity Function
μ	Mean Value
β	Cell Association Threshold
α	Pass Loss
σ^2	Noise Power

CHAPTER 1

INTRODUCTION

This chapter introduces the research background of this dissertation. Section 1.1 briefly describes the literature study, and Section 1.2 explains the research objective of this dissertation.

1.1 Literature Review

In cellular networks, cell association (CA) is an important procedure during which mobile terminals (MTs) establish an initial connection to the network. Well-designed CA mechanisms ensure that MTs connect to those base stations that offer the best signal strength or signal quality [1]. Therefore, the CA procedure is an appealing target for malicious attackers seeking to disrupt network performance. One important aspect in CA is authentication of whether a legitimate user is requesting connection to a legitimate base station (LBS). In current cellular networks such as Third-Generation Partnership Project (3GPP) Long-Term Evolution (LTE), the security of the association and handover (HO) process is based on higher-layer key-based cryptographic techniques [2], [3].

Ye et al. [1] presented a load-aware CA method and distributed algorithm for downlink heterogonous networks (HetNets). First, the authors undertook an optimization theoretic approach to the load-balancing problem, where they considered CA and resource allocation jointly. They decoupled the joint general utility maximization problem by assuming (optimistically) that users can be associated with more than one base station (BS). This approach provides an upper bound on the achievable network utility and can serve as a benchmark. However, in a real system, it is much more difficult to implement multi-BS associations than a single-BS association. Therefore, they formulated a logarithmic utility maximization problem for a single-BS association and showed that equal resource allocation is actually optimal over a

sufficiently large time window. This observation allows the coupled problem in a single-BS association to reduce to a cell-association problem with an equal resource allocation, which along with the fractional association assumption converts the previously intractable combinatorial problem into a convex optimization problem. Next, they exploited the convexity of the problem to develop a distributed algorithm via dual decomposition that converges towards the optimal solution with a guarantee on the maximum gap from optimality. This provides a feasible, efficient, and low-overhead algorithm for implementation in HetNets. Finally, they leveraged their provable optimal solutions to ask a basic question: How much of the performance gain can a simple policy based on a priori bias factors achieve? Their results show that this simple approach gets surprisingly close to the gains of the load-aware utility maximization. The gains from this approach are shown to be very large for most users in the system, ranging from 2 to 3.5x for the bottom half of users. To put this in context, this is a gain on par with what would otherwise be achieved by a doubling or tripling of the amount of spectrum for a given service provider. Cell interior users experience little to no rate gain (or a small loss), but this has little relevance in practice since such users are already well-served.

In the work of Cao et al. [2], the authors presented a comprehensive survey of security aspects in LTE/LTE-A networks. Their efforts and contributions made in this work include the following: (1) an overview of the security architectures and functionalities in the LTE/LTE-A networks, (2) an analysis of the security issues and vulnerabilities in the LTE networks and the security aspects of the new features introduced in the LTE-A networks, (3) a discussion of existing solutions to overcome these vulnerabilities, and (4) an exploration of the potential areas and research directions for future research work.

For the research of Han and Choi [3], first of all, the authors identified flaws in the handover key management of the evolved packet system (EPS) security mechanism; second, they designed a promising mathematical model for the EPS handover key management to measure the effect of a compromised key; and last, they investigated the performance criteria (e.g., user mobility, network topology, and so on) involved in selecting an optimal operational point for key updating. Extensive simulation results validated the analytical model and revealed how the optimal key update interval changes in practice.

Dhillon et al. [4] developed a tractable, flexible, and accurate model for a downlink heterogeneous cellular network consisting of K tiers of randomly located BSs, where each tier may differ in terms of average transmit power, supported data rate, and BS density. They also derived an expression for the probability of coverage (equivalently outage) over the entire network under both open and closed access, which assumes a strikingly simple closed-form in the high signal-to-interference-plus-noise ratio (SINR) regime and is accurate down to −4 dB, even under weaker assumptions

Damnjanovic et al. [5] discussed the need for an alternative strategy, where low-power nodes are overlaid within a macro network, creating what is referred to as a heterogeneous network. They surveyed the current state of the art in heterogeneous deployments and focused on a 3GPP LTE air interface to describe future trends. A high-level overview of the 3GPP LTE air interface, network nodes, and spectrum allocation options is provided, along with the enabling mechanisms for heterogeneous deployments.

Kahwa and Georganas [6] considered the problem of channel assignment in mobile communication systems, where the service area is divided into hexagonal cells. In particular, a

hybrid channel assignment scheme is studied, and certain results are obtained using a general purpose simulation scheme to model a 40-cell system.

Eklundh [7] investigated a directed retry facility, which enables subscribers in a mobile telephone system to look for free radio channels in more than one cell, with respect to blocking probability and channel utilization. Analytical results were compared with simulations and good agreement was. Results showed that a substantial improvement, compared with systems without a directed retry facility, can be achieved as far as carried traffic is concerned. The improvement is accomplished at the expense of those subscribers who cannot make use of the directed retry facility due to variations in radio coverage.

Wu et al. [8] proposed a new channel-allocation scheme, or mobile-assisted connection admission (MACA), in which special channels are deployed among cells to achieve load balancing. They examined the performance of MACA with a two-cell analytical model and a 7 x 7-cell simulation model, and found that the performance can greatly improve, in some cases comparable to dynamic channel allocation. Sang et al. [9] proposed an opportunistic downlink scheduling algorithm, called the weighted alpha rule, to provide high aggregate throughput and tunable resource fairness among users within each cell. To leverage the asymmetric traffic loading across the whole system, they proposed a medium access control layer "cell breathing" to coordinate the scheduling or the coverage of mobile stations (MSs) in neighboring cells. They also proposed a load-aware handoff and cell-site selection scheme for individual MSs to proactively avoid hot-spots and locate a good service sites.

Corroy et al. [10] proposed a new theoretical framework enabling one to analyze dynamic cell association in a multi-cell HetNet and derive an upper bound on the achievable downlink sum rate using convex optimization. They proposed a heuristic with a low complexity coming

close to the upper bound. They validated their theoretical results for a simple setup through numerical evaluations and implement their heuristic in an LTE simulator to analyze its behavior in a more realistic system.

Jo et al. [11] presented a novel analytical model and set of results for an SINR in downlink heterogeneous cellular networks (HCNs) with flexible cell association. They derived a pair of prerequisite quantities that are of interest in their own right. They derived the complete outage probability over all SINRs with arbitrary biasing. They also derived two measures of spectral efficiency in their proposed HCN model: the average ergodic rate of a randomly chosen user in the whole network (or a certain tier), and the minimum average user throughput—the smallest value among the average user throughputs supported by one cell in each tier.

However, this dissertation is the first research work on the following: (a) radio link failure (RLF) probability with malicious base stations (MBSs) attacked; (b) CA probability with MBSs attacked, and (c) conditional RLF probability given a false CA condition.

This dissertation proposes and analyzes a novel physical-layer security attack on CA process. Namely, it considers a set of MBSs that mislead MTs into being associated with suboptimal target cells, resulting in RLF. This is achieved by emulating or spoofing reference signals of the LBSs that are used by nodes to estimate signal strengths. For example, in the LTE standard, an LBS periodically broadcasts cell-specific reference signals (CRSs) on certain frequency tones for this purpose. In the scenario here, the MBSs emulate these CRSs, for example. Disrupting the association process severely degrades the MT quality of service and leads to service interruptions because it is necessary to reestablish connection to the network. Physical-layer security problems are generally related to eavesdropping or jamming adversaries [12], whereas the research here studies the impact of physical-layer attacks on the critical CA

procedure. The spoofing of reference signals from a physical-layer secrecy perspective and detection of such attacks have been investigated [13], [14]. Spoofing or emulation of primary-user waveforms has also been investigated in the context of cognitive radio (CR) networks [15], [16], where the objective of the attackers is to deny spectrum access to secondary users.

In the work of Zhou et al. [13], the authors showed the detrimental effect of the pilot contamination attack on the secrecy performance. Therefore, it is important for the legitimate user to detect such an attack and design countermeasures. The detection of the pilot contamination attack may be achieved by transmitting a sufficiently long pilot sequence in the reverse training phase and analyzing the variance of the received signal at Alice after normalizing it by the pilot sequence. If the variance is close to that of the receiver noise, then it indicates that the pilot contamination attack may have been used by Eve. In order to make this attack ineffective, blind channel estimation can be used by Alice based on the data transmission from Bob, assuming two-way communications.

In the research of Xiong et al. [6], the main contributions of the method are summarized as follows: (1) the enfergy ratio detector (ERD) does not require drastic changes on either the design of pilot signals or the channel estimation phase structure. The main justification is using a certain short period of the downlink data phase to calculate the power of received signal and detect the existence of the attack; (2) they derived the closed-form expression of the test statistic's probability density function (PDF) and found that the detection threshold of the ERD does not depend on either the legitimate or illegitimate channel condition. This is a significant advantage because it suggests the ERD could work under all possible channel realizations. Numerical results show that the ERD could detect the pilot spoofing attack with very high probability; and (3) large power utilization by Eve could increase the gain to the eavesdropper

but also considerably increase the risk of Eve being detected by the legitimate system. Therefore, the trade-off brought by the power consumption of Eve is studied. Results show that their ERD could efficiently reduce the ergodic information leakage, which is the largest information rate that Eve could possibly obtain by choosing the optimal power budget, to a trivial level.

The main contribution of the research of Chen et al. [15] is twofold. First, they identified a security issue that poses a serious threat to CR networks. The existing body of research on CR network security is very small. The work presented in this paper contributes to this body of research. Second, they proposed a localization-based defense (LocDef) as a transmitter verification scheme capable of detecting primary user emulation (PUE) attacks and pinpointing PUE attackers. As the core component of LocDef, the proposed non-interactive localization scheme can be employed in hostile environments. LocDef can be integrated into existing spectrum sensing schemes to enhance the trustworthiness of the sensing decisions.

Peng et al. [16] analyzed two attacks on a cognitive radio network: spoofing and jamming. For an intelligent adversary with an energy constraint, a joint optimization problem considering both spoofing and jamming was formulated by minimizing the average sum throughput of the secondary users. Numerical results showed that the optimal attack for an intelligent adversary is a combination of spoofing and jamming. Furthermore, they numerically analyzed how the spoofing and jamming capabilities vary with different system parameters. Specifically, in their CR system, as either the number of spectral vacancies required by secondary users increases, or the value of integration-time-bandwidth product at the energy-detection receiver at the energy detector of the secondary increases, the optimal attack for the intelligent adversary transitions from jamming to spoofing.

1.2 Research Objective

A Poisson point process (PPP) probability distribution to model the stochastic geometry of LBSs and MBSs with the origin as the target MT location [17] has been assumed. Figure 1.1 shows an example realization of the spatial locations of the LBSs and MBSs. The target MT is in the center of a 250-meter circle. The squares and small circles represent base stations (BSs) from Tier 1. The crosses and triangles represent BSs from Tier 2.

