氏　　名	Zhang Yuanyu
学　位　名	博士（システム情報科学）
学位記番号	第３４号
学位授与年月日	平成２９年３月２３日
学位論文題目	Physical Layer Security Performance Study for Wireless Networks with Cooperative Jamming
論文審査委員	主査　姜　暁鴻
	副査　藤野　雄一
	副査　稲村　浩
	副査　和田　雅昭

論　文　要　旨

Due to the rapid development of wireless communication technology and widespread proliferation of wireless user equipment, wireless networks become indispensable for lots of applications in daily life. The broadcast nature of wireless medium makes information exchange in such networks vulnerable to eavesdropping attacks from malicious eavesdroppers, resulting in network security one of the major concerns for system designers. Physical layer (PHY) security has been proposed as one promising technology to provide security guarantee for wireless communications, owing to its unique advantages over traditional cryptography-based mechanisms, like an everlasting security guarantee and no need for costly secret key distribution/management and complex encryption algorithms. This thesis therefore focuses on the PHY security performance study for wireless networks with cooperative jamming (a typical PHY security technique), where non-transmitting helper nodes generate jamming signals to counteract eavesdropping attacks.

We first explore the PHY security performances of small-scale wireless networks with non-colluding (i.e., independently-operating) eavesdroppers, for which we study the eavesdropper-tolerance capability (ETC) of a two-hop wireless network with one source-destination pair, multiple relays and multiple non-colluding eavesdroppers. We consider two relay selection schemes to forward the packets from the source to the destination, i.e., random relaying and opportunistic relaying. For both relaying schemes,

we first derive the secrecy outage probability (SOP) and transmission outage probability (TOP) of the network by applying the classical Probability Theory. We then determine the ETC of the network by solving an optimization problem that aims to maximize the number of eavesdroppers that can be tolerated under a certain SOP constraint and a certain TOP constraint. Finally, we present extensive simulation and numerical results to demonstrate the validity of the theoretical analysis and also to illustrate our theoretical findings.

We then investigate the PHY security performances of small-scale wireless networks with colluding (i.e., cooperatively-operating) eavesdroppers, for which we study the SOP performance of a two-hop wireless network with one source-destination pair, multiple relays and multiple colluding eavesdroppers. Based on the classical Probability Theory, we first conduct analysis on the SOP of the simple non-colluding case. For the SOP analysis of the more hazardous M-colluding scenario, where any M eavesdroppers can combine their observations to decode the message, the techniques of Laplace transform, keyhole contour integral, and Cauchy Integral Theorem are jointly adopted to work around the highly cumbersome multifold convolution problem involved in such analysis, such that the related signal-to-interference ratio modeling for all colluding eavesdroppers can be conducted and thus the corresponding SOP can be analytically determined. Finally, simulation and numerical results are provided to demonstrate the validity of the theoretical analysis also to illustrate our theoretical findings.

Finally, we examine the cooperative jamming design issue in large-scale wireless networks. Towards this end, we propose a friendship-based cooperative jamming scheme to ensure secure communications in a finite Poisson network with one source destination pair, multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through three location-based policies. To understand both the security and reliability performances of the proposed jamming scheme, we first model the sum interference at any location in the network by deriving its Laplace transform under two typical path loss scenarios. With the help of the interference Laplace transform results, we then derive the exact expression for the TOP and determine both the upper and lower bounds on the SOP, such that the overall outage performances of the proposed jamming scheme can be depicted. Finally, we present extensive numerical results to validate the theoretical

analysis of TOP and SOP and also to illustrate the impacts of the friendship-based cooperative jamming on the network performances.

審査結果の要旨

This thesis focuses on the fundamental physical layer (PHY) security performance study for wireless networks with the security technique of cooperative jamming. More specifically, this thesis conducts the studies on: 1) the PHY security performance of small-scale wireless networks with non-colluding eavesdroppers, 2) the PHY security performance of small-scale wireless networks with colluding eavesdroppers, and 3) the cooperative jamming design for large-scale wireless networks. In the first study, this thesis presents an attempt on the analysis of eavesdropper-tolerance capability of two-hop wireless networks under two relaying schemes (i.e., random and opportunistic relaying). In the second study, this thesis tackles the technical challenge of exactly modeling the distribution of aggregate signal-to-interference ratio of colluding eavesdroppers and provides analysis on the secrecy outage probability (SOP) of two-hop wireless networks with colluding eavesdroppers. In the last study, this thesis proposes a friendship-based cooperative jamming scheme for Poisson Networks and studies the related performances of SOP and transmission outage probability.

