氏　　名	張　品昌
学　位　名	博士（システム情報科学）
学位記番号	第４５号
学位授与年月日	令和２年３月２３日
学位論文題目	Physical Layer Authentication for 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

Authentication serves as a critical property of secure communication to verify the identity of the entity involved in the communication. With the rapid development of wireless technologies, the flexible and cost-effective authentication is becoming an increasingly urgent demand for future wireless networks. This is because on one hand, the open and broadcast natures of wireless communications make wireless networks more vulnerable to spoofing attacks, where an unauthorized transmitter may impersonate as a legitimate one. On the other hand, with the wide deployment of Internet of things (IoT) and continuous evolvement of wireless technologies toward the fifth generation (5G) and beyond networks, it is foreseeable that future wireless networks will be consisted of a large number of heterogeneous devices, making cryptographic authentication techniques in wireless networks a challenging issue. Recently, physical layer authentication techniques, which exploit intrinsic and unique features of physical layer for authentication, has drawn a considerable attention to enhance and complement conventional cryptography-based authentication solutions. This thesis focuses on the study of physical layer authentication for wireless communications.

We first explore the channel-based authentication solution taking hardware impairments into account and thus propose a new channel-based authentication scheme for massive multiple input-multiple-output (MIMO) systems with non-ideal hardware.

In particular, based on signal processing theory, we formulate channel estimation under hardware impairments and determine error covariance matrix to assess the quantity caused by hardware impairments on authentication performance. With the help of hypothesis testing and matrix transformation theories, we are able to derive exact expressions for the probabilities of false alarm and detection under different channel covariance matrix models. Extensive simulations are carried out to validate theoretical results and illustrate the efficiency of the proposed scheme. Impacts of system parameters on performance are revealed as well.

We then propose a novel authentication solution which not only exploits location-specific wireless channels but also utilizes transmitter-specific hardware impairments for authentication, and thus propose an improved channel-based scheme jointly utilizing channel gain and phase noise in heterogeneous MIMO systems. Three properties of the proposed scheme: covertness, robustness, and security, are analyzed in detail. By using a maximum-likelihood estimator (MLE) and extended Kalman filter (EKF), we estimate channel gains and phase noise, and formulate variances of estimation errors. We also quantize the temporal variations of channel gains and phase noise through the developed quantizers. Based on theories of hypothesis testing and stochastic process, we then derive the closed-form expressions for false alarm and missed detection probabilities with the consideration of quantization errors. Simulations are carried out to validate theoretical results of the two probabilities. Based on theoretical models, we further demonstrate that the proposed scheme makes it possible for us to flexibly control performance by adjusting parameters (such as channel gain threshold, phase noise threshold, and decision threshold) to achieve a required authentication performance in specific MIMO applications.

Finally, we focus on the study of physical layer authentication in a dual-hop wireless network with an untrusted relay and propose an end-to-end (E2E) channel-based authentication scheme. This scheme fully utilizes wireless channel feature (i.e., channel impulse response in the dimensions of amplitude and path delay), and adopts artificial jamming technique, so that it is not only resistant to impersonate attack from an unauthorized transmitter but also resilient to replay attack from the untrusted relay. Theoretical analysis is conducted to derive expressions for false alarm and missed detection probabilities. Finally, numerical and simulation results are provided to illustrate both the efficiency of these theoretical results and the E2E performance of dual-hop wireless networks.

審査結果の要旨

This thesis focuses on the study of physical layer authentication for wireless communications. More specifically, this thesis conducts the studies on: 1) the channel-based authentication solution taking hardware impairments into account, 2) the authentication solution which not only exploits location-specific wireless channels but also utilizes transmitter-specific hardware impairments for authentication, and 3) an end-to-end (E2E) channel-based authentication scheme for a dual-hop wireless network with an untrusted relay. In the first study, this thesis proposes a new channel-based authentication scheme for massive multiple input-multiple-output (MIMO) systems with non-ideal hardware. In the second study, this thesis presents an improved channel-based scheme jointly utilizing channel gain and phase noise in heterogeneous MIMO systems. In the last study, this thesis designs an end-to-end (E2E) channel-based authentication scheme fully utilizing wireless channel feature (i.e., channel impulse response in the dimensions of amplitude and path delay).

・論文の構成

Chapter 1 Introduction
Chapter 2 Related Works
Chapter 3 End-to-End Physical Layer Authentication for Dual-Hop Wireless Networks
Chapter 4 Physical Layer Authentication for Massive MIMO Systems with Hardware Impairments
Chapter 5 Physical Layer Authentication Jointly Utilizing Channel and Phase Noise for MIMO Systems
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 physical layer authentication for wireless communications. More specifically, this thesis conducts the studies on: 1) the channel-based authentication solution taking hardware impairments into account, 2) the authentication solution jointly exploiting location-specific wireless channel gain and phase noise, and 3) the end-to-end (E2E) channel-based authentication solution in a dual-hop wireless network with an untrusted relay.

In the first work, we propose a new channel-based authentication scheme for massive multiple input-multiple-output (MIMO) systems with non-ideal hardware.

Based on signal processing theory, channel estimation under hardware impairments and error covariance matrix are derived. Exact expressions for the probabilities of false alarm and detection under different channel covariance matrix models are modeled analytically as well. Extensive numerical results are provided to validate theoretical results and illustrate the efficiency of this proposed scheme.

In the second work, we propose an improved channel-based authentication scheme jointly utilizing channel gain and phase noise in heterogeneous MIMO systems. Three properties of the proposed scheme: covertness, robustness, and security, are analyzed in detail. By using a maximum-likelihood estimator (MLE) and extended Kalman filter (EKF), we estimate channel gains and phase noise, and formulate variances of estimation errors. Based on theories of hypothesis testing and stochastic process, we then derive the closed-form expressions for false alarm and missed detection probabilities with the consideration of quantization errors.

In the last work, we focus on end-to-end (E2E) channel-based authentication solution, and propose a scheme which adopts artificial jamming technique and utilizes wireless channel feature (i.e., channel impulse response in the dimensions of amplitude and path delay), so it is not only resistant to impersonate attack from an unauthorized transmitter but also resilient to replay attack from the untrusted relay. Theoretical analysis is conducted to derive expressions for false alarm and missed detection probabilities. Finally, numerical and simulation results are provided to illustrate the efficiency of these theoretical results and the new authentication 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 physical layer authentication solutions. Our results show that flexible authentication performance control can achieved by adjusting system parameters, and these proposed schemes have the capability of satisfying different performance requirements for future emerging wireless networks.

2. The results in this thesis help us to understand the potential effects of multi-dimensional physical layer features (e.g., channel impulse response, channel frequency response, I/Q imbalance, carrier frequency offset, and phase noise) on authentication performance.

3. The results imply that these proposed authentication schemes and related theoretical

models will be useful for providing a guideline to devise the coping schemes against various attacks, as well as for understanding the fundamental authentication performance of multi-hop wireless networks.