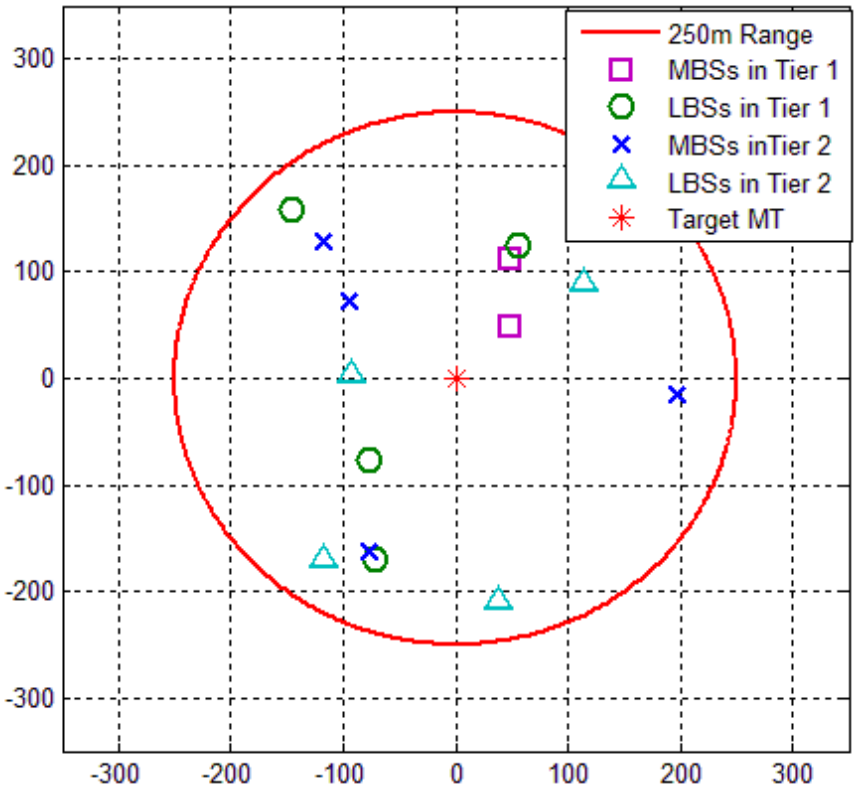

Figure 1.1. Example scenario of stochastic geometry of considered LBSs and MBSs.

This research considers T = 2 independent tiers of LBSs and MBSs with independent spatial densities. The number of tiers means the number of different kinds of heterogeneous networks. Each network tier can consist of multiple nodes. Then it analytically derives the conditional probability of the RLF given a CA triggered by an MBS using either a signal-to-interference-plus-noise ratio or a signal-to-interference ratio (SIR), and verifies the theoretical

results using simulations. The PPP MATLAB simulation has typically been difficult, especially when intensity is low, e.g., $\lambda = 1/(250^2\pi)$, i.e., one LBS on average within a cell area with a 250-meter radius, which is practical but requires a very large number of trials when the unit is a square meter. This is because with high probability, almost no BS is available within a cell area with a 250-meter radius. Therefore, this research uses a scale such as the 250-meter radius times the number of PPP outcomes for $\lambda = 1/(250^2\pi)$ (i.e., number of Poisson points generated within the unit area of a square meter). Later on in the results section, Table 4.1 presents a successful simulation method that produces results very close to the analytical. Finally, this research discusses the appropriate threshold with which an MT requests CA with the connected LBS and another appropriate threshold with which the LBS claims an RLF.

This dissertation is organized as follows: Chapter 2 introduces the mathematical model and the necessary probability definitions. Chapter 3 presents probability expressions for CA, unconditional RLF, and conditional RLF given CA. Chapter 4 demonstrates both the analyzed and simulation results and discussions, and Chapter 5 offers conclusions. The appendices show detailed proofs for Theorems 1 to 5.

Notation: This dissertation denotes the boldface lower case letter as a vector; $CN(0,\sigma^2)$ is a complex Gaussian random variable with zero mean and σ^2 variance; $\|x\|_p$ is L^p-norm, $p>1$, i.e., $\boldsymbol{x} = (x_1,...,x_n) \in \mathbb{R}^{2n}, \|\boldsymbol{x}\|_p = (\sum_{i=1}^{n} |x_i|^p)^{1/p}$; x_i denotes the two-dimensional location of the ith node; and $h_i \in CN(0,1)$ denotes a complex fading coefficient random variable from the ith node to the origin.

1.3 Main Contributions

The contributions and significance of this dissertation are summarized as follows:

- The unconditional RLF probability using an SIR metric at the connected LBS is presented in Theorem 1. This probability equation is an integration expression, which shows what the RLF probability occurs when RLF is defined by the SIR metric with the following parameters: RLF threshold θ, path loss α, and number of BSs n. The number of BSs is related to the number of integral folds.
- The unconditional RLF probability using an SINR metric at the connected LBS is presented in Theorem 2. This probability equation is an integration expression, which shows that what the RLF probability is when RLF is defined by the SINR metric with the following parameters: RLF threshold θ, path loss α, number of BSs n, and noise power σ. Again, the number of BSs is related to the number of integral folds.
- The CA probability using the total received power metric including MBSs at the connected LBS is presented in Theorem 3. This probability equation is an integration expression, which shows what the CA probability is when CA is defined by total power metric with the following parameters: CA threshold β, path loss α, and number of BSs n. Again, the number of BSs is related to the number of integral folds.
- The CA probability using the aggregated SINR at the connected LBS including MBSs is presented in Theorem 4. This probability equation is an integration expression, which shows what the CA probability is when CA is defined by the SINR metric, for given CA threshold β, path loss α, number of BSs n, and noise power σ. Again, the number of BSs is related to the number of integral folds.

- The conditional RLF probability given CA triggered by one MBS is presented in Theorem 5. For the RLF and CA probabilities, the SINR metric excluding the MBS and the aggregated received power metric including the MBS, respectively, are used. This probability equation is an integration expression with four parameters: CA threshold β, RLF threshold θ, path loss α, and noise power σ. It shows the conditional RLF probability for a given condition of CA. This is a special case when the number of BSs equals two. That is to say, there is one LBS and one MBS.
- This dissertation also finds that, when either SINR or SIR metrics are used, the analyzed RLF and CA probabilities only depend on the thresholds, path loss, and the number BSs. Other parameters do not affect the results because of cancellations in the ratios.
- Finally, this dissertation presents what would be appropriate ranges of thresholds for CA and RLF using the conditional RLF probability given CA triggered by MBS attacks.

CHAPTER 2

MATHEMATICAL MODEL

2.1 Introduction

In this work, a cellular network composed of two tiers of base stations on a two-dimensional Euclidean plane is considered. In the *T*th tier, the BSs are spatially distributed according to a PPP Φ_T with intensity λ_T . The LBS and MBS transmit powers are P_1 and P_2, respectively. The MBS transmits on the same carrier frequency as the LBS network. Here, the focus is on a target mobile terminal located at the origin (0, 0) for the performance analysis, as is common in stochastic geometry literature [12], [13], [18], and [19].

In 3GPP LTE, BSs transmit cell-specific reference signals that allow neighboring users to measure their strength and quality (e.g., SINR). After scanning different frequencies and cell signals, users entering the network or transitioning out of the idle mode then associate with the BS that potentially offers the best signal quality by sending a connection request to them. MBSs attack this process by synchronizing in time with the LBSs, and then secretly emulating the cell identification and CRS patterns of the LBSs such that MTs perceive a higher LBS signal strength than actually exists. CAs can only be performed with other LBSs and not with MBSs, since MBSs will not pass the authentication phase, i.e., man-in-the-middle attacks are not considered here. Once CA with the target LBS is initiated due to the MBSs, there is an increased probability of radio link failure since the true signal quality may be worse than the minimum operating requirement.

2.2 Mathematical Model

Consider the target MT at the origin, which scans the signals received from adjacent BSs. In this dissertation, subindex 1 is used to indicate the LBS, subindex 2 for the first MBS,

subindex 3 for the second MBS, and so on. Those MBSs are cooperative with each other in terms of spoofing the same LBS signals [20]. Let $D \subset \bigcup_i \Theta_i$ denote the locations of the LBS and MBS set sending the same reference signal to the target MT. When under attack by MBSs that are spoofing the CRS of a particular LBS, the received signal at the MT can be written as

$$r = \sum_{x_i \in D} \frac{\sqrt{P_i}}{\|x_i\|^{\alpha/2}} h_i X + \sum_{x_i \in D^c} \frac{\sqrt{P_i}}{\|x_i\|^{\alpha/2}} h_i Z_i + n \tag{2.1}$$

where $x_i \in D$ represents the LBS and MBS locations, $\|x_i\|^{1/2}$ is the corresponding distance from the *i*th node to the origin, $h_i \in CN(0,1)$ is the corresponding random fading coefficient, $\alpha > 2$ is the path-loss exponent, X is a cell-specific reference signal sent by the LBS and spoofed by the MBSs, $D^c = \bigcup_{i=1,2} \Theta_i \setminus D$ is the set of interfering BSs sending different references or data signals Z_i in two different tiers, $i = 1,2, n \sim CN(0,\sigma^2)$ is an additive circular symmetric complex Gaussian noise, and the transmit signals X and Z_i are assumed to be independent, zero-mean random variables of unit variance. All channel coefficients and signals are assumed to be mutually independent.

The deceptive received signal power at the MT, including LBS and all spoofing MBSs signals, is

$$\hat{P}_r = \left| \sum_{x_i \in D} \sqrt{P_i} h_i \|x_i\|^{-\alpha/2} \right|^2 \tag{2.2}$$

where the additive white Gaussian noise (AWGN) power is excluded. On the other hand, the true received signal power at the MT, assuming no MBSs and including only the LBS, is

$$P_r = |h_1|^2 \|x_1\|^{-\alpha}. \tag{2.3}$$

Thus, the deceptive SINR including the LBS and all spoofing MBSs signals is

$$Q_r = \frac{P_r}{\sigma^2 + \sum_{x_i \in D^c} P_i \left| h_i \right|^2 \left\| x_i \right\|^{-\alpha}} \tag{2.4}$$

On the other hand, the true SINR [21] including only the LBS and excluding the MBSs is

$$Q_r = \frac{P_r}{\sigma^2 + \sum_{x_i \in D^c} P_i \left| h_i \right|^2 \left\| x_i \right\|^{-\alpha}} \tag{2.5}$$

Finally, the deceptive SIR excluding the thermal noise power σ^2 is defined as

$$R_r = \frac{\hat{P}_r}{\sum_{x_i \in D^c} P_i \left| h_i \right|^2 \left\| x_i \right\|^{-\alpha}} \tag{2.6}$$

In LTE cellular networks, either the power of reference signals or metrics like SINR are used to determine CA. This dissertation focuses on the case where the MT CA is triggered if either the false reference signal power $\hat{P}_r$ or the false SINR $\hat{Q}_r$ is above some predefined threshold β. The reason why this dissertation focuses on the false CA is because the CA is triggered by the MBSs. After CA, RLF is declared, i.e., the MT user is dropped from service, if either the true SINR Q_r or the deceptive SIR $\hat{R}_r$ is below some predefined threshold θ. The main reason for RLF is the inability of the MT to decode downlink control signals from the LBS, since the actual signal strength is poorer than the MT's estimation. The reason why this research also considers the RLF based on the true SINR metric is to make comparisons with the false RLF caused by the MBSs.

CHAPTER 3

CELL ASSOCIATION TRIGGER ATTACK

In this chapter, the detailed research problem will be illustrated in Section 3.1. Then, the results of all probability are given in Section 3.2.

3.1 Probability Definition

For the theoretical impact of the reference signal spoofing attack, and based on the preceding discussion, the conditional probability of a radio link failure given a deceptive CA trigger attack is defined as

$$\mathrm{P_{RC}} = \mathbb{P}\left(\mathrm{RLF}|\mathrm{CA}\right) \tag{3.1}$$

where the conditioning is on the event CA, which represents a CA having been triggered. Depending on which metric (false power or false SINR) is used, this dissertation has the CA probability [23] defined as

$$\mathrm{P_{CA}} = \mathbb{P}\left\{\hat{P}_r > \beta\right\} \tag{3.2}$$

or

$$\mathrm{P_{CA}} = \mathbb{P}\left\{\hat{Q}_r > \beta\right\}. \tag{3.3}$$

Furthermore, the probability of radio link failure is written as

$$\mathrm{P_{RLF}} = \mathbb{P}\left\{\hat{R}_r < \theta\right\} \tag{3.4}$$

or

$$\mathrm{P_{RLF}} = \mathbb{P}\left\{\hat{Q}_r < \theta\right\} \tag{3.5}$$

depending on whether the false SIR or true SINR metric used. For qualifying the RLF, the true SIR or SINR should be used. Otherwise, the RLF information is misleading. Note that this

dissertation will have true SIR or true SINR, when © = 1 for equation (2.2) in equations (2.6) and (2.4), respectively.

