Western Graduate&PostdoctoralStudies

Western University
Scholarship@Western

Electronic Thesis and Dissertation Repository

8-18-2020 9:00 AM

Intelligent Security Provisioning and Trust Management for Future Wireless Communications

He Fang, *The University of Western Ontario*

Supervisor: Wang, Xianbin, *The University of Western Ontario*
A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Electrical and Computer Engineering
© He Fang 2020

Follow this and additional works at: https://ir.lib.uwo.ca/etd

Part of the Systems and Communications Commons

Recommended Citation

Fang, He, "Intelligent Security Provisioning and Trust Management for Future Wireless Communications" (2020). *Electronic Thesis and Dissertation Repository*. 7313.
https://ir.lib.uwo.ca/etd/7313

This Dissertation/Thesis is brought to you for free and open access by Scholarship@Western. It has been accepted for inclusion in Electronic Thesis and Dissertation Repository by an authorized administrator of Scholarship@Western. For more information, please contact wlswadmin@uwo.ca.

Abstract

The fifth-generation (5G)-and-beyond networks will provide broadband access to a massive number of heterogeneous devices with complex interconnections to support a wide variety of vertical Internet-of-Things (IoT) applications. Any potential security risk in such complex systems could lead to catastrophic consequences and even system failure of critical infrastructures, particularly for applications relying on tight collaborations among distributed devices and facilities. While security is the cornerstone for such applications, trust among entities and information privacy are becoming increasingly important. To effectively support future IoT systems in vertical industry applications, security, trust and privacy should be dealt with integratively due to their close interactions. However, conventional technologies always treat these aspects separately, leading to tremendous security loopholes and low efficiency. Existing solutions often feature various distinctive weaknesses, including drastically increased latencies, communication and computation overheads, as well as privacy leakage, which are extremely undesirable for delay-sensitive, resource-constrained, and privacy-aware communications.

To overcome these issues, this thesis aims at creating new multi-dimensional intelligent security provisioning and trust management approaches by leveraging the most recent advancements in artificial intelligence (AI). The performance of the existing physical-layer authentication could be severely affected by the imperfect estimate and the variation of physical link attributes, especially when only a single attribute is employed. To overcome this challenge, two multi-dimensional adaptive schemes are proposed as intelligent processes to learn and track the all available physical attributes, hence to improve the reliability and robustness of authentication by fusing multiple attributes. To mitigate the effects of false authentication, an adaptive trust management-based soft authentication and progressive authorization scheme is proposed by establishing trust between transceivers. The devices are authorized by their trust values, which are dynamically evaluated in real-time based on the varying attributes, resulting in soft security and progressive authorization. By jointly considering security and privacy-preservation, a distributed accountable recommendation-based access scheme is proposed for blockchain-enabled IoT systems. Authorized devices are introduced as referrers for collaborative authentication, and the anonymous credential algorithm helps to protect privacy. Wrong recommendations will decrease the referrers reputations, named as accountability. Finally, to secure resource-constrained communications, a lightweight continuous authentication scheme is developed to identify devices via their pre-arranged pseudo-random access sequences. A device will be authenticated as legitimate if its access sequences are identical to the pre-agreed unique order between the transceiver pair, without incurring long latency and high overhead.

Applications enabled by 5G-and-beyond networks are expected to play critical roles in the coming connected society. By exploring new AI techniques, this thesis jointly considers the requirements and challenges of security, trust, and privacy provisioning, and develops multi-dimensional intelligent continuous processes for ever-growing demands of the quality of service in diverse applications. These novel approaches provide highly efficient, reliable, model-independent, situation-aware, and continuous protection for legitimate communications, especially in the complex time-varying environment under unpredictable network dynamics. Furthermore, the proposed soft security enables flexible designs for heterogeneous IoT devices, and the collaborative schemes provide efficient solutions for massively distributed entities, which are of paramount importance to diverse industrial applications due to their ongoing convergence with 5G-and-beyond networks.

Keywords: 5G-and-beyond, security provisioning, trust management, privacy protection, artificial intelligence

Lay Summary

The fifth-generation (5G)-and-beyond will provide ultra-reliable broadband access everywhere not only to cellular hand-held devices but also to a massive number of new devices related to the Internet of Things (IoT) and Cyber-Physical Systems (CPSs). Any potential security risks and attacks in such dense networks could lead to catastrophic consequences and cause avalanche-like damages. This is mainly due to the critical roles of 5G-and-beyond to support a wide variety of vertical applications by connecting massive number of heterogeneous devices, machines, and industrial processes, as well as cascaded reactions from the enormous parallel interconnections. Moreover, the widely used resource-constrained devices, e.g., sensors, can be compromised easily, resulting in widely distributed security threats through data injection, spoofing, eavesdropping, and so on. With the cascading effects, these security threats could also lead to the failure of a whole system, especially for those applications relying on tight collaborations among diverse entities. To enhance security and achieve more efficient management in 5G-and-beyond, this thesis develops intelligent security provisioning and trust management approaches by exploiting the help of artificial intelligence (AI) to address the related technical issues and challenges.

Firstly, two multi-dimensional adaptive physical-layer authentication schemes are proposed based on AI techniques as an intelligent process to learn and utilize the time-varying and imperfectly estimated communication link attributes, i.e., the kernel-learning-based scheme and fuzzy-learning-based scheme. In the former scheme, a kernel-based fusion model is designed to deal with the multiple attributes without knowledge of their statistical properties. The proposed authentication is developed as a linear convex model. Such a convex property will greatly reduce authentication complexity. In the latter scheme, fuzzy functions are explored to characterize the multiple physical-layer attributes with imperfectness and uncertainties as parametric models since the model structure can be learned from the data as a priori. A hybrid learning-based adaptive algorithm is proposed to near-instantaneously update the authentication parameters. These two schemes both act as an intelligent process to tackle the variations of the utilized attributes and hence to improve the reliability and robustness of the authentication.

To mitigate the effects of inevitable erroneous decision of authentication, an adaptive trust management based soft authentication and progressive authorization scheme is proposed by

intelligently exploiting the time-varying communication link-related attributes. The trust relationships between transceivers are established based on their evaluations of the selected attributes for fast authentication. The transmitter can be authorized by the specific level of services/resources corresponding to its trust level. To dynamically update the trust level of the transmitter, an online conformal prediction-based adaptive trust adjustment algorithm is proposed relying on the real-time validation of attributes estimated at the receiver, resulting in soft security and progressive authorization.

A privacy-preserved distributed access control scheme is proposed for blockchain-enabled IoT systems, which involves an accountable recommendation mechanism, an anonymous credential generation strategy, and a reputation update mechanism. In the recommendation mechanism, multiple authorized devices are utilized as referrers to authenticate a public device and issue the required credential for joining the system. Then, the anonymous credential generation strategy helps to further achieve privacy protection, and the reputation update mechanism evaluates the behaviors of the authorized devices. A wrong recommendation will decrease the referrers' reputation, named as accountability.