・論文の構成

Chapter 1 Introduction
Chapter 2 Related Works
Chapter 3 Physical Layer Security Performance Study of Small-Scale Wireless Networks with Non-Colluding Eavesdroppers
Chapter 4 Physical Layer Security Performance Study of Small-Scale Wireless Networks with Colluding Eavesdroppers
Chapter 5 Cooperative Jamming Design in Large-Scale Wireless Networks
Chapter 6 Conclusion
Appendices A, B, C.1, C.2, C.3, C.4

・研究目的の妥当性，従来の手法との比較においての有意性，および理論・実験手法の新規性

This thesis studied the fundamental security performance of wireless networks with physical layer (PHY) security technology. More specifically, this thesis focuses on the PHY security technique of cooperative jamming and conducts the studies of: 1) the PHY security performance of

small-scale wireless networks with non-colluding eavesdroppers, 2) the PHY security performance of small-scale wireless networks with colluding eavesdroppers, and 3) the cooperative jamming design for large-scale wireless networks.

In the first work, we study the eavesdropper-tolerance capability (ETC) of two-hop wireless networks. Despite much work has been done on this topic, the exact ETC of such networks remains uninvestigated. This thesis represents a first attempt to address this issue. By applying the classical Probability Theory, this thesis first provides the exact models for the transmission outage probability (TOP) and secrecy outage probability (TOP), then formulates the ETC as an optimization problem under the constraints of SOP and TOP, and finally obtains the exact ETC result by solving the optimization problem based on both the Stochastic Ordering theory and method of proof by contradiction.

In the second work, we study the SOP performance of two-hop wireless networks with colluding eavesdroppers. Despite much work on this topic, the SOP study with the consideration of cooperative jamming technique remains an open problem due to the technical challenge of exactly modeling the distribution of the aggregate signal-to-interference ratio of colluding eavesdroppers. We conduct such a SOP study with the consideration of cooperative jamming and tackle the above technical challenge by jointly applying the mathematical tools of Laplace transform, keyhole contour integral and Cauchy Integral Theorem.

In the last work, we consider the cooperative jamming design issue with the consideration of social relationships. Available works on this topic suffer from two main limitations: they usually adopt some over-simplified social relationship models (e.g., social trust and social tie) that fail to capture the geometry-based social behaviors; and they usually consider some over-simplified network scenarios with only one eavesdropper and several jammers (i.e., nodes that send jamming signals to suppress eavesdroppers). To address these limitations, we consider a more general friendship model and a large-scale wireless network with the Poisson Point Process. We propose a friendship-based cooperative jamming scheme that selects nodes that are friends of the transmitter as jammers, and also propose three jammer selection policies based on the geometry properties of the network. Based on the theory of Stochastic Geometry, we conduct studies on the TOP and SOP performances of the concerned large scale networks with the proposed cooperative jamming scheme.

・得られた知見のシステム情報科学の分野における意義

The results of this thesis provide the following insights.

1. The studies conducted in this thesis will be helpful for the design of secure wireless networks. The results in the ETC study illustrate the tradeoffs among security, reliability and ETC of a wireless network, which can serve as a guideline for the design of wireless networks with various performance requirements.

2. The results in the SOP study under colluding eavesdroppers shop the impact of eavesdropper collusion on network security, and thus shed light on the design of new PHY security techniques to effectively counteract such more hazardous eavesdropping attacks.
3. The results in this thesis help us to understand the potentials of cooperative jamming tschnique in counteracting the eavesdropping attacks. In particular, the proposed friendship-based cooperative jamming scheme could open a new approach for the design of more powerful cooperative jamming schemes by fully exploring not only the social behavior but also other inherent properties of wireless networks.