For analysis, it is assumed that set *D* is composed of the BS nearest to the target MT from each tier, i.e., the LBS and MBS nearest the origin. Next, the unconditional RLF probability and the CA probability have been derived. In the results below, this dissertation denotes $c := \pi \sum_{i=1}^{T=2} \lambda_i P_i^{\frac{2}{\alpha}}$, where λ_i is the average intensity (i.e., average number of BSs) in tier © with PPP distribution. Function F is defined as $\mathrm{F}(x) := \int_x^{\infty} \frac{m}{1+m^{\alpha}} \mathrm{d}m$.

3.2. Probability Results

3.2.1 Probability of RLF

Theorem 1: Let the unconditional probability of the false RLF be defined by equation (3.4) with equation (2.6). Then, the result is

$$\mathrm{P}_{\mathrm{RLF}} = 1 - \int_{\substack{0<u_1<u_2< \\ \ldots<u_n<\infty}} \exp\left(-u_n - \frac{2u_n \mathrm{F}\left(\theta^{-\frac{1}{\alpha}} u_n^{\frac{1}{2}} \left(\sum_{i=1}^{n} \frac{1}{u_i^{\frac{\alpha}{2}}} \right)^{\frac{1}{\alpha}} \right)}{\theta^{-\frac{2}{\alpha}} u_n \left(\sum_{i=1}^{n} \frac{1}{u_i^{\frac{\alpha}{2}}} \right)^{\frac{2}{\alpha}}} \right) \mathbf{du}. \tag{3.6}$$

Proof: See Appendix A.

Theorem 2: Let the unconditional probability of the true RLF be defined by equation (3.5) with equation (2.4). Then, the result is

$$\mathrm{P_{RLF}} = 1 - \int\limits_{\substack{0<u_1<u_2< \\ \ldots<u_n<\infty}} \exp\left(-u_n - \frac{2u_n \mathrm{F}\left(\theta^{-\frac{1}{\alpha}} u_n^{\frac{1}{2}} \left(\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}} \right)^{\frac{1}{\alpha}} \right)}{\theta^{-\frac{2}{\alpha}} u_n \left(\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}} \right)^{\frac{2}{\alpha}}} \right) \exp\left(\frac{-c^{-\frac{\alpha}{2}} \sigma^2 \theta}{\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}}} \right) \mathrm{d}\mathbf{u}. \tag{3.7}$$

Proof: See Appendix B.

3.2.2 Probability of CA

Theorem 3: Let the probability of a false CA be defined by equation (3.2) with the false power in equation (2.2). Then, the result is

$$\mathrm{P_{CA}} = \int\limits_{0<u_1<\ldots<u_n<\infty} \exp\left(-\frac{\beta \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{-\frac{\alpha}{2}}}{\sum_{i=1}^{n} \left(u_i \right)^{-\frac{\alpha}{2}}} - u_n \right) \mathrm{d}\mathbf{u}. \tag{3.8}$$

Proof: See Appendix C.

Theorem 4: Let the probability of a false CA be defined by equation (3.3) with the false SINR in equation (2.4). Then, the result is

$$\mathrm{P_{CA}} = \int\limits_{\substack{0<u_1<u_2< \\ \ldots<u_n<\infty}} \exp\left(-u_n - \frac{2u_n \mathrm{F}\left(\beta^{-\frac{1}{\alpha}} u_n^{\frac{1}{2}} \left(\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}} \right)^{\frac{1}{\alpha}} \right)}{\beta^{-\frac{2}{\alpha}} u_n \left(\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}} \right)^{\frac{2}{\alpha}}} \right) \exp\left(\frac{-c^{-\frac{\alpha}{2}} \sigma^2 \beta}{\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}}} \right) \mathrm{d}\mathbf{u}. \tag{3.9}$$

Proof: Similar to the proof of Theorem 2 found in Appendix B.

3.2.3 Conditional Probability of RLF Given CA Trigger Attack

Theorem 5: Let the probability of the true RLF given a false CA be defined by equation (2.5) with the false power in equation (2.2) for the case of one MBS attacked. Then, the result is

$$
\mathrm{P_{RH}} = \left[\int_{0<u_1<u_2<\infty} \exp\left(-\frac{\beta\left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{-\frac{\alpha}{2}}}{\sum_{i=1}^{n=2} (u_i)^{-\frac{\alpha}{2}}} - u_n \right) \mathrm{d}\mathbf{u} - \right.
$$

$$
\left. \int_{0<u_1<u_2<\infty} \exp\left(-u_2 - \frac{2u_2 \mathrm{F}\left(\theta^{-\frac{1}{\alpha}} u_2^{\frac{1}{2}} \left(\sum_{i=1}^{2} u_i^{-\frac{\alpha}{2}} \right)^{\frac{1}{\alpha}} \right)}{\theta^{-\frac{2}{\alpha}} u_2 \left(\sum_{i=1}^{2} u_i^{-\frac{\alpha}{2}} \right)^{\frac{2}{\alpha}}} \right) \exp\left(\frac{-c^{-\frac{\alpha}{2}} \sigma^2 \theta}{\sum_{i=1}^{2} u_i^{-\frac{\alpha}{2}}} \right) \mathrm{d}\mathbf{u} \right] \div \qquad (3.10)
$$

$$
\int_{0<u_1<u_2<\infty} \exp\left(-\frac{\beta\left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{-\frac{\alpha}{2}}}{\sum_{i=1}^{n=2} (u_i)^{-\frac{\alpha}{2}}} - u_n \right) \mathrm{d}\mathbf{u}
$$

Proof: See Appendix D.

Remark 1: $c := \pi \sum_{i=1}^{T=2} \lambda_i P_i^{\frac{2}{\alpha}}$ is a constant number, not a random variable because the number of tiers, density, and transmit power are all deterministic parameters.

Remark 2: According to Theorem 1 in equation (3.6), the integral function F(x) is not a function of the number of tiers *T*, transmit power *P*, and density λ. In others words, Theorem 1 depends only on path loss α, threshold θ, and number of MBSs (n – 1) involved. The reason behind this is because as the intensity of each BS tier increases, the sum of transmit power and the sum of interference power also increase. Consequently the ratio, e.g., SIR, still stays the same.

Remark 3: Also in equations (3.7) and (3.9), if the noise power σ^2 is close to or equal to zero, then the exponential term with σ^2 will become one. This scenario could also be applied to equation (3.10).

CHAPTER 4

RESULTS AND DISCUSSION

In this section, simulation results have been compared with numerical results obtained through the analysis discussed in Chapter 3. Results of the unconditional probability of radio link failure, probability of false CA, and conditional probability of radio link failure given a false CA trigger attack condition are shown.

4.1 Simulation Method and Parameters

This dissertation considers two tiers of the cellular network, $T = 2$, if $n = 2$, which implies that one MBS has been attacked; meanwhile, if $n = 1$, then only an LBS is active. Assuming that the path loss $\alpha = 4$ and Rayleigh fading coefficients h_i are independent, according to the PPP mapping theorem and Theorem 2.34 from the work of Haenggi [22], the PPP density is $\lambda(x) = \sum_{i=1}^{T} \lambda_i \frac{2\pi}{\alpha} P_i^{\frac{2}{\alpha}} x^{\frac{2}{\alpha}-1}$ [21], [24]. The density (or intensity) of each tier is $\lambda_1 = \lambda_2 = \left(250^2 \pi\right)^{-1}$ for the analytical results. The transmit power $P_1 = P_2 = 10$ watts. The total number of trials is 100,000 for simulations.

The target MT is located at the origin (0,0). The number and location of all base stations satisfy PPP probability distributions with given density. The simulation area can be either a circular disk or square; both yield the same simulation results. This research used a circular disk area with a 250-meter radius. Simulation steps for the unconditional probability RLF are listed in Table 4.1. More details will be explained following Table 4.1. Simulation results for other analytical cases can be obtained using a similar method as shown in Table 4.1. MATLAB was used for the simulation.

TABLE 4.1

SIMULATION PROCEDURE FOR RADIO LINK FAILURE

1:	Initialize basic parameters: Transmit power = *P*, Intensity = $\lambda_{1,2}$, Path loss = α, AWGN power = σ^2, Total No. of trials = NoTtra, Radius = radi
2:	**for** indexTH =1: The range of interest
	RLF(indexTH)=0;
	Notra2(indexTH)=0; %% Initialize a vector for good trials
3:	**for** i=1: NoTtra
4:	%% === Start making PPP in a circle for λ ===
	sz1=poissrand(λ_1); %% number of BS with λ_1
	r1 = radi*sqrt(rand(sz1,1));
	theta1 = 2*pi*rand(sz1,1);
	x1 = r1.*cos(theta1); y1 = r1.*sin(theta1); %% location of BS
5:	Repeat with λ_2 and return the number of BS sz2, location of BS x2,y2
	%%=== end of PPP ====
	npoints1 = [x1 y1]; %% BS location matrix with λ_1
	npoints2 = [x2 y2]; %% BS location matrix with λ_2
	Find out nearest point to the origin, resort to the 1st row.
6:	**If** (sz1>2 && sz2>2)
	Notra2(indexTH)= Notra2(indexTH)+1; %%update good trails
	Calculate the SIR
	if (SIR(indexTH) < threshold);
8:	RLF(indexTH)= RLF(indexTH)+1;
	end
	end
	end
9:	ProbofRLF(indexTH)=RLF(indexTH)/Notra2(indexTH);
	end
	Plot the figure.

In Table 4.1, Step 1 initializes all the basic parameters. Note that intensities λ_1 and λ_2 used for each tier in the simulation can be different from intensities $\lambda_1 = \lambda_2 = \left(250^2\pi\right)^{-1}$ used for analytical calculations with equations (3.6) and (3.7). Intensities λ_1 and λ_2 in the simulation are the average number of BSs in the unit area in the tier, and this does not matter because the simulation takes the SINR metric, considering not only the LBS and MBS but also the interference BSs. An intensity larger than at least two has been used. For instance, in the simulation for tier one, if $\lambda_1 = 4$, then the average number of BSs for all trials will be four,

where one is for the LBS, one is for an MBS, and the other two are for interference BSs. This is also the reason why in Step 6, a valid trial realization must satisfy the number of points (BSs) in both tiers being larger than two, such that interference is also included. Simulation results for $\lambda_1 = \lambda_2 = 4$ and 100 with the analysis results of $\lambda_1 = \lambda_2 = \left(250^2 \pi\right)^{-1}$ have been compared, and it can be seen that the probability difference between them for the same threshold is less than 0.05. Step 4 generates the points in a circle area with the radius parameter, radi. The number of points obtained using the MATLAB function for a given λ is poissrnd(λ). Then those points are uniformly distributed within the circle area. Since there are two tiers, this step should be repeated for tier 2. Step 8 calculates the probability of RLF by dividing the count of RLF events with the number of good trials.

This dissertation uses MATLAB to evaluate the integral expression. For example, if n = 2, then the integral range is denoted by $0 < u_1 < u_{n=2} < \infty$, that is, first the integral with respect to u_1 from zero to u_2 is taken, and second, the integral with respect to u_2 from zero to infinity is taken.

