氏　　名	何　吉
学　位　名	博士（システム情報科学）
学位記番号	第４８号
学位授与年月日	令和２年９月１７日
学位論文題目	Secure Communication Protocol Design for Buffer-Aided Relaying Systems
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

With the rapid evolution of information and communication technologies, more complicated network architectures and more advanced network topologies and access techniques are exploited to support the unprecedented growth of data traffic in the 5G communication. This fact, therefore, leads to an enormous amount of sensitive and confidential information transmitted via the wireless channels, e.g., financial data, medical records, and customer files. How to guarantee information security has attracted increasing concerns from both academia and industry recently. 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 design of communication protocols with PHY security techniques to secure a buffer-aided relaying system, where relay buffers are adopted to help the transmission of information.

We first investigate the secure communication in a two-hop cooperative wireless network, where a buffer-aided relay helps forward data from the source to destination, and a passive eavesdropper attempts to intercept data transmission from both the source and relay. To ensure the transmission security and communication quality of

service (QoS) of the system, we design the novel communication protocols for two cases that the instantaneous channel state information is available or unavailable at the source node. For the evaluation of system performance, we then derive the closed-form expressions of end-to-end secrecy outage probability, system throughput and secrecy throughput, respectively. Based on the theoretical performance analysis, we further explore the performance optimization issues, revealing the insightful tradeoffs between the transmission security and QoS. An iterative algorithm is developed to identify the optimal setting of link selection parameters, which is helpful for the practical configuration of link selection policies to satisfy various system performance requirements. Finally, we conduct simulations to validate our theoretical performance analysis, and also provide extensive numerical results to illustrate the efficiency of the proposed communication protocols for ensuring secure communication in the buffer-aided relaying system.

We then investigate the secure communication in a wireless relaying system where the packet lifetime is limited, multiple buffer-aided relays help the source forward packets to the destination, and a passive eavesdropper attempts to wiretap the transmissions over both hops. To guarantee the end-to-end transmission security and timeliness in the system, we design a novel security/delay-aware communication protocol that grants transmission nodes different priorities for packet delivery based on the wireless channel state, real-time buffer state, and packet delay requirement. To evaluate the performance of the proposed protocol, we then develop a Markov chain-based theoretical framework to fully characterize the packet occupancy process in the relay buffers. With the help of this framework, we further derive under two typical fading channel cases the closed-form expressions for three fundamental system performance metrics, namely the reliable outage probability, packet discarding probability and achievable secrecy throughput. Finally, we present extensive simulation and numerical results to validate our theoretical results, as well as to demonstrate the efficiency of the proposed protocol for ensuring secure and timely communication in the buffer-aided relaying system. The results indicate that the proposed communication protocol can be flexibly controlled according to different lifetime constraints to satisfy different performance requirements of the system.

審査結果の要旨

This thesis focuses on the study of secure communication protocol design for buffer-aided relaying (BAR) systems. More specifically, this thesis conducts the studies on: 1) the design of secure communication protocol for BAR systems, 2) the design of security/delay-aware communication for BAR systems. In the first study, this thesis proposes the secure communication protocols for two transmission modes (i.e., adaptive-rate transmission and fixed-rate transmission), respectively, to satisfy various quality of service (QoS) requirements (i. e., end-to-end secrecy outage probability, throughput and secrecy throughput). In the second study, this thesis proposes a novel security/delay-aware communication protocol to ensure the security and timeliness of data transmission for BAR system, and provides analysis on the reliable outage probability, packet discarding probability and achievable secrecy throughput of the proposed protocol.

・論文の構成

Chapter 1 Introduction
Chapter 2 Related Works
Chapter 3 Secure Communication Protocol for Buffer-Aided Relaying Systems
Chapter 4 Security/Delay-Aware Communication Protocol for Buffer-Aided Relaying Systems
Chapter 5 Conclusion
Appendices A, B

・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 the PHY security techniques of buffer-aided relaying (BAR) and cooperative jamming to design: 1) Secure communication protocol for BAR systems; 2) Security/delay-aware communication protocol for BAR systems.

In the first work, we propose two communication protocols to secure the transmission in a BAR system under adaptive-rate and fixed-rate transmission models. Despite some initial works on this topic, how to conduct link selection to reconcile the transmission security with the consideration of communication quality of service (QoS) guarantee is still an open issue. As a step forward in this direction, this thesis investigates the important trade-off issue between transmission security and communication QoS, and designs the corresponding secure communication protocols. The theoretical framework based on the optimization theory is also established for performance optimization of the proposed communication protocols.

In the second work, we propose a novel security/delay-aware communication protocol for a BAR system. It is worth noting that available works are based on the ideal assumption that the

packet lifetime is unlimited. However, to support the critical delay-sensitive applications, it is of great importance to further investigate the protocol design and performance analysis for BAR networks with the constraint of limited packet lifetime. Hence, we propose a communication protocol to guarantee both the security and timeliness of packet transmission in a BAR network with limited packet lifetime constraint. Furthermore, a Markov chain-based theoretical framework is developed to fully characterize the packet occupancy process in buffers such that the overall performance of the proposed protocol can be theoretically analyzed.

・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. It is expected that the results in this study can shed new insights on the design of communication protocol to achieve secure communication in wireless networks while satisfying the various QoS requirements.

2. The novel theoretical frameworks developed in this thesis could be helpful for exploring the performance in other network scenarios as well.