Finally, to meet the stringent and diverse security requirements of 5G-and-beyond systems, a lightweight continuous authentication scheme is developed for identifying multiple resource-constrained IoT devices via their pre-arranged pseudo-random access time sequences. A transmitter will be authenticated as legitimate if and only if its access time-sequential order is identical to a pre-agreed unique pseudo-random binary sequence (PRBS) between itself and the base station. The seeds for generating PRBS between each transceiver pair are determined by exploiting the channel reciprocity, which is time-varying and difficult for a third party to predict. Hence, the proposed scheme provides seamless protections for legitimate communications as the seeds can be refreshed adaptively without incurring long latency, complex computation, and high communication overhead.

As a conclusion, by exploring AI techniques, this thesis studies security, privacy, and trust comprehensively to meet diverse communication requirements, supporting emerging applications of future connected society enabled by 5G-and-beyond networks.

To my parents, husband, and expected baby

Acknowledgments

I would like to express my deepest appreciation to my supervisor, Dr. Xianbin Wang, for all his invaluable guidance, precious time, and strongest support. It was his enlightening supervision that leads me to discover and solve the persistent challenges in communications security, at the same time, to deal with the newly emerged problems due to the fast evolution of nowadays wireless communication technologies. Under his guidance, we have significantly achieved close cooperation and great progress in my research, as well as expanded my research plan on several new research directions, as exemplified by intelligent security provisioning, trust management, and resource allocation. Dr. Wang always shared his valuable and precise ideas with me, which helped me a lot in extending my thinking, in improving my research skills, as well as in defining research objectives. It was an extremely fruitful and enjoyable experience to learn from and work together with him during these years. In addition, Dr. Wang is extremely hard-working, diligent, and capable of carrying out and well-balanced diverse activities at the same time. These invaluable capabilities will always encourage me in my future career.

Sincere thanks to Dr. Abdallah Shami, Dr. Jayshri Sabarinathan, Dr. Grace Yi, and Dr. Hai Jiang for being my examination committee. I highly appreciate their precious time and constructive suggestions on my thesis and research. Sincere thanks to Dr. Lajos Hanzo, Dr. Stefano Tomasin, Dr. Li Xu, Dr. Naofal Al-Dhahir, Dr. Nan Zhao, Dr. Kan Zheng, Dr. Yulong Zou, Dr. Kim-Kwang Raymond Choo, Dr. Xinyi Huang, Dr. Liang Xiao, Dr. Zhiwei Lin, and all my collaborators worldwide for their valuable time and suggestions during our collaborations. They always share their precious comments and latest views on our research areas with me.

Additionally, I would like to thank all course instructors and administrative staff that I met at Western University. I cannot complete this degree without their assistance and kindness during these four years. I would also like to express my thanks and gratitude to my research group colleagues, who helped me a lot in both work and daily life just like my brothers and sisters. I was so lucky to meet such a big and warm research group. I would also like to extend my thanks to all my friends and neighbors, who gave me strong support whenever and wherever I needed help.

As always, I feel so grateful to my parents, my parents-in-law, and my family. I highly appreciate their love and support throughout not only this degree but also my life. Specifically, I would like to thank the love of my life, my husband. He always puts up with me, loves me, and protects me. I am no longer afraid when I meet difficulties or lose direction in my life since he is always there for me and always back me up. I will never forget the first sight we met each other, and every moment we get together for the rest of my life. In the end, I would also like to express my deepest thanks to my expected baby. I could feel her intimate company when I was preparing this thesis.

Contents

Certificate of Examination **ii**

Abstract **ii**

Lay Summary **iv**

Dedication **vi**

Acknowledgments **vii**

List of Figures **xiii**

List of Tables **xvii**

1 Introduction **1**

1.1 Research Motivations 1

1.1.1 Threats in Explosively Growing Collaboration among Entities 1

1.1.2 Open Issues and Challenges for Conventional Mechanisms 5

1.1.3 Intelligent Security Provisioning and Trust Management 7

1.2 Research Objectives 10

1.3 Thesis Contributions 10

1.4 Thesis Organization 12

2 Background Study on Security, Trust, Privacy, and Artificial Intelligence **15**

2.1 Risks and Threats Landscape in 5G-and-Beyond 15

2.2 Existing Solutions for Secure Communication and Their Challenges 18

2.2.1 Authentication 18

Cryptographic Techniques . . . 18
Physical Layer Authentication Techniques . . . 19
Challenges for Existing Physical Layer Authentication Techniques . . . 20
2.2.2 Access Control . . . 22
2.2.3 Trust Management . . . 23
2.2.4 Privacy Protection . . . 25
2.3 AI for Security, Trust, and Privacy Enhancement . . . 26
2.3.1 Benefits of AI for Security, Trust, and Privacy . . . 26
2.3.2 Categories of Machine Learning for Intelligent Management . . . 28
Parametric Learning Methods . . . 28
Non-Parametric Learning Methods . . . 29
Supervised Learning Techniques . . . 30
Unsupervised Learning Techniques . . . 30
Reinforcement Learning Techniques . . . 30
2.3.3 AI-based Security Provisioning . . . 31
2.4 Chapter Summary . . . 32

3 Physical Layer Authentication as an Intelligent Process 33
3.1 Introduction . . . 33
3.1.1 Kernel Learning-based Authentication Scheme . . . 35
3.1.2 Fuzzy Learning-based Authentication Scheme . . . 38
3.2 System Model and Problem Formulation . . . 41
3.3 Kernel Learning-based Authentication Scheme . . . 44
3.3.1 Kernel Machine-based Multiple Physical Layer Attribute Fusion . . . 44
3.3.2 Adaptive Authentication based on Kernel Learning . . . 47
3.3.3 Simulation Results . . . 54
3.4 Fuzzy Learning-based Authentication Scheme . . . 60
3.4.1 Multi-Dimensional Adaptive Authentication Architecture . . . 65
3.4.2 Hybrid Learning for Parameters Update . . . 66
Gradient Descent for Nonlinear Parameter Update . . . 66

Least-Square Estimator for Linear Parameter Update 67
Hybrid Learning Algorithm 69
3.4.3 Convergence Analysis of Fuzzy Learning-based Scheme 70
3.4.4 Simulation Results 71
3.5 Chapter Summary 78

4 Adaptive Trust Management for Soft and Progressive Security 80
4.1 Introduction 81
4.2 System Model and Problem Formulation 85
4.3 Proposed Adaptive Trust Management Scheme 90
4.3.1 Conformal Predictor for Classification of Attribute Estimates 90
4.3.2 Adaptive Trust Adjustment based on Online Machine Learning 92
4.3.3 Security Performance Analysis 96
4.4 Simulation Results 103
4.5 Chapter Summary 111