4.2 Figures

Figure 4.1 shows the probability of false CA versus threshold β in dB using the sum of the received power $\hat{P}_r$ metric in equations (2.2), (3.2), and (3.8). According to the curves, it can be seen that as the CA threshold increases, the probability of false CA triggered by the spoofing MBSs decreases. The curve with circles shows analytical results by using equation (3.8), while the curve with crosses indicates simulation results. Observe that both analytical and simulation results agree very well with each other.

Figure 4.2 demonstrates the probability of false CA versus threshold β in dB, using the SINR metric in equations (2.4), (3.3), and (3.9). In the case of one LBS with three MBSs, the

evaluation of equation (3.9) involves four-fold integrals. With only one MBS, this will mean double integrals. For the case without an MBS (i.e., only an LBS), there is only one integral for the analytical expression.

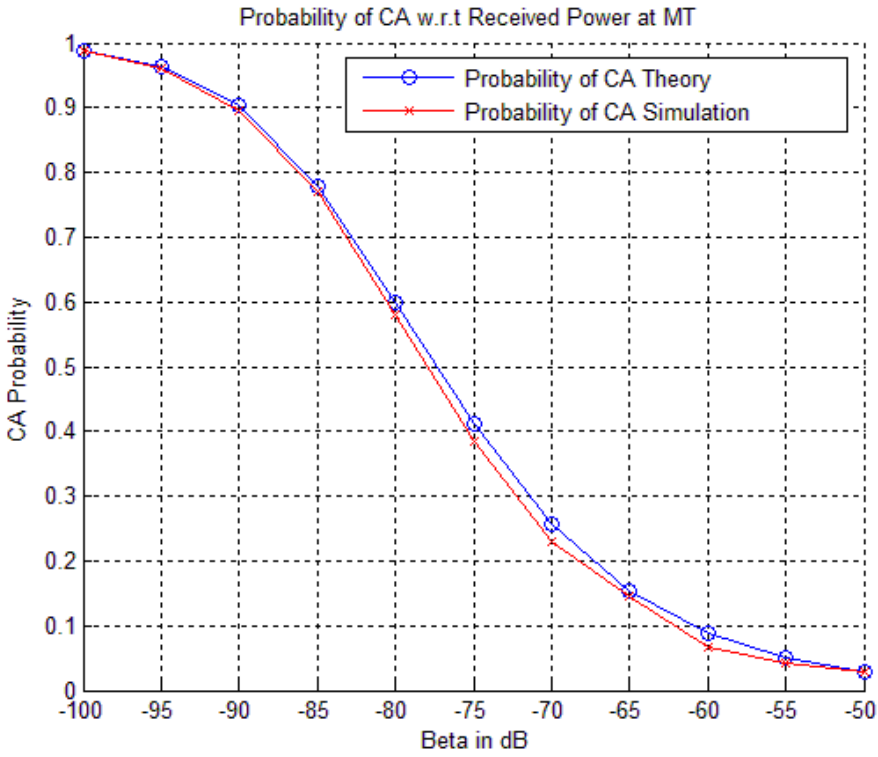

Figure 4.1. False CA probability versus threshold β in dB with $T = 2$, $\lambda_1 = \lambda_2 = \left(250^2 \pi\right)^{-1}$, $P_1 = P_2 = 10$ watts, and $\alpha = 4$.

Observe that if there are no MBSs, then the probability of CA is the smallest, compared with all other cases with MBSs. If the MBSs attack, then CA is easier (higher in probability) to trigger compared to the case without an MBS attack. For instance, at threshold $\beta = 10$ dB, the true CA probability for the no-MBS attack case is 0.2, which is less than the false CA probability 0.3 for the one-MBS attack case, and which is less than the false CA probability of 0.45 for the three-MBS attack case. Intuitively, this result is expected because it is easier to have a false CA event if more MBSs attack. Hence, the false CA probability of the MBS attack case is higher than the true CA probability of the LBS-only case. Recall that the CA probability using the SINR metric

is independent of the number of network tiers T, power P, and intensity λ. However, when the sum of the received power metric is used, all parameters affect the false CA probabilities. This dissertation verified this observation through both the simulation and analysis in the proofs of the theorems in the appendices.

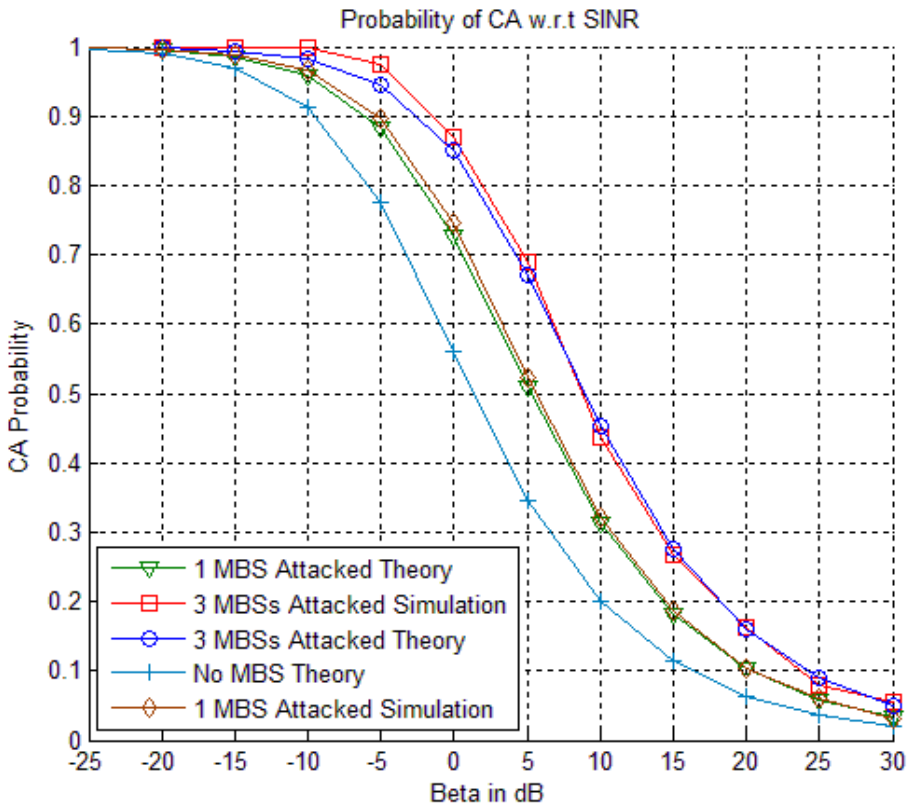

Figure 4.2. False CA probability versus threshold β in dB using SINR metric for one or three MBS attack cases and LBS-only case.

Figure 4.3 demonstrates the unconditional probability of RLF versus threshold θ in dB, using the SIR metric in equations (2.6), (3.4) and (3.6). The equation evaluation of the case with one LBS and three MBSs involves four-fold integrals, and double integrals for the one LBS and one MBS case. The single integral case is for only true RLF information for the LBS. Observe that as the threshold increases, the unconditional probability of RLF increases for all cases. This makes sense because as the threshold increases, the radio link between a user and a base station

has a higher chance of failing. If MBSs are involved, then those MBSs will mislead the RLF probability information. The more MBSs that are active, the lower the false RLF probability is miscalculated. For instance, at a threshold of 10 dB, the RLF probability of the LBS-only case is 0.8, which is the highest compared with all other cases. With the one-MBS-attacker case, the false RLF probability is misled to 0.68. The three-MBS-attackers case has the lowest probability value of 0.55. In other words, the communication system uses wrong judgment when MBSs are involved because of their false signal strength.

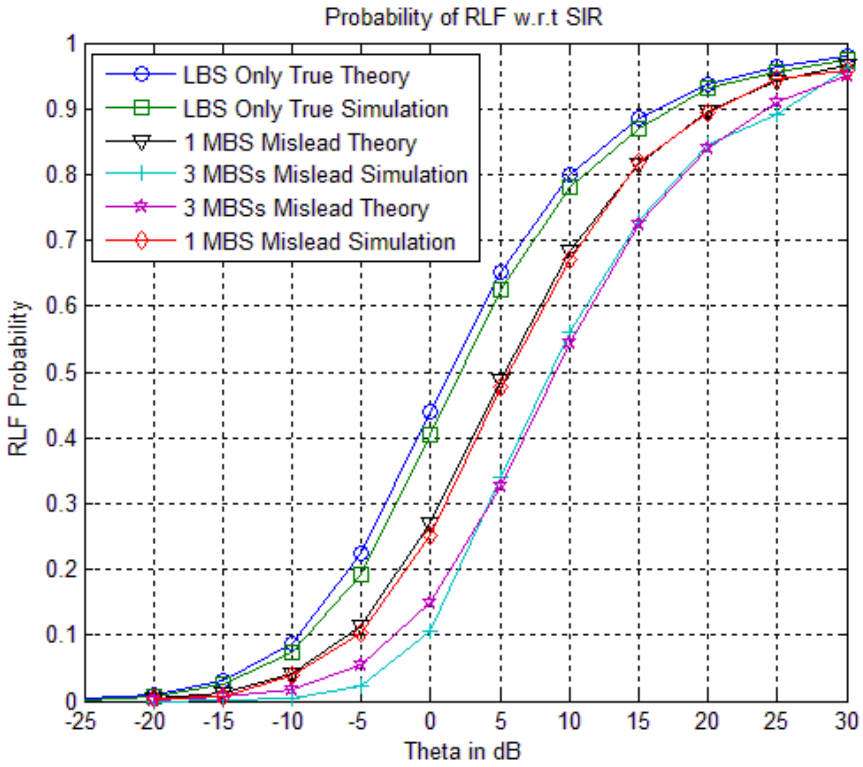

Figure 4.3. Unconditional RLF probability versus threshold θ in dB with SIR metric for one or three MBS attack cases and LBS-only case.

Figure 4.4 demonstrates the unconditional probability of RLF versus threshold θ in dB, using the SINR metric in equations (2.4), (3.5), and (3.7). Although the metric for RLF has been changed from SIR to SINR, it still shows similar results; for example, the unconditional RLF probability decreases as the number of MBSs increases.

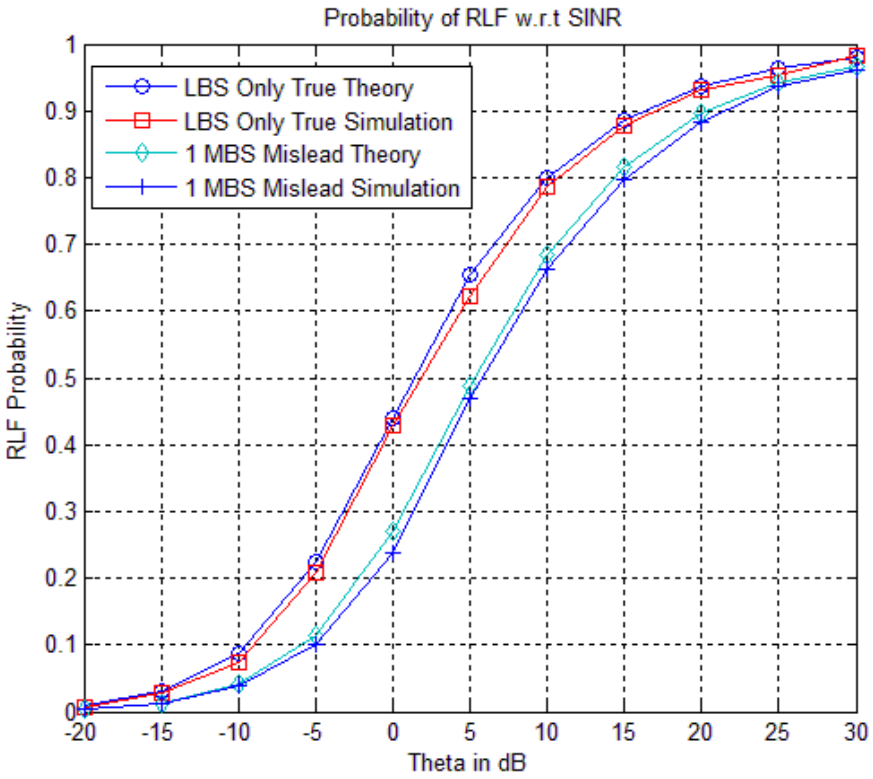

Figure 4.4. Unconditional RLF probability versus threshold θ in dB, using SINR metric for one MBS attack case and LBS-only case.

