氏名	呉　恵恵
学位名	博士（システム情報科学）
学位記番号	第５７号
学位授与年月日	令和３年９月１６日
学位論文題目	On Achieving Covertness and Secrecy in Wireless Communications
論文審査委員	主査　姜　暁鴻
	副査　稲村　浩
	副査　藤野　雄一
	副査　和田　雅昭

論文要旨

Due to the rapid development of information and communication technologies and widespread proliferation of wireless user equipment, an enormous amount of sensitive and confidential information is transmitted via wireless channels, so wireless communications have become the most fundamental communication technology indispensable in our daily life. The broadcast nature of wireless medium makes the exchange of confidential information in such communication vulnerable to various security attacks, which brings security vulnerabilities and threats in wireless information transmission. Therefore, the fundamental research of wireless communication security is of great importance for the development of secure network communication, information security and communication privacy. It is notable that in modern secure wireless communication applications, covertness and secrecy serve as two typical properties. Covertness concerns with the protection of wireless communication from detection attacks that attempt to detect the existence of the communication, while secrecy deals with the protection of wireless communication from eavesdropping attacks which manage to intercept the information conveyed by the communication. With the wide applications of secure wireless communication, how to ensure both the covertness and secrecy of such communication has become an increasingly urgent demand. Thanks to the rapid progress of information and communication technologies, physical layer security (PLS) technique is now regarded as

a highly promising approach to counteract the detection and eavesdropping attacks and thus to ensure the covertness and secrecy properties of wireless communications. This thesis therefore focuses on exploring a new secure wireless communication paradigm where the PLS technology is applied to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed.

We first investigate the covertness guarantee for a two-way two-hop wireless communication system, where two sources wish to covertly exchange information through a relay against the detection from a detector, i.e., a malicious node that attempts to detect the existence of communication between the two sources. We consider various scenarios regarding the detector's prior knowledge about the relay, the sources/relay's prior knowledge about the detector, as well as different relaying patterns, and then propose the covertness strategy to resist the detector's detection for each scenario. To depict the performance limit of the system, we derive the scaling law result for the covert throughput of the system for each scenario, i.e., the maximum number of bits that the two sources can exchange subject to a constraint on the detection probability of the detector. Our results indicate that the covert throughput of the concerned system follows the well-known square root scaling law, which is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledges of the sources/relay and detector.

We next consider the covertness and secrecy guarantees in wireless communications, and explore a new secure wireless communication paradigm where the critical covertness and secrecy properties are jointly guaranteed under the passive detection/eavesdropping attacks by applying the PLS technique. We first provide theoretical modeling for covertness outage probability (COP), secrecy outage probability (SOP) and transmission probability (TP) to depict the covertness, secrecy and transmission performances of the paradigm. To understand the fundamental security performance under the new paradigm, we then define a new metric - covert secrecy rate (CSR), which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP. We further conduct detailed theoretical analysis to identify the CSR under various scenarios determined by the detector-eavesdropper relationships and the secure transmission schemes adopted by transmitters. We also provide numerical results to illustrate the achievable performances under the new secure communication paradigm.

Finally, we extend the secure wireless communication paradigm to the active attacker scenario where attackers can perform jamming and detection/eavesdropping simultaneously. To understand the covertness, secrecy and transmission performances in the active attacker scenario, we first provide theoretical modeling for covertness outage probability, secrecy outage probability and transmission probability, respectively. Based on the theoretical model, we further conduct detailed theoretical analysis to identify the CSR in this scenario under power control (PC)-based and artificial noise (AN)-based transmission schemes adopted at transmitters. Extensive numerical results are then presented to validate the theoretical analysis, reveal the impact of active attackers on the CSR under each transmission scheme and illustrate the achievable performances in the secure wireless communication paradigm under the active attacker scenario.

審査結果の要旨

This thesis focuses on exploring a new secure wireless communication paradigm where the physical layer security (PLS) technology is applied to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed. More specifically, the thesis first investigates the covertness guarantee in a two-way two-hop wireless communication system, derives the corresponding scaling law result for the covert throughput of the system. The thesis then explores a new secure wireless communication paradigm where the critical covertness and secrecy properties are jointly guaranteed under the passive detection/eavesdropping attacks, and provides detailed theoretical analysis on the covert secrecy rate (CSR) under various scenarios determined by the detector-eavesdropper relationships and the secure transmission schemes adopted by transmitters. Finally, the thesis extends the secure wireless communication paradigm to the active attacker scenario where attackers can perform jamming and detection/eavesdropping simultaneously.

・論文の構成

Chapter 1 Introduction

Chapter 2 Related Works

Chapter 3 Covertness Guarantee in Two-Way Relay Wireless Communications

Chapter 4 Covertness and Secrecy Guarantees in Wireless Communications with Passive Attackers

Chapter 5 Covertness and Secrecy Guarantees in Wireless Communications with Active Attackers

Chapter 6 Conclusion

・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 explores a new secure wireless communication paradigm where the physical layer security (PLS) technology is applied to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed.

This thesis first investigates the covertness guarantee in a two-way two-hop wireless communication system, where two sources wish to covertly exchange information through a relay against the detection from a detector. For achieving covertness in the system, covertness strategies are proposed based on the detector's prior knowledge about the relay, the sources/relay's prior knowledge about the detector and different relaying patterns. To depict the performance limit, the scaling law results are derived for the covert throughput of the system.

This thesis further explores a new secure wireless communication paradigm where the critical covertness and secrecy properties are jointly guaranteed under the passive detection/eavesdropping attacks by applying the PLS technique. To depict the covertness, secrecy and transmission performances of the paradigm, theoretical models are provided for covertness outage probability (COP), secrecy outage probability (SOP) and transmission probability (TP). To understand the fundamental security performance under the new paradigm, a new metric - covert secrecy rate (CSR) is defined, which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP. The detailed theoretical analysis is conducted to identify the CSR under various scenarios determined by the relationships between detector and eavesdropper and the secure transmission schemes adopted by transmitters. Finally, this thesis extends the new secure wireless communication paradigm to the active attacker scenario where attackers can perform jamming and detection/eavesdropping simultaneously. The work in this thesis represents the first attempt on investigating the joint covertness and secrecy guarantees in wireless communications.

・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 valuable insights.

1. The work of this thesis can inspire the future studies on the joint guarantees of the critical covertness and secrecy properties in wireless communications.
2. It is expected that the theoretical models developed for the new secure wireless communication paradigms could be helpful for exploring the performance in other network scenarios as well.