5 Accountable Distributed Access Control with Privacy Preservation 112
5.1 Introduction 113
5.1.1 Security Weaknesses and Motivations 114
5.1.2 Technical Contributions 115
5.2 System Model 116
5.3 Proposed Distributed Access Control Scheme 118
5.3.1 Recommendation for Distributed Access Control 118
5.3.2 Anonymous Credential Generation 122
5.3.3 Accountability based on Adaptive Reputation Update and Dynamic Multiple-Level Authorization 123
5.3.4 Analysis 125
5.4 Simulation Results 126
5.5 Chapter Summary 131

6 Lightweight Continuous Authentication via Intelligent Access 133

6.1 Introduction 134
6.2 System Model and Dynamically Arranged Pseudo-Random Access 138
6.3 Intelligently Arranged Access for Lightweight Continuous Authentication . . . 142
    6.3.1 Seed Acquisition Technique 143
    6.3.2 PRBS Generation and Update 149
    6.3.3 Performance Analysis 150
6.4 Simulation Results 152
    6.4.1 Implementation of The Proposed Scheme 152
    6.4.2 Comparison Results 155
6.5 Chapter Summary 160

7 Conclusion and Future Work **161**
7.1 Conclusion 161
7.2 Future Work 162

Bibliography **164**

Curriculum Vitae **185**

List of Figures

1.1 5G-and-beyond design principle. 2

1.2 Security, trust, and privacy in explosively growing collaboration among entities. 4

1.3 Multi-objectives of intelligent security provisioning and trust management in 5G-and-beyond. 8

1.4 Thesis organization. 12

2.1 Typical risks and threats in 5G-and-beyond networks. 16

2.2 Comparison of cryptographic and physical authentication techniques. 20

2.3 Categories of machine learning (ML) techniques for intelligent security provisioning and trust management. 28

2.4 Framework diagram of intelligent authentication design. 31

3.1 Adversarial system and physical layer authentication in a wireless network. . . 42

3.2 Kernel machine-based multiple physical layer attribute fusion. 44

3.3 Training performance of the kernel learning-based scheme (Algorithm 1) relying on the CFO, CIR and RSSI triplet. 55

3.4 Training performance of the kernel learning-based scheme (Algorithm 1) relying on 2 attributes and 3 attributes. 56

3.5 Authentication performance of the kernel learning-based scheme relying on the CFO, CFO & CIR, CFO & RSSI, and CFO & CIR & RSSI scenarios. 57

3.6 Authentication performance of the kernel learning-based scheme relying on the CFO & CIR and CFO & CIR & RSSI scenarios. 58

3.7 Authentication performance comparison results of the kernel learning-based scheme with different numbers of attributes. 58

3.8 Comparison results between the kernel learning-based scheme and the process without updating system parameters relying on CFO & CIR & RSSI. 59

3.9 Multi-dimensional adaptive authentication architecture with linear parameters $\widehat{\alpha}_n$ and nonlinear parameters $\widehat{\mu}_n, \widehat{\sigma}_n^2$. 66

3.10 Schematic diagram of the proposed hybrid learning process. 70

3.11 An urban scenario in the simulation. 72

3.12 Variation measurements of CFO, CIR, RSSI, and IQI of Alice and Eve for simulation. 73

3.13 Parameter design and update by Algorithm 2. 74

3.14 Convergence performance of Algorithm 2 for 11-th observation in Figure 3.13. 75

3.15 False alarm rate of the fuzzy learning-based scheme by different numbers of attributes. 75

3.16 Robust performance of the fuzzy learning-based scheme. 76

3.17 Comparison results of the fuzzy learning-based scheme and the optimal weight-based scheme of [114]. 77

3.18 Comparison results of the fuzzy learning-based scheme and the neural network-based scheme of [119]. 77

4.1 Soft authentication and progressive authorization system between Alice and Bob using a physical layer attribute continuously. 85

4.2 Performance of the proposed online conformal predictor relying on CFO. . . . 104

4.3 Performance of the proposed online conformal predictor relying on RSSI. . . . 106

4.4 Individual satisfaction vs. threshold of individual risk for the numbers of authorization levels $N = 2$, $N = 3$, and $N = 4$ based on the results of Figure 4.2. 107

4.5 Performance of the proposed progressive authorization solution for different forgetting factors benchmarked against the static binary authentication scheme. 108

4.6 Security performance and robustness of the proposed progressive authorization solution parameterized by different numbers of authorization levels. 109

4.7 Individual satisfaction comparison results of the proposed scheme and the scheme of [2] in the scenario that false alarms happen during the authentication process. 110

5.1 Framework of a consortium blockchain-enabled IoT system. 117
5.2 The proposed recommendation mechanism for distributed access control. . . . 119
5.3 Anonymous credential generation procedure. 123
5.4 Misdetection rate vs. false alarm rate with different numbers of referrers. 127
5.5 False alarm rate vs. number of referrers with respect to different thresholds in the distributed access control. 128
5.6 Misdetection rate vs. number of referrers with respect to different thresholds in the distributed access control. 128
5.7 Comparison results of privacy preservation between the scheme of [8] and the proposed scheme in the case that the trusted third party or one of Alice's referrers is compromised with a probability. 129
5.8 Reputation update of the misdetected adversary with respect to different attacking behaviors in the proposed scheme. 130
5.9 Reputation update of the misdetected adversary and its referrers in the proposed scheme. 131

6.1 System model in the 5G-and-beyond network. The communications between multiple IoT devices and a base station suffer from the spoofing attacks caused by the adversaries. 138
6.2 The developed authentication method between IoT devices 1-4 (transmitters) and a base station (receiver) through the identification of the pre-arranged pseudo-random access time sequences of IoT devices according to the pre-agreed PRBSs. 139
6.3 Framework of the proposed lightweight continuous authentication scheme through identifying the pre-arranged pseudo-random access time sequences of IoT devices. 142
6.4 Process of the developed new seed acquisition technique for PRBS generation containing three phases: Channel probing, Quantization, and Verification. . . . 143

6.5 The schematic diagram of the developed SVM-based quantization method with multiple boundaries. The red dots are the measurements of physical layer attributes used. 144

6.6 Simulation scenario of the proposed scheme. 153

6.7 Observations of physical layer attributes used at base station and Device 1. . . . 153

6.8 Initial binary sequences obtained (100 bits) at the base station and Device 1 in Phase II of the developed seed acquisition technique, as well as the unique seed acquired (50 bits) in the proposed scheme. 154

6.9 Comparison results between RSS-based quantization method of [175] and the proposed SVM-based quantization method. 155

6.10 Comparison results between the proposed scheme and the physical layer key generation schemes of [174, 175, 176, 177, 178]. 156

6.11 False alarm comparison results between the Kernel Learning-based Authentication as an Intelligent Process (KLAIP) scheme of [2] and the proposed Lightweight Continuous Authentication (LCA) scheme. 157

6.12 Misdetection comparison results of the Kernel Learning-based Authentication as an Intelligent Process (KLAIP) scheme of [2], Static Authentication (SA) scheme, and the proposed Lightweight Continuous Authentication (LCA) scheme. 158