Figure 4.5 demonstrates the conditional probability of RLF given a false CA condition triggered by one MBS attack, using the SINR metric for RLF in equations (2.5) and (3.5), and the power metric for CA in equations (2.4) and (3.3). In this case, both the RLF and the CA use the same SINR metric. Recall that β is the threshold for CA, and θ is the threshold for RLF. This three-dimensional (3D) plot shows that for a given CA threshold β, as the threshold of RLF θ increases, the probability of RLF also increases. This behavior matches results shown in Figures 4.3 and 4.4. On the other hand, at a given RLF threshold θ, the conditional probability of RLF decreases as the false CA threshold β increases. This observation also matches with results shown in Figures 4.1 and 4.2.

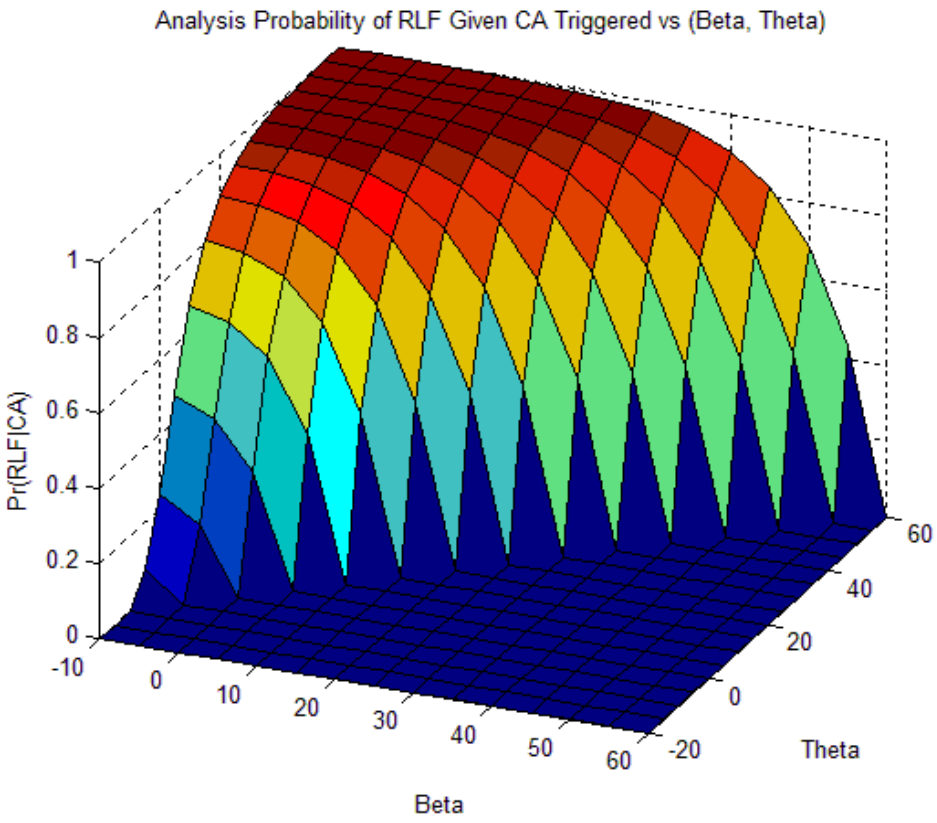

Figure 4.5. Conditional RLF probabilities given false CA condition triggered by one MBS attack versus RLF threshold θ and CA threshold β, when $T = 2$, $\lambda_1 = \lambda_2 = \left(250^2 \pi\right)^{-1}$, $P_1 = P_2 = 10$, and $\alpha = 4$.

Remark 4: Note that to reduce the RLF event, this paper prefers to choose thresholds that yield a low RLF probability, i.e., the bottom area of Figure 4.5. This implies that it would be desirable to choose the RLF threshold θ to be as low as possible and the CA threshold β to be as high as possible. The opposite is implied if the thresholds are chosen in the northwest corner, i.e., a large θ and a low β, and most likely the conditional RLF probability under a false CA condition triggered by the MBSs will be high. Drawing a line from β = –10 dB to θ = 60 dB, approximately separates Pr(RLF|CA) into the above zero area and the area almost equal to zero. If there is no MBS attack, then the line should be from β = –6 dB to θ = 60 dB because of the

approximate 4 dB difference between the true and false CA probabilities when the parameters here are applied, as indicated in Figures 4.2 and 4.3.

Figure 4.6 illustrates the simulated conditional RLF probability for a given false CA condition triggered by one MBS attack, using the SINR metric for RLF in equations (2.5) and (3.5), and the power metric for CA in equations (2.4) and (3.3). These 3D simulation results agree very well with the analyzed ones using equation (3.10), as shown in Figure 4.5.

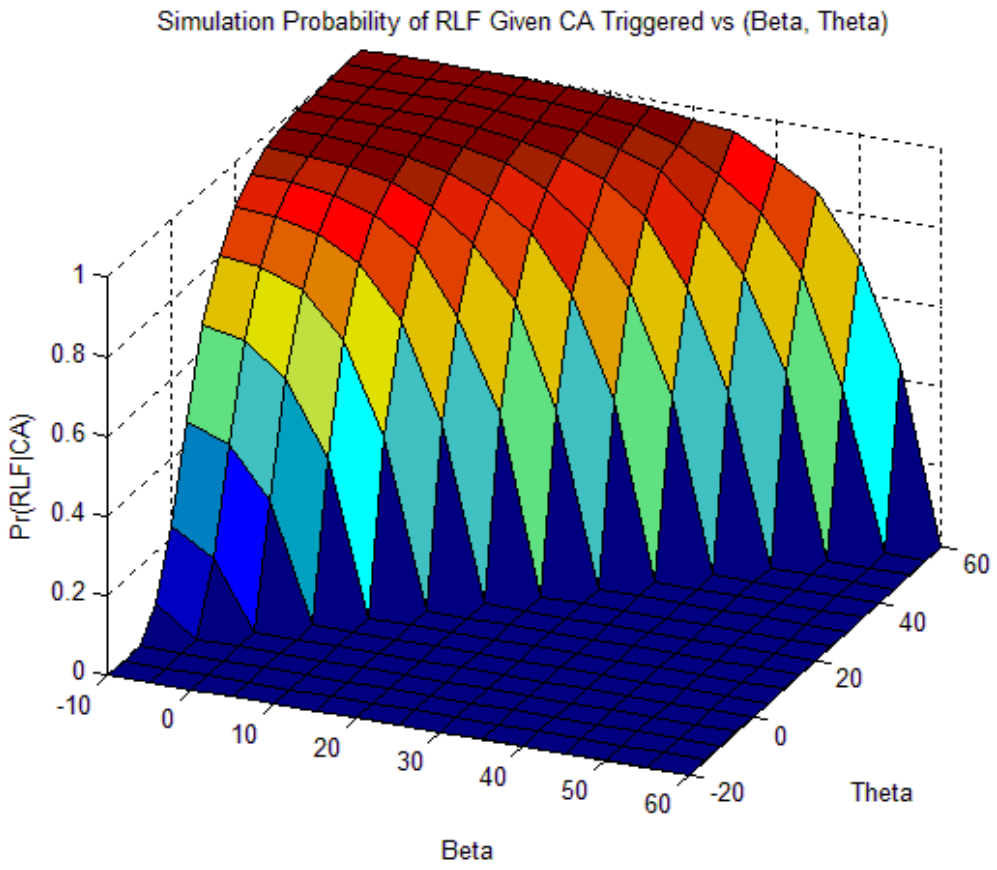

Figure 4.6. Simulated conditional RLF probability given false CA condition triggered by one MBS attack versus RLF threshold θ and CA threshold β, when $T = 2$, radius $= 250$, $P_1 = P_2 = 10$, and $\alpha = 4$.

Remark 5: There are two ways to perform the simulation. Method 1 is to simulate the conditional probability Pr(RLF|CA) directly without using the Bayes rule. In other words, at a

certain pair of (β, θ), first check whether the metric value for CA satisfies the threshold β or not. If yes, then check whether the metric value for RLF satisfies the threshold condition θ or not. If yes, then the RLF count parameter shown in Table 4.1 will be updated. Finally, divide the last RLF count by the total number of good trials. This is the method of simulation that was used in this dissertation research to generate Figure 4.6. Method 2 is to simulate the conditional probability Pr(RLF|CA) indirectly, using the conditional probability definition: Pr(RLF|CA) = Pr(RLF|CA) / Pr(CA).

This implies that the conditional probability Pr(RLF|CA) by simulating the joint probability Pr(RLF|CA) and the false CA probability Pr(CA) for a common false CA event can be obtained. Method 2 is helpful in verifying the theoretical derivations. This is because instead of proving the final results of Pr(RLF|CA) through simulation, the theoretical derivations of Pr(RLF|CA) and Pr(CA) through simulation will be more certain. However, note that the simulations of Pr(RLF|CA) and Pr(CA) cannot be performed independently. In other words, the RLF event shown in Table 4.1 for Pr(RLF|CA) and Pr(CA) simulations should be updated for the same common false CA event. If the Pr(RLF|CA) and Pr(CA) are simulated independently, then the RLF count cannot be calculated for the common CA event. Independent simulations can cause Pr(RLF|CA) to be larger than one when Pr(CA) is very small, which obviously is not correct.

Figure 4.7 illustrates the analysis conditional probability of RLF given a false CA condition triggered by one MBS attack, using the SINR metric for RLF in equations (2.5) and (3.5), and the power metric for CA in equations (2.2) and (3.2). Observe that these behaviors are similar to those shown in Figure 4.6. For example, for a given β, Pr(RLF|CA) increases as θ increases. And if θ is fixed, then Pr(RLF|CA) decreases as β increases. Note also that the

biggest difference compared with the results shown in Figures 4.5 and 4.7 is that the range of CA threshold β is changed to (–110 dB, –10 dB) from (–10 dB, 60 dB). Such β range difference also matches well with the β range difference between Figures 4.1 and Figure 4.2. This difference is mainly due to using different metrics such as the SINR in equation (2.4) and the sum of power in equation (2.2) for Figures 4.5 and 4.7, respectively.

