氏　　名	廖　雪宁
学　位　名	博士（システム情報科学）
学位記番号	第３９号
学位授与年月日	平成３０年９月２０日
学位論文題目	Physical Layer Security Performance Study for Two-Hop Wireless Networks with Buffer-Aided Relay Selection
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

As wireless communication technologies continue to evolve rapidly, an unprecedented amount of sensitive information, such as financial data, physical health details and personal profile data, are transmitted through various wireless networks. However, the broadcast nature of wireless medium makes it difficult to shield these sensitive information from unauthorized users (eavesdroppers), and thus securing wireless communication is becoming an increasingly urgent demand. 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 tow-hop wireless networks with buffer-aided relay selection (a typical PHY security technique), where relay buffers will be adopted to help the transmission of the message.

We first investigate the security-delay trade-off of the buffer-aided relay selection scheme in a two-hop wireless network with multiple randomize-and-forward (RF) relays. To evaluate the security and delay performances of the system, we derive analytical expressions for the end-to-end (E2E) secure transmission probability (STP) and the expected E2E delay under both perfect and partial eavesdropper channel state information (CSI) cases. These analytical expressions help us to explore the inherent

trade-off between the security and delay performances of the concerned system. In particular, the results in this paper indicate that: 1) the maximum E2E STP increases as the constraint on the expected E2E delay becomes less strict, and such trend is more sensitive to the variation of the number of relays than that of the relay buffer size; 2) on the other hand, the minimum expected E2E delay tends to decrease when a less strict constraint on E2E STP is imposed, and this trend is more sensitive to the variation of the relay buffer size than that of the number of relays.

We then investigate the PHY security performances of two-hop wireless networks with multiple DE relays, for which we extend the buffer-aided relay selection with RF relays and propose a new buffer-aided relay selection scheme to resist the eavesdropper's combining decoding in two-hop wireless networks with DF relays. To validate the efficiency of the new scheme, a theoretical framework is developed to analyze the E2E delivery process of a packet. Based the theoretical framework, we derive the closed form of the security and delay performances in terms of the E2E STP and the expected E2E delay. Then, extensive numerical results are conducted to validate the efficiency of the new buffer-aided relay selection scheme, and the security-delay trade-off issue is also studied to explore the achievable E2E STP (expected E2E delay) region under a given expected E2E delay (E2E STP) constraint. Finally, comparisons are made between the new buffer-aided relay selection scheme and the Max-Ratio scheme, results show that our new scheme outperforms the Max-Raito buffer-aided relay selection scheme in terms of the E2E STP.

審査結果の要旨

This thesis focuses on the fundamental physical layer (PHY) security performance study for two-hop wireless networks with the security technique of buffer-aided relay selection. More specifically, this thesis conducts the studies on: 1) the PHY security performance of buffer-aided relay selection scheme for two-hop wireless networks with randomize-and-forward (RF) relays, where different codebooks are adopted at the source and relay nodes respectively, and 2) the PHY security performance of buffer-aided relay selection scheme for two-hop wireless networks with decode-and-forward (DF) relays, where the same codebook is adopted at the source and the relay nodes. In the first study, this thesis presents an attempt on the analysis of security-delay trade-off issue for two-hop wireless networks with RF relays. In the second study, this thesis aims to propose new buffer-aided relay selection scheme for two-hop wireless networks DF relays and provides

analysis on the E2E secure transmission probability (STP) and the expected E2E delay of the proposed scheme.

・論文の構成

Chapter 1 Introduction

Chapter 2 Related Works

Chapter 3 Physical Layer Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-hop Wireless Networks with RF Relays

Chapter 4 Physical Layer Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-hop Wireless Networks with DF Relays

Chapter 5 Conclusions

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 studies the fundamental security performances of wireless networks with physical layer (PHY) security technology. More specifically, this thesis focuses on the PHY security technique of buffer-aided relay selection and conducts the studies of: 1) the PHY security performance of buffer-aided relay selection for two-hop wireless networks with randomize-and-forward (RF) relays, 2) the PHY security performance of buffer-aided relay selection for two-hop wireless networks with decode-and-forward (DF) relays.

In the first work, we consider the security-delay issue of the buffer-aided relay selection scheme in a two-hop wireless network with RF relays. Available works on this topic suffer from two main limitations: they usually consider the security of a single link to validate the security performance, which fails to capture end-to-end (E2E) performance of the network; and they rarely consider the packet delay issue. To address these limitations, we consider in this work the E2E security and delay performances of the concerned network. To validate the security and delay performances of the network, a theoretical framework is first developed based on the Markov chain theory to depict the E2E delivery process of a tagged packet. With the help of the framework and the queuing theory, analytical expressions of the E2E secure transmission probability (STP) and the expected E2E delay are then derived. Finally, extensive numerical results are conducted to examine the effect of network parameters on the network performances, and explore the security-delay trade-off in terms of the E2E STP and the expected E2E delay.

In the second work, we study the PHY security performance of two-hop wireless networks with DF relays. Despite much work on this topic, the PHY security performances study with the consideration of buffer-aided relay selection technique for wireless network with DF relays remains

an open problem. We consider a two-hop wireless network with DF relays and propose a new buffer-aided relay selection scheme to resist the combining decoding of the signals by eavesdroppers. With help of the Markov chain theory, queuing theory and the probability theory, closed form expressions of the E2E STP and the expected E2E delay are first derived. Then, extensive numerical results are conducted to validate the efficiency of the new buffer-aided relay selection scheme over available ones.

・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 E2E security-delay study illustrate the tradeoffs between security and delay 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 buffer-aided relay selection scheme study for networks with DF relays show the impact of eavesdropper's decoding strategy 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 buffer-aided relay selection technique in counteracting the eavesdropping attacks. In particular, the proposed buffer-aided relay selection scheme could open a new approach for the design of more powerful buffer-aided relay selection schemes by fully considering not only the link quality but also other inherent properties of wireless networks.