6.13 Computation cost comparison between the proposed Lightweight Continuous Authentication (LCA) scheme and the schemes of [39], namely IAG, FW, and dFW. 159

List of Tables

3.1 Notations of Chapter 3 41
3.2 Simulation parameters of Chapter 3 72

4.1 Notations of Chapter 4 84

5.1 Notations of Chapter 5 116

6.1 Notations of Chapter 6 138
6.2 Simulation parameters of Chapter 6 152

Chapter 1

Introduction

1.1 Research Motivations

1.1.1 Threats in Explosively Growing Collaboration among Entities

The fifth-generation (5G)-and-beyond wireless networks have received tremendous attention from both academia and industries alike, which are expected to enable a wide variety of vertical applications by connecting heterogeneous devices and machines [1, 2]. With extremely dense deployments of base stations, 5G-and-beyond will provide ultra-reliable and affordable broadband access everywhere not only to cellular hand-held devices but also to a massive number of new devices related to Machine-to-Machine communication (M2M), Internet of Things (IoT), and Cyber-Physical Systems (CPSs) [3]. In addition, the dramatically growing number of low-cost devices and access points with increased mobility and heterogeneity leads to the extremely complex and dynamic environment of 5G-and-beyond wireless networks [4]. Such enrichment implies that 5G-and-beyond is not a mere incremental advancement of 4G as one might intuitively think, but an integration of new disruptive technologies to meet the ever-growing demands of user traffic, emerging services, and IoT devices [4].

As shown in Figure 1.1, the 5G-and-beyond networks are expected to provide diverse and stringent Quality of Service (QoS) requirements, including extremely very high data rates, higher coverage with significantly improved communication reliability, and low latency [3]. To meet these future communication demands, tight collaboration among devices and communi-

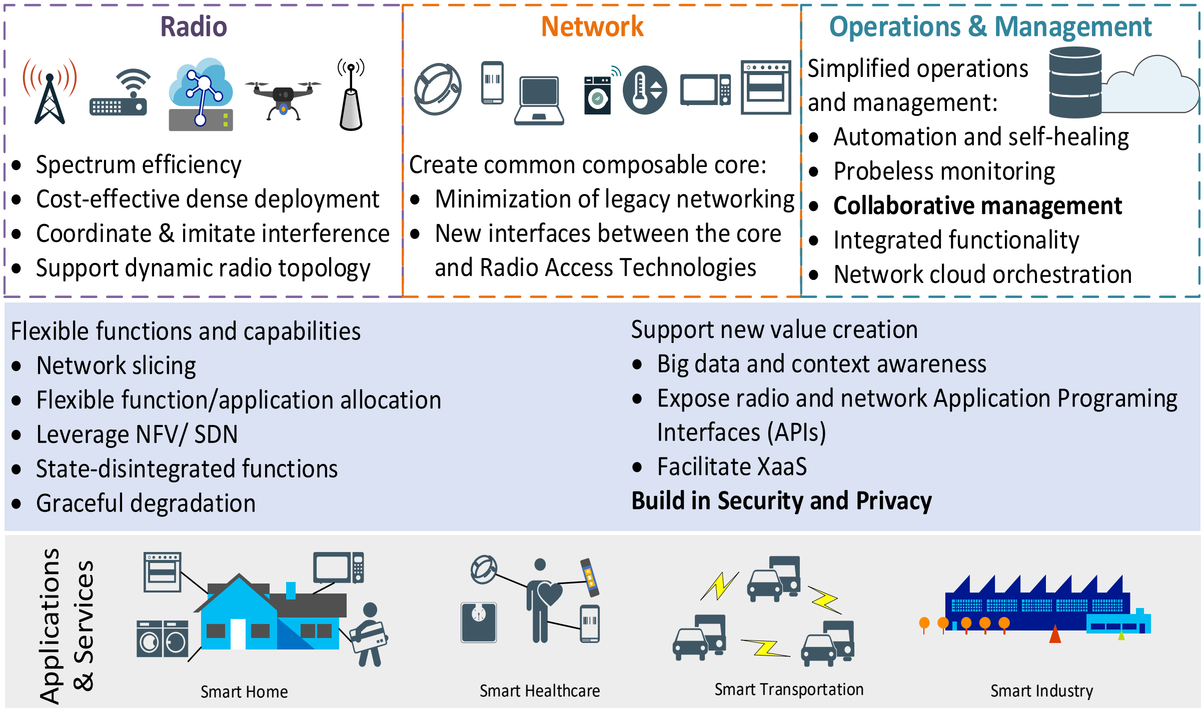

Radio
Spectrum efficiency
Cost-effective dense deployment
Coordinate & imitate interference
Support dynamic radio topology
Network
Create common composable core:
Minimization of legacy networking
New interfaces between the core and Radio Access Technologies
Operations & Management
Simplified operations and management:
Automation and self-healing
Probeless monitoring
Collaborative management
Integrated functionality
Network cloud orchestration
Flexible functions and capabilities
Network slicing
Flexible function/application allocation
Leverage NFV/ SDN
State-disintegrated functions
Graceful degradation
Support new value creation
Big data and context awareness
Expose radio and network Application Programing Interfaces (APIs)
Facilitate XaaS
Build in Security and Privacy
Applications & Services
Smart Home
Smart Healthcare
Smart Transportation
Smart Industry

Figure 1.1: 5G-and-beyond design principle.

cation systems is required and will be extremely important for future wireless communications. Many related areas and technologies have attracted a multitude of interests from research and industrial communities, as exemplified by the collaborative computing, manufacturing, software development, and machine learning, just to name a few [5, 6]. However, the complexity of future communication systems as well as dramatically increased use of intelligent machines and devices within industry processes bring many vulnerabilities and new design challenges, which will obviously fail the required collaboration if they are not fully addressed. The threats in the explosive growth of collaboration among entities can be classified into three categories as follows:

- **Security risks**. Potential security risks and attacks could lead to catastrophic consequences and cause avalanche-like damages in 5G-and-beyond networks. This is mainly due to the critical roles of 5G-and-beyond system to support a wide variety of vertical applications by connecting tremendous heterogeneous devices, machines, and industrial processes, as well as cascaded reactions from the enormous parallel interconnection contained in 5G-and-beyond. Moreover, the widely used resource-constrained devices, e.g., sensors, can be compromised easily, thus resulting in widely distributed threats to the IoT network through data injection, spoofing, eavesdropping, and so on. With the cascading effect, these security threats could also lead to the failure of a whole system, especially for those applications relying on tight collaboration among diverse entities.