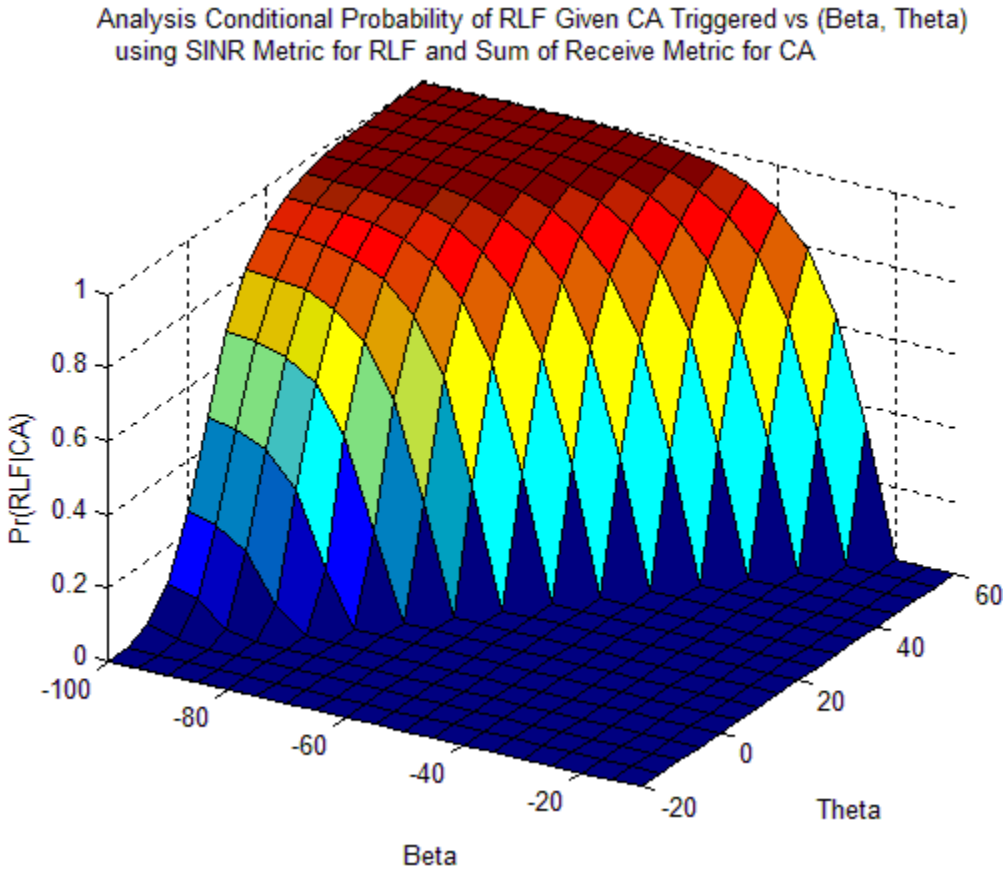

Figure 4.7. Analyzed conditional RLF probability for a given false CA condition triggered by one MBS attack versus RLF threshold θ and CA threshold β, using SINR metric for RLF and sum of receive power for CA, when $T = 2$, $\lambda_1 = \lambda_2 = \left(250^2 \pi\right)^{-1}$, $P_1 = P_2 = 10$, $\alpha = 4$.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

This dissertation study involved the problem when a set of MBSs misleads a MT into associating with suboptimal LBSs and results in RLF, assuming that the locations of BSs are PPP distributed. The following were derived: (a) probability of the CA process using the SINR metric and the sum of the receive power metric; (b) unconditional probability of RLF using SINR and SIR metrics; and (c) conditional probability of eight RLFs for a given condition of MBS attack using the SINR metric and the sum of the receive signal power metric. The theoretical expression for the unconditional RLF probability with SIR metric shows that the probability is independent with power, density, and number of tiers. The reason for this is because the ratio of the sum of LBS and MBS power over the sum of interference power stays the same, even if the power, density, and number of tiers changes (e.g., density increases). For the unconditional RLF probability, simulation results also show that as the RLF threshold increases, an RLF event has a higher chance of occurring. The simulations also prove that the false CA event has a greater chance of being triggered as the CA threshold decreases. The simulation of Pr(RLF|CA) can be performed in two ways: by directly simulating the conditional probability, and by separately counting the Pr(RLF|CA) and Pr(CA) for a common CA event. Finally, according to the three-dimensional figures, it was observed that the interesting area in which to avoid the conditional RLF given a false CA condition is when the CA threshold is high and the RLF threshold is low, for example, $\beta > -10$ dB and $\theta < 60$ dB, respectively, for the environments considered in this study.

5.2 Impact to Society

This dissertation will impact members of society who seek secure wireless communications cellular networks because it provides general guidelines on how to choose the thresholds to maintain a safe cell association and avoid radio link failure. Examples of the guidelines are as follows:

- In a case where CA is defined as the received power metric, the threshold should be less than –100 dB to ensure that CA probability is close enough to 100 percent.
- In a case where CA is defined as the SINR metric, if MBSs attacked, then the CA probability will be increased. For example, for a given CA probability of 0.8, the threshold will be 5 dB higher in the case of one MBS attacked or 10 dB higher for if three MBSs are attacked, compared to the case of no MBSs attacked.
- In a case where RLF is defined as the SIR metric, if MBSs are attacked, then the RLF probability will be miscalculated, that is, the misled RLF probability is lower than the true one. For example, if the threshold is 10 dB, then this is 10 percent lower than the true one in the case of one MBS attacked and 23% percent lower than the true one in the case of three MBSs attacked. This result is also similar to the case where RLF is defined as an SINR metric.
- In a case where RLF is defined as the SINR, CA is defined as a power metric, and only one MBS is attacked, the safe design region of the condition RLF probability given a false CA condition will be a CA threshold larger than –10dB and an RLF threshold smaller than 60 dB.

- In a case where both RLF and CA are defined as SINR, and only one MBS is attacked, the safe design region of the condition RLF probability given a false CA condition will be a CA threshold larger than –100 dB and an RLF threshold smaller than 60 dB.

5.3 Future Work

Future work can be summarized as follows:

- The $\mathbb{P}(\text{RLF}|\text{CA})$ for a set of MBSs attacked could be derived. This study focused only on n = 2, which is the case of one LBS and one MBS.
- If each BS uses multiple antennas, then the performance could be different. A scenario involving a multiple input and multiple output case is worth researching. This study focused on the case of only one antenna.
- This research shows the performance of CA probability for MBSs attacked. There could be a method to decrease the effect of the MBSs attacked. Such a scenario would be worth investigating.

REFERENCES

REFERENCES

[1] Q. Ye, B. Rong, Y. Chen, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "User association for load balancing in heterogeneous cellular networks," *IEEE Trans. Wireless Commun*., vol. 12, no. 6, pp. 2706–2716, June 2013.

[2] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts*., vol. 16, no. 1, pp. 283–302, First Quarter 2014.

[3] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE network," *IEEE Trans. Mobile Comput*., vol. 13, no. 2, pp. 457–468, Feb. 2014.

[4] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE Journal on Sel. Areas in Communications*, vol. 30, pp. 550–560, Apr. 2012.

[5] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Communications Magazine*, vol. 18, pp. 10–21, June 2011.

[6] T. Kahwa and N. Georganas, "A hybrid channel assignment scheme in large-scale, cellular-structured mobile communication systems," *IEEE Trans. on Communications,* vol. 26, pp. 432–438, Apr. 1978.

[7] B. Eklundh, "Channel utilization and blocking probability in a cellular mobile telephone system with directed retry," *IEEE Trans. on Communications*, vol. 34, pp. 329–337, Apr. 1986.

[8] X. Wu, B. Mukherjee, and S. H. G. Chan, "MACA-an efficient channel allocation scheme in cellular networks," in *Proc., IEEE Globecom*, vol. 3, pp. 1385–1389, 2000.

[9] A. Sang, X. Wang, M. Madihian, and R. D. Gitlin, "Coordinated load balancing, handoff/cell-site selection, and scheduling in multi-cell packet data systems," *Wireless Networks*, vol. 14, pp. 103–120, Jan. 2008.

[10] S. Corroy, L. Falconetti, and R. Mathar, "Dynamic cell association for downlink sum rate maximization in multi-cell heterogeneous networks," *IEEE International Conference on Communications (ICC)*, pp. 2457 – 2461, 2012.

[11] H. Jo, Y. Sang, P. Xia, and J. Andrews, "Heterogeneous cellular networks with flexible cell association: a comprehensive downlink SINR analysis," *IEEE Trans. on Wireless Communications*, vol.11, pp.3484-3495, July 2011.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts*., vol. 16, 2014.

[13] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun*., vol. 11, no. 3, pp. 903–907, Mar. 2012.

[14] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[15] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun*., vol. 26, no. 1, pp. 25–36, Jan. 2008.

[16] Q. Peng, P. C. Cosman, and L. B. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE J. Sel. Areas Commun*., vol. 29, no. 4, pp. 903–911, Apr. 2011.

[17] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, pp. 996–1019, July 2013.

[18] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications.* New York: Wiley, 1995.

[19] D. Stoyan and H. Stoyan. Fractals, *Random Shapes and Point Fields*. New York: Wiley, 1994.

[20] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, 2004.

[21] G. Nigam, P. Minero, and M. Haenggi, "Coordinated multipoint in heterogeneous networks: A stochastic geometry approach," in *Proc. IEEE GLOBECOM Workshop on Emerging Technologies for LTE-Advanced and Beyond 4G*, Atlanta, GA, Dec. 2013.

[22] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge: Cambridge University Press, 2013.

[23] A. Guo and M. Haenggi, "Asymptotic deployment gain: A new approach to characterize coverage probability," IEEE International Conference on Communications, Sydney, Australia, June 2014.

[24] G. Nigam, P. Minero, and M. Haenggi, "Coordinated multipoint joint transmission in heterogeneous networks," *IEEE Trans. Commun*., vol. 62, no. 11, pp. 4134–4146, Oct. 2014.

[25] M. Haenggi and R. K. Ganti, *Interference in Large Wireless Networks*. Hanover, MA: Now Publishers, 2010.

[26] A. Baddeley. *Spatial Point Processes and Their Applications*. Springer, 1982.

[27] V. Baumstark and G. Last, "Some distributional results for Poisson-Voronoi tessellations," *Last Advances in Appl. Prob*., vol. 39, no. 1, pp.16–40, Mar. 2007.

[28] D. Moltchanov, "Survey paper: Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, Aug. 2012.

APPENDICES

APPENDIX A

PROOF OF THEOREM 1

$$\mathrm{P}_{\mathrm{RLF}} = 1 - \mathbb{P}\left(\mathrm{SIR} > \theta\right)$$

$$\overset{(a)}{=} 1\text{-}\mathbb{P}\left(\frac{\left| \sum_{i=1}^{n} P_i \left\| x_i \right\|^{\frac{-\alpha}{2}} h_i \right|^2}{\sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2} > \theta \right) \tag{A.1}$$

$$= 1\text{-}\mathbb{P}\left(\left| \sum_{i=1}^{n} P_i \left\| x_i \right\|^{\frac{-\alpha}{2}} h_i \right|^2 > \theta \sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2 \right) \tag{A.2}$$

$$\overset{(b)}{=} 1\text{-}\mathbb{E}_{\mathbf{x},\mathbf{h}} \left(\exp\left(- \frac{\theta \sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2}{\sum_{i=1}^{n} P_i \left\| x_i \right\|^{-\alpha}} \right) \right), \tag{A.3}$$

where *(a)* uses the definition of SIR as in equation (2.6), and for *(b)*, it is assumed that the Rayleigh fading coefficients are all independent. Since $\left| h_i \right|^2 \sim \exp(1)$, for a given condition $P_i \left\| x_i \right\|^{-\frac{\alpha}{2}}$, it follows that $\left| \sum_{i=1}^{n} \left(P_i \left\| x_i \right\|^{-\alpha} \right)^{\frac{1}{2}} h_i \right|^2 \sim \exp\left(\left(\sum_{i=1}^{n} P_i \left\| x_i \right\|^{-\alpha} \right)^{-1} \right)$.

