氏名	李　笑晨
学位名	博士（システム情報科学）
学位記番号	第５０号
学位授与年月日	令和２年９月１７日
学位論文題目	Secure Protocol Design for Mobile Ad Hoc Networks
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 technology evolves continuously, mobile ad hoc networks (MANETs) become highly appealing for supporting lots of critical applications in daily life. However, due to the open nature of wireless medium, wireless communication is vulnerable to eavesdropping attacks by unauthorized receivers (eavesdroppers), posing a great threat to the security of MANETs. Recently, a promising security approach, called physical layer (PHY) security, has been proposed to provide a strong security guarantee by exploiting the inherent physical properties of wireless channels, such as noise, interference and time-varying fading. Compared to the cryptography-based methods, the PHY security technology can provide an everlasting security guarantee without the need of costly secret key management/distribution and complex cryptographic protocols. This thesis therefore focuses on the secure protocol design and performance analysis of MANETs based on the typical PHY security techniques (i.e., secrecy guard zone, cooperative jamming, artificial noise).

For cell-partitioned MANETs, we first consider a scenario where each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone (SGZ). For this scenario, we propose an SGZ-based secure transmission protocol, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its SGZ. To understand the security performance of the SGZ-based secure transmission protocol, we first derive two basic secure transmission probabilities of the network by applying the classical Probability Theory. We then obtain the exact secrecy throughput capacity of the concerned network under the SGZ-based secure transmission protocol based on the analysis of two secure transmission probabilities. Finally, we present extensive simulation and numerical results to validate our theoretical analysis and also to illustrate the impacts of the SGZ-based secure transmission protocol on the secrecy throughput capacity performance.

For cell-partitioned MANETs, we then consider a new scenario where each transmitter can know the exact locations of eavesdroppers in its transmission range. For this scenario, we propose a cooperative jamming (CJ) based secure transmission protocol, which allows non-transmitting legitimate nodes to send artificial noise to suppress eavesdroppers. The transmission of a selected transmitter will be conducted only if all eavesdroppers in the transmission range of the transmitter are suppressed. To understand the security performance of the proposed secure transmission protocol, based on the classical Probability Theory, we first conduct analysis on two basic secure transmission probabilities of the network. We then derive the exact analytical expression for the secrecy throughput capacity of the network under the CJ-based secure transmission protocol. Finally, extensive simulation and numerical results are provided to verify the theoretical analysis also to illustrate the impacts of the CJ-based secure transmission protocol on the secrecy throughput capacity performance.

For continuous MANETs, by combining PHY security techniques and the conventional Aloha protocol, we propose two secure Aloha protocols, i.e., artificial noise (AN)-based Aloha protocol and secrecy guard zone (SGZ)-based Aloha protocol, to ensure secure medium access for legitimate transmitters. In the AN-based Aloha protocol, all potential transmitters (i.e., transmitters scheduled by the conventional Aloha protocol) are allowed to be active and each active transmitter injects AN into its transmitted signals to confuse eavesdroppers. In the SGZ-based protocol, each potential transmitter has an SGZ, a circle centered at itself, and only the potential transmitters whose SGZ contains no eavesdroppers are allowed to be active. To understand both the security and reliability performance of the proposed secure Aloha protocols, we first apply tools from Stochastic Geometry to derive analytical expressions for the connection outage probability (COP) as well as the upper and lower bounds on the secrecy outage probability (SOP) of the considered network under both the AN-based Aloha protocol and SGZ-based Aloha protocol. Based on the COP and SOP, we then derive the secrecy transmission capacity of the network under both protocols. Finally, we provide simulation/numerical results to validate the theoretical analysis of COP and SOP and also to show the impacts of secure Aloha protocols on the secrecy transmission capacity performance.

審査結果の要旨

This thesis focuses on the study of the secure protocol design for mobile ad hoc networks (MANETs) with physical layer (PHY) security technologies. For cell-partitioned MANETs, this thesis proposes two secure protocols based on the PHY security technology, i.e., protocols based on secrecy guard zone or cooperative jamming. To understand the security performance of the proposed protocols, this thesis analyzes the exact secrecy throughput capacity of the concerned network under both secure protocols by applying the classical Probability Theory. For continuous MANETs, by combining PHY security techniques and the conventional Aloha protocol, this thesis proposes two secure protocols, i.e., artificial noise based protocol and secrecy guard zone based protocol, to ensure secure medium access of legitimate transmitters. To understand the security performance of the proposed protocols, this thesis applies tools from Stochastic Geometry to analyze the secrecy transmission capacity of MANETs under both protocols.

・論文の構成

Chapter 1 Introduction

Chapter 2 Related Works

Chapter 3 Secrecy Guard Zone based Secure Protocol in Cell-Partitioned MANETs

Chapter 4 Cooperative Jamming based Secure Protocol in Cell-Partitioned MANETs

Chapter 5 Secure Protocols based on Artificial Noise and Secrecy Guard Zone in Continuous MANETs

Chapter 6 Conclusion

Appendices

・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 secure protocol design and fundamental security performance analysis of mobile ad hoc networks (MANETs) with physical layer (PHY) security technologies.

For cell-partitioned MANETs, we propose two secure protocols based on the PHY security technology, i.e., protocols based on secrecy guard zone or cooperative jamming. To understand the security performance of the proposed protocols, we analyze the exact secrecy throughput capacity

(STC) of the concerned network under both secure protocols by applying the classical Probability Theory. Despite much work on the scaling law results of MANET STC, the exact STC study of such networks remains an open problem. Our work, for the first time, investigates the exact STC of a cell-partitioned MANET with group-based scheduling scheme from the PHY security perspective.

For continuous MANETs, by combining PHY security techniques and the conventional Aloha protocol, we propose two secure protocols, i.e., artificial noise based protocol and secrecy guard zone based protocol, to ensure secure medium access of legitimate transmitters. Available works simple adopted Aloha as the transmission protocol, while they ignored the crucial issue of protecting the transmissions from eavesdropping. To address this issue, this thesis therefore combines two widely-used PHY security schemes, i.e., artificial noise injection and secrecy guard zone, with the Aloha protocol to propose novel secure protocols and then applies tools from Stochastic Geometry to analyze the secrecy transmission capacity performance of MANETs under both protocols.

・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 results obtained in this thesis can inspire subsequent theoretical researches on the exact study of the fundamental and important secrecy throughput capacity issue in mobile ad hoc networks.

2. It is expected that the proposed secure protocols and related theoretical models will provide an important guideline for the design of flexible and cost-effective secure protocols for wireless communications.