- **Lack of trust**. The collaborations among devices and communication systems heavily depend on devices' perceptions of the system as a trustworthy infrastructure for providing accurate information and reliable communication. On one hand, the trust is based on the authentication solutions, where messages must be authenticated to prevent external attackers from injecting, altering, and replaying messages, as well as to prevent eavesdropping and location tracking. On the other hand, assessing the credibility of the reported data and behaviors of devices could help in establishing the trust of these devices. Hence, the trust establishment for collaboration contains both the solutions for defending against security risks and methods for assessing the behaviors of devices.
- **Privacy leakage**. To provide high-quality services, large amounts of multi-dimensional data will be collected in the 5G-and-beyond networks. However, the collection and correlation of these data allow the creation of detailed profiles encompassing every aspect of a device/user [10]. Moreover, the significantly increased level of the interconnectivity of a 5G-and-beyond system could further lead to privacy leakage. To be more specific, combining multiple dimensions of data from different layers, devices, and applications can improve service quality, but increases the risk for leaks of sensitive data through correlation as well. The leaked private information of a device/user not only leads to security risks but also destroys the established trust during the collaboration process.

The relationship between security, trust, and privacy is shown in Figure 1.2. To be more specific, security risks and attacks could lead to privacy leakage, including the leakage of sensitive data, user location, and identity information [12]. Both security attacks and inappropriate behaviors of devices could result in untrustworthy collaboration among devices and communication systems. Trust system can also be used in assessing the quality of received information, to provide network security services such as access control, authentication, malicious node detections, and secure resource sharing [9]. The leaked private information of a device/user could

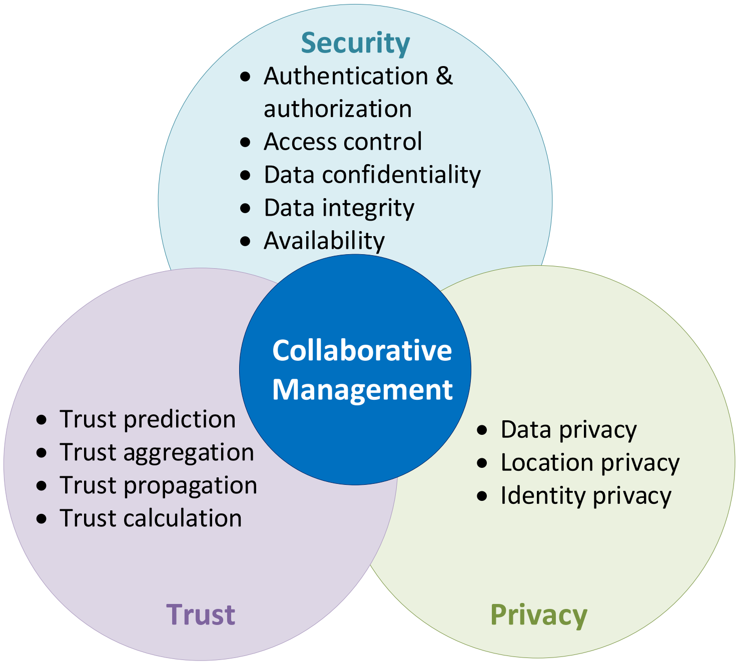


Figure 1.2: Security, trust, and privacy in explosively growing collaboration among entities.

be leveraged by attackers, thus leading to security risks and lack of trust. Hence, to effectively support future IoT systems in vertical industry applications, security, trust, and privacy should be dealt with integratively due to their close interactions.

In achieving collaboration among entities, multi-dimensional requirements should be considered, which are summarized as follows:

- **Authentication and authorization.** Both of them have been considered as key security mechanisms and critical designs for 5G-and-beyond networks since adversaries need access to communication systems to launch attacks [7, 11]. These mechanisms secure legitimate communications by confirming the identities of all devices and their right access to authorized resources, data, and services. To be more specific, the authentication mechanism confirms the identities of communicating entities, ensures the validity of their claimed identities, and provides assurance against various attacks [14].

- **Access control.** This protects against unauthorized use of network resources, and also ensures that only authorized persons or devices can access the network resources, services, data, and information flows [3].

- **Data confidentiality.** It protects data from unauthorized disclosure, and ensures that the data content cannot be understood by unauthorized entities [3, 18].
- **Data integrity.** It ensures the correctness and accuracy of data, and protects from unauthorized creation, modification, deletion, and replication [3, 18].
- **Availability.** It ensures that there is no denial of authorized access to network resources, stored information, services, and applications [3, 18].
- **Trust management.** A trust management system aims to provide a process to produce high-quality trust prediction for users [16, 17]. It usually contains several components, such as trust calculation, trust propagation, trust aggregation, and trust prediction.
- **Privacy protection.** It provides protection for information that might be derived from the observation of network activities as well as for data stored on the Internet [15]. Some key properties can be used for privacy protection in 5G-and-beyond: anonymity, unlinkability, undetectability, unobservability, and pseudonymity [12].

1.1.2 Open Issues and Challenges for Conventional Mechanisms

The security solutions and architectures used in previous generations of wireless networks (i.e., 3G and 4G) are apparently not sufficient for 5G-and-beyond, mainly because of its dynamics of new services and technologies [12]. Moreover, the latency requirements of security management, especially in machine communications, such as vehicular communication or Unmanned Aerial Vehicles (UAVs), are much critical. Those security architectures of the previous generations lack the sophistication needed to secure 5G-and-beyond networks. Furthermore, there are new technological concepts or solutions that will be used in 5G-and-beyond to meet the demands of increasingly diverse applications and connected devices, as exemplified by the cloud computing [19], Software Defined Networking (SDN) [19], and Network Function Virtualization (NFV) [20]. These fast-emerging technologies bring new security challenges. Explicitly, those IoT devices suffering from resource limitation could not support the security methods requiring high communication and computation overhead. Tremendous devices contained in a 5G-and-beyond system also claim low-delay transmissions to guarantee their communication performance. Hence, to defend against threats in the explosive growth of collaboration among entities, this thesis firstly focuses on studying the challenges for conventional mechanisms and then on envisioning new approaches for security and trust enhancement.

The conventional security methods, including key-based cryptography techniques and physical layer key generation techniques, may suffer from their high complexity and long latency, and may be ineffective to adapt to the complex dynamic environment, especially in large-scale networks. Furthermore, their generated keys may be leaked in the security management procedures, e.g., key distribution. As discussed above, while security is the cornerstone for such applications, trust among entities and information privacy are becoming increasingly important. Security, trust, and privacy should be dealt with integratively due to their close interactions. However, conventional technologies always treat these aspects separately, leading to tremendous loopholes and low efficiency. To be more specific, some open issues and challenges for conventional mechanisms in supporting secure communications are summarized as follows.

- **Long security overhead induced latency in large-scale networks.** The conventional cryptography techniques require increased overhead and lengthy process for the increased level of security, thus leading to high communication and computation overhead, as well as long communication latency [2]. These are intolerable for the large-scale network having significantly increasing number of intelligent machines and resource-constrained devices with concurrent communications. Moreover, the conventional statistical-based methods for authentication also require enough time and computational resources for obtaining the statistical properties [2], thus leading to limited capability in detecting attacks promptly.