From now on, define $r_i \coloneqq P_i^{-1} \left\| x_i \right\|^{\alpha}$ as the path loss between user and base station normalized with power P_i, The above equation can be rewritten as

$$\mathrm{P}_{\mathrm{RLF}} = 1\text{-}\mathbb{E}_{\mathbf{r},\mathbf{h}} \left(\exp\left(- \frac{\theta \sum_{i>n} r_i^{-1} \left| h_i \right|^2}{\sum_{i=1}^{n} r_i^{-1}} \right) \right), \tag{A.4}$$

Now, use the property of Laplace transformation $\mathcal{L}\{f\}(s)=\mathbb{E}\left(e^{-sv}\right)$, where f is the density function of V. In the current case, v is $\sum_{i>n} r_i^{-1}\|h_i\|^2$. Equation (A.4) yields

$$\mathrm{P_{RLF}}=1\text{-}\mathbb{E}_{\mathbf{r}}\left(\mathcal{L}\left(\frac{\theta}{\sum_{i=1}^{n} r_i^{-1}}\right)\right) \tag{A.5}$$

To compute $\mathcal{L}\{f\}(s)=\mathrm{E}\left(e^{-sv}\right)$, expand it by using the definition of expectation:

$$\mathcal{L}\{f\}(s)=\mathbb{E}\left(e^{-sv}\right)$$

$$=\mathbb{E}_{\mathbf{r,h}}\left(e^{-s\sum_{i>n} r_i^{-1}\|h_i\|^2}\right) \tag{A.6}$$

$$=\mathbb{E}_{\mathbf{r}}\left(\prod_{i>n}\mathbb{E}_{\mathbf{h}}\left(e^{-s|h_i|^2 r_i^{-1}}\right)\right) \tag{A.7}$$

$$=\mathbb{E}_{\mathbf{r}}\left(\prod_{i>n}\frac{1}{1+sr_i^{-1}}\right) \tag{A.8}$$

where the last equality is because the moment-generating function of an exponential random variable x with parameter λ is defined as $\mathrm{M}_x(t)=\frac{\lambda}{\lambda-t},(t<\lambda)$. According to the probability-generating function of the Poisson point process Θ, if $\lambda(x)$ is the intensity function of this PPP, then $\mathrm{G}_\Theta\left(f_g\right)=\exp\left[\int_{\mathbb{R}}\left(f_g(x)-1\right)\lambda(x)\mathrm{d}x\right]$. In the current case, $f_g(x)=\frac{1}{1+sr_i^{-1}}$. Because of the consideration of non-cooperative interference $\coprod_{i>n}$, the region will be r_n to ∞. After applying $\lambda(x)$, equation (A.8) yields

$$\exp\left[\frac{2\pi}{\alpha}\sum_{i=1}^{T=2}\lambda_i P_i^{2/\alpha}\int_{r_n}^{\infty}\left(\frac{1}{1+sx^{-1}}-1\right)x^{\frac{2}{\alpha}-1}\mathrm{d}x\right]$$

$$=\exp\left[-2\pi s^{\frac{2}{\alpha}}\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\mathrm{F}\left(\left(r_n s^{-1}\right)^{\frac{1}{\alpha}}\right)\right]. \tag{A.9}$$

where $T=2$ is the number of ties. The last equality above is obtained by changing the integration variable into $x=st^{\alpha}$ and $\mathrm{F}(x)\coloneqq\int_{x}^{\infty}\frac{m}{1+m^{\alpha}}\mathrm{d}m$.

Using the result of joint distance distribution to the nearest point in a PPP from the work of Stoyan and Stoyan [19], for $0<r_1<r_2<\ldots<r_n<\infty$, the joint distribution of $\boldsymbol{r}$ can be derived as

$$f(\mathbf{r})=\left(\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\pi\frac{2}{\alpha}\right)^n e^{-\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\pi r_n^{2/\alpha}}\prod_{i=1}^{n}r_i^{\frac{2}{\alpha}-1}. \tag{A.10}$$

Finally, by defining $s=\frac{\theta}{\sum_{i=1}^{n}r_i^{-1}}$, substituting this s into equation (A.8), and combining equations (A.8) and (A.4) with equation (A.9), the RLF probability equation yields

$$\mathrm{P_{RLF}}=1-\int_{0<r_1<r_2<\ldots<r_n<\infty}\exp\left[-2\pi\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\left(\frac{\theta}{\sum_{i=1}^{n}r_i^{-1}}\right)^{\frac{2}{\alpha}}\times\right.$$
$$\left.\mathrm{F}\left(r_n^{\frac{1}{\alpha}}\left(\sum_{i=1}^{n}r_i^{-1}\right)^{\frac{1}{\alpha}}\theta^{-\frac{1}{\alpha}}\right)\right]f(\mathbf{r})\mathrm{d}\mathbf{r}. \tag{A.11}$$

Since $\pi\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}$ is a constant number without any random variable, let $c\coloneqq\pi\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}$. After simplifying equation (A.11) by using $u_i=r_i^{2/\alpha}\pi\sum_{j=1}^{T=2}\lambda_j P_j^{2/\alpha}$, this proves Theorem 1.

APPENDIX B

PROOF OF THEOREM 2

$$\mathrm{P_{RLF}} = 1 - \mathbb{P}\left(\mathrm{SINR} > \theta\right)$$

$$\overset{(a)}{=} 1 - \mathbb{P}\left(\frac{\left| \sum_{i=1}^{n} P_i \left\| x_i \right\|^{\frac{-\alpha}{2}} h_i \right|^2}{\sigma^2 + \sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2} > \theta \right) \tag{B.1}$$

$$= 1 - \mathbb{P}\left(\left| \sum_{i=1}^{n} P_i \left\| x_i \right\|^{\frac{-\alpha}{2}} h_i \right|^2 > \theta \left(\sigma^2 + \sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2 \right) \right) \tag{B.2}$$

$$\overset{(b)}{=} 1 - \mathbb{E}_{\mathbf{x},\mathbf{h}} \left(\exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n} P_i \left\| x_i \right\|^{-\alpha}} \right) \exp\left(-\frac{\theta \sum_{i>n} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2}{\sum_{i=1}^{n} P_i \left\| x_i \right\|^{-\alpha}} \right) \right) \tag{B.3}$$

$$\overset{(c)}{=} 1 - \mathbb{E}_{\mathbf{r},\mathbf{h}} \left(\exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n} r_i^{-1}} \right) \exp\left(-\frac{\theta \sum_{i>n} r_i^{-1} \left| h_i \right|^2}{\sum_{i=1}^{n} r_i^{-1}} \right) \right) \tag{B.4}$$

$$\overset{(d)}{=} 1 - \mathbb{E}_{\mathbf{r}} \left(\exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n} r_i^{-1}} \right) \mathcal{L}\left(\frac{\theta}{\sum_{i=1}^{n} r_i^{-1}} \right) \right) \tag{B.5}$$

$$= 1 - \int_{0<r_1<r_2<..<r_n<\infty} \exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n} r_i^{-1}} \right) \mathcal{L}\left(\frac{\theta}{\sum_{i=1}^{n} r_i^{-1}} \right) f(\mathbf{r}) \mathrm{d}\mathbf{r}, \tag{B.6}$$

where *(a)* follows the definition of SINR in equation (2.4); *(b)* uses dependency of fading and

$\left|\sum_{i=1}^{n}\left(P_i\|x_i\|^{-\alpha}\right)^{\frac{1}{2}}h_i\right|^2 \sim \exp\left(\left(\sum_{i=1}^{n}P_i\|x_i\|^{-\alpha}\right)^{-1}\right)$ and $|h_i|^2 \sim \exp(1)$ for a given condition $P_i\|x_i\|^{-\frac{\alpha}{2}}$; *(c)* follows by changing $P_i^{-1}\|x_i\|^{\alpha}$ into the variable r_i; and *(d)* uses the property of Laplace transformation $\mathcal{L}\{f\}(s)=\mathbb{E}\left(e^{-sv}\right)$. As with Theorem 1 proof, the result equation (A.9) can be used for the derivation. To simplicity further, the joint pdf equation (A.10) can be rewritten as

$$f(\mathbf{r}) = e^{-\pi r_n^{2/\alpha}\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}}\prod_{i=1}^{n}\left(\frac{2}{\alpha}r_i^{-1}r_i^{\frac{2}{\alpha}}\pi\sum_{j=1}^{T=2}\lambda_j P_j^{\frac{2}{\alpha}}\right) \tag{B.7}$$

The last step is to substitute equations (B.7) and (A.9) into equation (B.6) and simplify the equation as

$$\mathrm{P_{RLF}} = 1 - \int_{0<r_1<\ldots<r_n<\infty}\exp\left[-2\pi\left(\frac{\theta}{\sum_{i=1}^{n}r_i^{-1}}\right)^{\frac{2}{\alpha}}\left(\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\right)\mathrm{F}\left(\theta^{\frac{1}{\alpha}}\left(\sum_{i=1}^{n}\frac{r_n}{r_i}\right)^{\frac{1}{\alpha}}\right)\times\right.$$
$$\left.\frac{-\theta\sigma^2}{\sum_{i=1}^{n}r_i^{-1}} - \pi r_n^{\frac{2}{\alpha}}\sum_{i=1}^{T=2}\lambda_i P_i^{\frac{2}{\alpha}}\right]\prod_{i=1}^{n}\left(\frac{2}{\alpha}r_i^{-1}r_i^{\frac{2}{\alpha}}\pi\sum_{j=1}^{T=2}\lambda_j P_j^{\frac{2}{\alpha}}\right)\mathrm{d}\mathbf{r} \tag{B.8}$$

$$\overset{(a)}{=} 1 - \int_{0<r_1<r_2<\ldots<r_n<\infty} \exp\left[-2 \left(\frac{\theta \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}} \left(r_n^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}}}{\sum_{i=1}^{n} \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}} u_i^{\frac{-\alpha}{2}} \left(r_n^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}}} \right)^{\frac{2}{\alpha}} \times \right.$$

$$\left. \mathrm{F}\left(\theta^{\frac{1}{\alpha}} \left(\sum_{i=1}^{n} \left(\frac{u_n}{u_i} \right)^{\frac{\alpha}{2}} \right)^{\frac{1}{\alpha}} \right) + \frac{-\theta\sigma^2}{\sum_{i=1}^{n} \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}} u_i^{-\frac{\alpha}{2}}} - u_n \right] \times \tag{B.9}$$

$$\prod_{i=1}^{n} \left(\frac{2}{\alpha} r_i^{-1} \pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} r_i^{\frac{2}{\alpha}} \right) \left(\frac{2}{\alpha} \right) \left(\sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \pi \right)^{\frac{-\alpha}{2}} \mathbf{u}^{\frac{\alpha}{2}-1} \mathrm{d}\mathbf{u}$$

$$= \int_{0<r_1<r_2<\ldots<r_n<\infty} \exp\left[-2 \left(\frac{\theta (u_n)^{\frac{\alpha}{2}}}{\sum_{i=1}^{n} \left(\frac{u_n}{u_k} \right)^{\frac{\alpha}{2}}} \right)^{\frac{2}{\alpha}} \mathrm{F}\left(\theta^{\frac{1}{\alpha}} \left(\sum_{i=1}^{n} \left(\frac{u_n}{u_i} \right)^{\frac{\alpha}{2}} \right)^{\frac{1}{\alpha}} \right) - \right. \tag{B.10}$$

$$\left. \frac{\theta u_n \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}}}{\sum_{i=1}^{n} u_i^{-\frac{\alpha}{2}}} - u_n \right] \mathrm{d}\mathbf{u}.$$

where *(a)* multiplies $\left(r_n^{\frac{2}{\alpha}} \right)^{\frac{\alpha}{2}}$ to both the numerator and denominator for the first term. After applying $c := \pi \sum_{i=1}^{T=2} \lambda_i P_i^{\frac{2}{\alpha}}$, the proof of Theorem 2 is completed.

APPENDIX C

PROOF OF THEOREM 3

$$\mathrm{P}_{\mathrm{CA}} = \mathbb{P}\left(P_r > \beta\right)$$

$$\overset{(a)}{=} \mathbb{P}\left(\left|\sum_{i=1}^{n=2} \sqrt{p_i}\left\|x_i\right\|^{-\frac{\alpha}{2}} h_i\right|^2 > \beta\right) \tag{C.1}$$

$$\overset{(b)}{=} \mathbb{E}_{\mathbf{h}}\left(\exp\left(-\frac{\beta}{\sum_{i=1}^{n} P_i\left\|x_i\right\|^{-\alpha}}\right)\right) \tag{C.2}$$

$$\overset{(c)}{=} \mathbb{E}_{\mathbf{r}}\left(\exp\left(-\frac{\beta}{\sum_{i=1}^{n} r_i^{-1}}\right)\right) \tag{C.3}$$

$$= \int_{0<r_1<..<r_{n=2}<\infty} \exp\left(-\frac{\beta}{\sum_{i=1}^{n=2} r_i^{-1}}\right) f(\mathbf{r})\mathrm{d}\mathbf{r}, \tag{C.4}$$

where *(a)* follows the definition of P_r; *(b)* is because of the assumption that Rayleigh fading coefficients are all independent and $\left|\sum_{i=1}^{n} \sqrt{p_i}\left\|x_i\right\|^{-\frac{\alpha}{2}} h_i\right|^2$ is exponentially distributed for given condition **h**; and *(c)* changes the random variable into $r_i := P_i^{-1}\left\|x_i\right\|^{\alpha}$. Since **r** is the only random variable in equation (C.14), and the joint pdf of **r** is given as equation (A.10), equation (C.4) can be expressed as:

$$\int_{0<r_1<r_2<..<r_n<\infty} \exp\left(\frac{-\beta}{\sum_{i=1}^{n} r_i^{-1}} - \pi r_n^{\frac{2}{\alpha}} \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right) \prod_{i=1}^{n=2} \left(\frac{2}{\alpha} r_i^{-1} r_i^{\frac{2}{\alpha}} \pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right) \mathbf{dr} \tag{C.5}$$

$$\overset{(a)}{=} \int_{0<u_1<..<u_{n=2}<\infty} \exp\left(- \frac{\beta \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{\frac{2}{\alpha}} \right)^{-\frac{\alpha}{2}}}{\sum_{i=1}^{n} (u_i)^{-\frac{\alpha}{2}}} - u_n \right) \mathbf{du} \tag{C.6}$$

where *(a)* changes the random variable r_i into u_i, $r_i^{-1} = u_i^{-\frac{a}{2}} \left(\pi \sum_{j=1}^{T=2} \lambda_j P_j^{2/\alpha} \right)^{-\alpha/2}$. After changing $\pi \sum_{i=1}^{T=2} \lambda_i P_i^{\frac{2}{\alpha}}$ into u_i, the proof of Theorem 3 is completed.

APPENDIX D

PROOF OF THEOREM 5

$$\mathrm{P_{RC}} = \mathbb{P}\left(\mathrm{RLF}|\mathrm{CA}\right) \overset{(a)}{=} \frac{\mathbb{P}\left(\mathrm{RLF},\mathrm{CA}\right)}{\mathbb{P}\left(\mathrm{CA}\right)} \tag{D.1}$$

where *(a)* is the definition of the conditional probability. Note that the derivation of $\mathbb{P}\left(\mathrm{CA}\right)$ was given in the proof of Theorem 3. Hence, $\mathbb{P}\left(\mathrm{RLF},\mathrm{CA}\right)$ needs to be derived first:

$$\mathbb{P}\left(\mathrm{RLF},\mathrm{CA}\right) = \mathbb{P}(Q_r < \theta, P_r > \beta) \tag{D.2}$$

$$\overset{(a)}{=} \mathbb{P}\left(\frac{\left| \sum_{i=1}^{n=1} P_i \left\| x_i \right\|^{\frac{-\alpha}{2}} h_i \right|^2}{\sigma^2 + \sum_{i>n=2} P_i \left\| x_i \right\|^{-\alpha} \left| h_i \right|^2} < \theta, \left| \sum_{i=1}^{n=2} \sqrt{p_i} \left\| x_i \right\|^{-\frac{\alpha}{2}} h_i \right|^2 > \beta \right) \tag{D.3}$$

$$\overset{(b)}{=} \mathbb{P}\left(\left| r_1^{-\frac{1}{2}} h_1 \right|^2 < \theta\sigma^2 + \theta \left| \sum_{i>n=2} r_i^{-\frac{1}{2}} h_i \right|^2, \left| \sum_{i=1}^{n=2} r_i^{-\frac{1}{2}} h_i \right|^2 > \beta \right) \tag{D.4}$$

$$\overset{(c)}{=} \mathbb{P}\left(\beta < \left| \sum_{i=1}^{n=2} r_i^{-\frac{1}{2}} h_i \right|^2 < \theta\sigma^2 + \left| \sum_{i>2} r_i^{-\frac{1}{2}} h_i \right|^2 + \left| r_2^{-\frac{1}{2}} h_2 \right|^2 \right), \tag{D.5}$$

where *(a)* uses the definition of SINR and P_r; *(b)* changes the random variable $\sqrt{P_i}\left\| x_i \right\|^{-\frac{\alpha}{2}}$ into $r_i^{-\frac{1}{2}}$; and *(c)* is according to the definition of the cumulative distribution function (CDF), $\mathbb{P}$ $(\mathrm{a} < \mathrm{X} < \mathrm{b}) = \mathrm{F}_x(b) - \mathrm{F}_x(a)$, and $\mathrm{F}_x(X) = \mathbb{P}(X < x)$. Meanwhile, note that $\left| \sum_{i=1}^{n} r_i^{-\frac{1}{2}} h_i \right|^2 \sim \exp\left(\left(\sum_{i=1}^{n} r_i^{-1} \right)^{-1} \right)$, because all the fading coefficients h_i are independent as assumed. Thus, equation (D.5) yields

$$\mathbb{E}_{\mathbf{r},\mathbf{h}}\left[\left(1-\exp\left(-\frac{\theta\sigma^2+\theta\left|\sum_{i>n=2} r_i^{-\frac{1}{2}}h_i\right|^2+\left|r_2^{-\frac{1}{2}}h_2\right|^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\right)-\left(1-\exp\left(-\frac{\beta}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\right)\right], \tag{D.6}$$

In equation (D.6), there are two terms. After canceling 1, the first term yields

$$\mathbb{E}_{\mathbf{r},\mathbf{h}}\left(-\exp\left(-\frac{\theta\sigma^2+\theta\left|\sum_{i>n=2} r_i^{-\frac{1}{2}}h_i\right|^2+\left|r_2^{-\frac{1}{2}}h_2\right|^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\right) \tag{D.7}$$

$$=\mathbb{E}_{\mathbf{r},\mathbf{h}}\left[-\exp\left(\frac{-\theta\sigma^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\exp\left(\frac{-\theta\left|\sum_{i>n=2} r_i^{-\frac{1}{2}}h_i\right|^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\exp\left(\frac{-\left|r_2^{-\frac{1}{2}}h_2\right|^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\right] \tag{D.8}$$

$$\overset{(a)}{=}\int_{0<r_1<r_2<..<r_n<\infty}\left\{\mathcal{L}\left(\frac{1}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\mathcal{L}\left(\frac{\theta}{\sum_{i=1}^{n=2} r_i^{-1}}\right)f(\mathbf{r})\right\}\mathrm{d}\mathbf{r}, \tag{D.9}$$

where *(a)* uses the properties of Laplace transformation $\mathcal{L}\{f\}(s)=\mathrm{E}\left(e^{-sv}\right)$. Compared with the proof of Theorem 2 equation (B.6), $\mathcal{L}\left(\left(\sum_{i=1}^{n=2} r_i^{-1}\right)^{-1}\right)$ is an extra term. Now, this term can be derived as follows:

$$\mathcal{L}\{f\}(s) = \mathbb{E}\left(e^{-sv}\right) \tag{D.10}$$

$$= \mathbb{E}_{\mathbf{r},\mathbf{h}}\left(e^{-sr_2^{-1}h_2^2}\right) \tag{D.11}$$

$$\overset{(a)}{=} \mathbb{E}_{\mathbf{r}}\left(\frac{1}{1+sr_2^{-1}}\right) \tag{D.12}$$

$$\overset{(b)}{=} \exp\left[\int_{\mathbb{R}}\left(\frac{1}{1+sx^{-1}}-1\right)\lambda(x)\mathrm{d}x\right] = 1 \tag{D.13}$$

where *(a)* is from the moment-generating function of an exponential random variable $\mathrm{M}_x(t) = \frac{\lambda}{\lambda - t}, (t < \lambda)$; and *(b)* follows the definition of the PPP probability-generating function. Compared with the proof in Theorem 1, s corresponds to only the single team $r_2^{-1}h_2^2$ in the current case. The integral range $\mathbb{R}$ is only a point r_2, which means an integral from r_2 to r_2. Hence, the integral is equal to 0, and exp(0) = 1.

The derivation of the second term in equation (D.5) can be derived as in the proof of Theorem 3. Since equation (D.13) is equal to 1, and the left over terms in equation (D.9) $\exp\left(-\frac{\theta\sigma^2}{\sum_{i=1}^{n=2} r_i^{-1}}\right)\mathcal{L}\left(\frac{\theta}{\sum_{i=1}^{n=2} r_i^{-1}}\right)$ can also be derived similarly as in the proof of Theorem 1, $\mathbb{P}(\mathrm{RLF},\mathrm{CA})$ can be found similarly by combining the results of Theorems 2 and 3 with equation (D.6) . That is to say, for the n = 2 case, the results of Theorem 3 subtracted from the results of Theorem 2 gives the derivation of $\mathbb{P}(\mathrm{RLF},\mathrm{CA})$. The final step is to divide $\mathbb{P}(\mathrm{RLF},\mathrm{CA})$ with the handover probability, which completes the proof.

If the CA probability is defined with the SINR metric larger than the threshold β, then a similar method as used for the SINR metric can be easily applied to the integral expression shown for Figure 4.5.

LIST OF PUBLICATIONS AND PAPERS UNDER REVIEW

LIST OF PUBLICATIONS AND PAPERS UNDER REVIEW

Publications

[1] Shuang Feng, Jie Yang, and Hyuck M. Kwon, "Blind relay network with viterbi detection," *IEEE Military Communications Conf.*, Baltimore, MD, October 6–8, 2014.

[2] Jie Yang, Kanghee Lee, Shuang Feng, and Hyuck M. Kwon, "Spreading sequence design for partial connectivity relay network," IEEE 9th Vehicular Technology Conference (VTC), Korea, May 18–21, 2014.

[3] Kanghee Lee, Hyuck M. Kwon, Wenhao Xiong, Hyunggi Kim, Shuang Feng, Hyuncheol Park, and Yong H. Lee, "Two-level MMSE relay strategy for an AF wireless relay network," 50th Allerton Conference on Communication, Control, and Computing, University of Illinois at Urbana-Champaign, IL, October 1–5. 2012.

Papers under Review

[1] Shuang Feng, Hyuck M. Kwon, and Amitav Mukherjee, "Cell association attack via reference signal spoofing in multi-cell wireless networks," submitted to *IEEE Transactions on Communications*, February 20, 2016.

[2] Shuang Feng, Hyuck M. Kwon, and Khanh Pham, "Exact symbol error rate of frequency-hopped MPSK under Rician fading and partial band tone jamming," submitted *to IEEE Transactions on Aerospace and Electronic Systems*, March 14, 2016.

[3] Matthew Hannon, Shaung Feng, Hyuck M. Kwon, and Khanh Pham, "Channel statistics-dependent frequency hopping," submitted to *IEEE Transactions on Communications*, February 18, 2016.

[4] Shuang Feng, Hyuck M. Kwon, and Amitav Mukherjee, "Stochastic Geometry Analysis of Reference Signal Spoofing Attack in Wireless Cellular Networks," submitted to *IEEE Global Communications Conference*, April 9, 2016.