- **Ineffective adaptation to dynamic communication environments.** Conventional security solutions may also suffer from cascading risks in dynamic communication scenarios due to their reliance on static binary mechanisms. Such mechanisms are difficult in learning from and adapting to the dynamic environment encountered, thus resulting in the failure of continuous protections for legitimate communications and decrease of security performance in dealing with varying security risks.

- **Potential key leakage in security management procedures.** Conventional cryptographic techniques also require necessary key management procedures to generate, distribute, refresh and revoke digital security keys, leading to the potential leakage of key information [2]. Furthermore, the key information transmission is also needed for information reconciliation in the physical key generation techniques [21]. These all result in tremendous loopholes for adversaries and wide security threats in 5G-and-beyond.

- **Separate treatment of security, trust, and privacy in tightly collaborative applications.** To achieve tight collaboration among entities in future wireless communications, security, privacy, and trust should be considered comprehensively. Conventional security methods that focus only on device-to-device data transmission are lack of trust evaluation in tight collaborative applications, which helps in predicting the future actions of users/devices and resulting in a good outcome in security enhancement. Hence, those conventional security methods that separately treat security, trust, and privacy will leave the amount of loopholes for attackers in tightly collaborative applications.

In a nutshell, the efficient security enhancement and trust management are of paramount importance for 5G-and-beyond networks, especially in the coming of information age requiring “Intelligence”.

1.1.3 Intelligent Security Provisioning and Trust Management

This thesis envisions new intelligent security provisioning and trust management approaches by exploiting the help of Artificial Intelligence (AI) to address the above challenges for security and trust enhancement as well as more efficient management in 5G-and-beyond networks. As illustrated in Figure 1.3, the 5G-and-beyond networks are expected to provide wide services having high communication and security performance as well as privacy-preserving transmissions. Based on these basic requirements, the intelligent security provisioning and trust management approaches are required to meet multi-objectives, namely for high cost-efficiency, high reliability, model independence, continuous protection, and situation awareness. More importantly, the flexible designs of security and trust management are extremely helpful in providing automatic services in different 5G-and-beyond communication scenarios, which are presented in different colors inside the pentagon of Figure 1.3. Meeting these multiple objectives supports the advantages of intelligent security provisioning and trust management based on AI as follows:

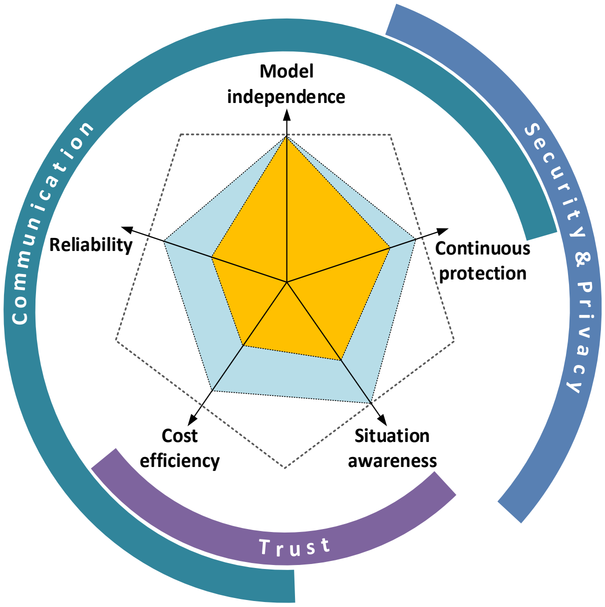


Figure 1.3: Multi-objectives of intelligent security provisioning and trust management in 5G-and-beyond.

- **High cost-efficiency:** Due to the increasing number of resource-constraint devices in 5G-and-beyond wireless applications, communication, security, privacy, and trust management should be executed concurrently to achieve cost-effective services. The opportunistic selection of features and dimension reduction methods [2] may help in decreasing the complexity of the security and trust management relying on multi-dimensional information as well as in reducing communication and computation overheads. Furthermore, by performing training and testing at devices having enough energy and storage space, efficient security and trust management can be achieved at resource-constraint devices.

- **High reliability:** Utilizing specific features and relationships in the multi-dimensional domain is extremely helpful for achieving security enhancement since it is more difficult for an adversary to succeed in predicting or imitating all attributes based on the received signals and observations. To be more specific, the multi-dimensional information, such as time, frequency, network architecture, and communication process, provides broader protections for legitimate users. Moreover, through using multi-dimensional information, more precise and comprehensive trust evaluation can be achieved. AI techniques could facilitate security and trust management by analyzing and fusing the multi-dimensional information.

- **Model independence:** A data-based scheme through exploring machine learning techniques overcomes the difficulties in modeling uncertainties and unknown dynamics of the security and trust management process. Hence, the model-free schemes remove the assumption of knowing structures of systems, resulting in a more scalable process design. This benefits the development of multi-dimensional intelligent processes for ever-growing demands of the quality of service in diverse applications, especially in the complex time-varying environment under unpredictable network dynamics.

- **Continuous protection:** Utilizing the received information along with data transmission for security enhancement could provide identification after login and control the varying security risks. In achieving this, machine learning techniques may be explored for data analysis and processing, so that the seamless protection for legitimate devices can be achieved in 5G-and-beyond networks.

- **Situation awareness:** The situation-aware management observes the varying objectives and security risks, and learns from the complex dynamic environment to enhance security and to achieve efficient collaboration. AI techniques provide powerful tools to learn the dynamic adversarial environment for self-optimization and self-organization, thereafter achieving automatic security and trust management. More importantly, machine learning techniques could help in the detection of time-varying communication scenarios as well as the adaptation of security and trust management process.

As a conclusion, by exploring AI techniques, this thesis introduces the intelligence to security and trust management in the complex time-varying environment, supporting radically new applications of 5G-and-beyond wireless networks.

1.2 Research Objectives

This thesis explores AI techniques for intelligent security provisioning and trust management. The research objectives of this thesis are summarized as follows.

- To develop new authentication schemes based on AI techniques as an intelligent process to learn and utilize the time-varying and imperfectly estimated communication link attributes, thus to provide continuous protection for legitimate devices.
- To propose a soft authentication and progressive authorization scheme based on trust management for achieving quick access and enhanced security by intelligently exploiting the time-varying communication link-related attributes.
- To develop a distributed access management scheme for consortium blockchain-enabled IoT systems by jointly considering security, privacy, and trust for achieving reliable access control to defend against both outside and inside attacks.
- To propose a new lightweight continuous security scheme with the assistance of AI techniques for identifying multiple resource-constrained IoT devices via their pre-agreed pseudo-random access time sequences.

1.3 Thesis Contributions

The main contributions of this thesis are summarized as follows.

- Two multi-dimensional adaptive physical layer authentication schemes are proposed based on AI techniques to learn and utilize the time-varying and imperfectly estimated communication link attributes. In the kernel-learning-based scheme, a fusion model is designed to deal with the multiple attributes without knowledge of their statistical properties. The authentication technique is developed as a linear convex model. Such a convex property will greatly reduce authentication complexity. In the fuzzy learning-based scheme, fuzzy functions are explored to characterize the multiple physical layer attributes with imperfectness and uncertainties as parametric models since the model structure can be learned from the data as a priori. A hybrid learning-based adaptive algorithm is proposed to near-instantaneously update the authentication parameters. These two schemes both act as an intelligent process to tackle the variations of the utilized attributes and hence to improve the reliability and robustness of the authentication.

- To mitigate the effects of inevitable wrong decision of authentication relying on the time-varying communication link-related attributes, an adaptive trust management based soft authentication and progressive authorization scheme is proposed. The trust relationships between transceivers are established based on their evaluations of the selected attributes for fast authentication. The transmitter can be authorized by the specific level of services/resources corresponding to its trust level. To dynamically update the trust level of the transmitter, an online conformal prediction-based adaptive trust adjustment algorithm is proposed relying on the real-time validation of attributes estimated at the receiver, resulting in soft security and progressive authorization.

- A privacy-preserved distributed access control scheme based on accountable recommendation is proposed for consortium blockchain-enabled IoT systems. It involves an accountable recommendation mechanism, an anonymous credential generation strategy, and a reputation update mechanism. In the recommendation mechanism, multiple authorized devices act as referrers to authenticate a public device and issue the required credential for joining the system. Then, the anonymous credential generation strategy is developed for further privacy protection. The reputation update mechanism is proposed to evaluate the behaviors of the authorized devices for achieving multiple-level authorization and accountable security services. Hence, the proposed scheme secure the integrated system through reliable access control to defend against both outside and inside attacks.

- A lightweight continuous authentication scheme is developed for identifying multiple resource-constrained IoT devices via their pre-arranged pseudo-random access time sequences. A transmitter will be authenticated as legitimate if and only if its access time-sequential order is identical to a pre-agreed unique pseudo-random binary sequence (PRBS) between itself and the base station. The seed for generating PRBS between each transceiver pair is determined by exploiting the channel reciprocity, which is time-varying and difficult for a third party to predict. Moreover, the Support Vector Machine (SVM) algorithm is applied for intelligently quantizing the physical layer attribute estimates to bits. Hence, the proposed scheme provides seamless protections for legitimate communications as the seeds can be refreshed adaptively without incurring long latency, complex computation, and high communication overhead.

1.4 Thesis Organization

The following details and Figure 1.4 demonstrate the organization of remaining chapters of this thesis.

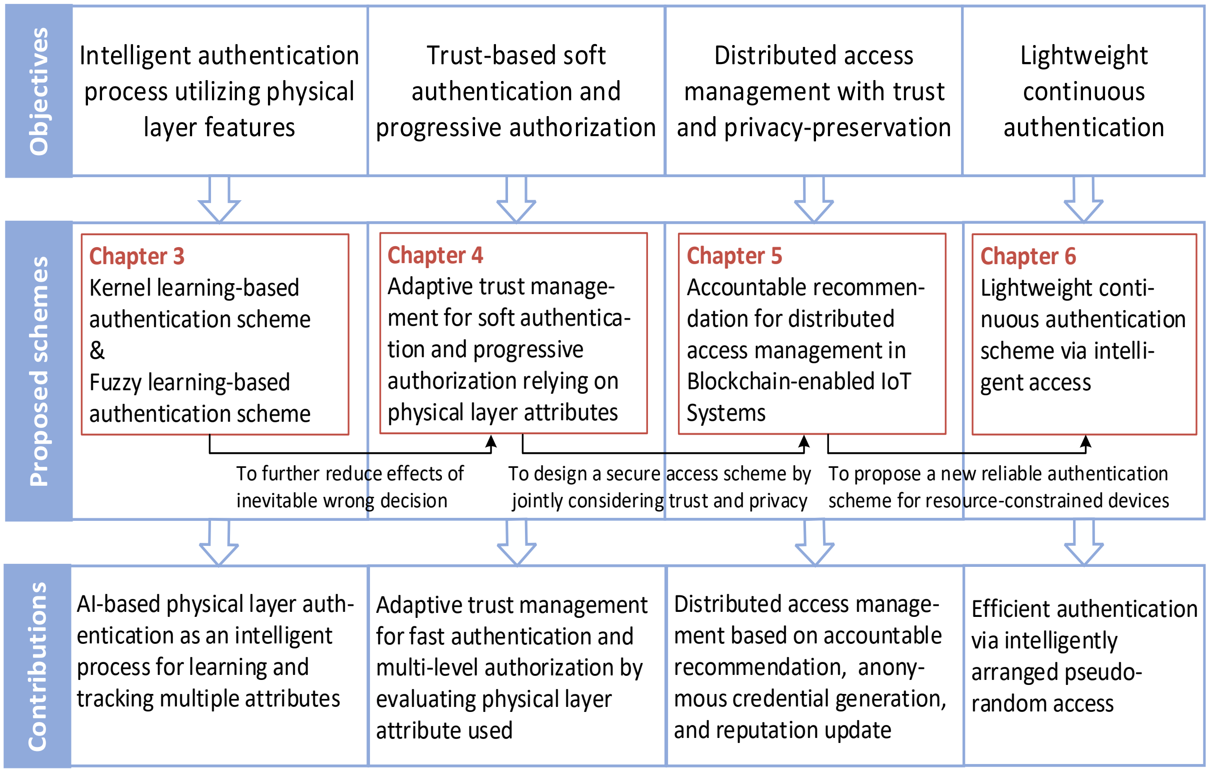

Objectives
Intelligent authentication process utilizing physical layer features
Trust-based soft authentication and progressive authorization
Distributed access management with trust and privacy-preservation
Lightweight continuous authentication
Proposed schemes
Chapter 3
Kernel learning-based authentication scheme
&
Fuzzy learning-based authentication scheme
Chapter 4
Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes
Chapter 5
Accountable recommendation for distributed access management in Blockchain-enabled IoT Systems
Chapter 6
Lightweight continuous authentication scheme via intelligent access
To further reduce effects of inevitable wrong decision
To design a secure access scheme by jointly considering trust and privacy
To propose a new reliable authentication scheme for resource-constrained devices
Contributions
AI-based physical layer authentication as an intelligent process for learning and tracking multiple attributes
Adaptive trust management for fast authentication and multi-level authorization by evaluating physical layer attribute used
Distributed access management based on accountable recommendation, anonymous credential generation, and reputation update
Efficient authentication via intelligently arranged pseudo-random access

Figure 1.4: Thesis organization.

It would be beneficial to first provide fundamentals related to wireless communication security, privacy, and trust, existing solutions to secure communication and their challenges, as well as the introduction of AI techniques for security enhancement, privacy protection, and trust management. All of these will be explained in Chapter 2.

Chapter 3 proposes two physical layer authentication schemes as an intelligent process to achieve continuous protections for legitimate devices, including kernel learning-based scheme and fuzzy learning-based scheme. The proposed kernel learning-based physical layer authentication scheme tracks multiple communication link-related features to achieve reliable authentication that leaves fewer loopholes for spoofers in intermittent communications, which is a nonparametric method. However, compared with another kind of methods, i.e., the parametric methods, more observed samples of the adopted attributes are required in building the authentication model by using the nonparametric methods, leading to a larger number of parameters in the authentication process to be determined. Then, the fuzzy learning-based authentication scheme is proposed, which is a parametric method. Through providing a form of system expression, more information has been involved in the attribute combination model, thus resulting in fewer parameters to be determined when compared to the nonparametric methods.

Considering the inherent misdetection and false alarm problems in physical layer authentication, an adaptive trust management-based soft authentication and progressive authorization scheme is developed in Chapter 4. This scheme establishes trust relationship between the transmitter and receiver based on the evaluation of selected physical layer attribute for fast authentication and multiple-level authorization. Through the designed trust model, the transmitter is authorized by the specific level of services/resources corresponding to its trust level, so that soft security is achieved. To dynamically update the trust level of the transmitter, an online conformal prediction-based adaptive trust adjustment algorithm is proposed relying on the real-time validation of its attribute estimates at the receiver, thus resulting in the progressive authorization.

By jointly considering security and privacy-preservation, an accountable recommendation-based distributed access control scheme is proposed for consortium blockchain-enabled IoT systems in Chapter 5. This scheme involves an accountable recommendation mechanism, an anonymous credential generation strategy, and a reputation update mechanism. In the recommendation mechanism, multiple authorized devices are utilized as referrers to authenticate a public device and issue the required credential for joining the system. Then, the anonymous credential generation strategy helps to further achieve privacy protection. To ensure the effectiveness of the proposed recommendation mechanism, a reputation update method is also developed to evaluate the behaviors of authorized nodes. An incorrect recommendation will lead to the decrease of referrers' reputation values, named as accountability. Moreover, the dynamic multiple-level authorization can be achieved for all devices based on their adaptive reputation values.

Chapter 6 develops a new lightweight continuous authentication scheme in IoT systems based on the access time slots of the devices. The access time sequence of each device is prearranged between itself and the base station based on the channel reciprocity. A new seed acquisition technique is proposed based on the Support Vector Machine (SVM) to achieve better quantization performance. With the acquired seed, a Pseudo-Random Binary Sequence (PRBS) can be generated for authentication. The identification of the access time sequences of devices can dramatically reduce the time latency for authentication. More importantly, the proposed scheme is lightweight at the IoT devices since they don't require high computation/communication costs in generating authentication keys/tags.

Finally, conclusions are drawn from the studies and future research directions are pointed out in Chapter 7.

Chapter 2

Background Study on Security, Trust, Privacy, and Artificial Intelligence

The 5G-and beyond wireless networks are critical to support diverse vertical applications by connecting heterogeneous devices and machines, which directly increase vulnerability for various security risks and threats. Conventional cryptographic and physical layer security techniques are facing inevitable challenges in complex dynamic wireless environments, including significant security overhead, low reliability, as well as difficulties in pre-designing a precise security model and providing continuous protection. This chapter presents the detailed risks and threats in 5G-and-beyond networks as well as existing solutions for secure communication and their challenges. Furthermore, the benefits of utilizing Artificial Intelligence (AI) for security provisioning and trust management are introduced. Machine learning paradigms for intelligent security design are also presented, namely for parametric/non-parametric and supervised/unsupervised/reinforcement learning algorithms. Based on these preliminaries, intelligent security provisioning and trust management will be further studied, as well as new schemes will be developed for achieving the objectives of this thesis in the following chapters.

2.1 Risks and Threats Landscape in 5G-and-Beyond

As shown in Figure 2.1, the backhaul of 5G networks can be divided into three different layers: infrastructure layer, control layer, and application layer [12]. The infrastructure layer contains the basic connectivity devices, such as base stations, routers, and switches. All the network control functionalities and decision-making entities are placed in the control layer, which interacts with the application layer. Besides, it can translate the network service requests from the application layer as control commands and deliver to the infrastructure layer devices. Thus, all the network services and applications are implemented in the application layer. In addition, the end-to-end management is used in parallel to synchronize the operation and collaboration of these layers.

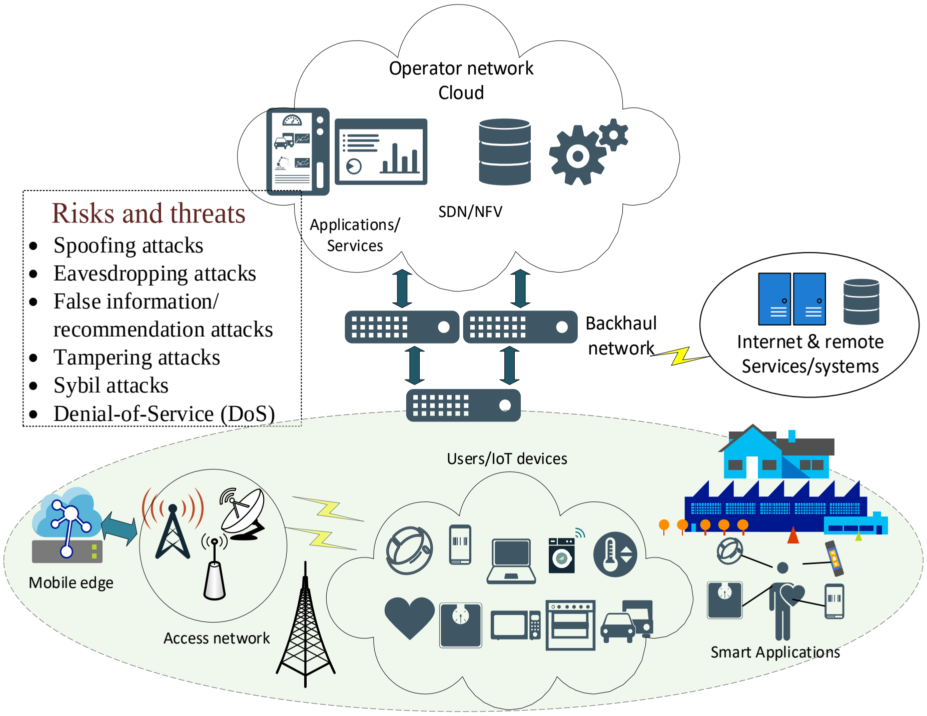


Figure 2.1: Typical risks and threats in 5G-and-beyond networks.

To support a wide variety of vertical IoT applications, the 5G-and-beyond networks connect a dramatically growing number of low-cost devices and access points with increased mobility and heterogeneity, leading to an extremely complex and dynamic environment. Specifically, due to the open broadcast nature of radio signal propagation, widely adopted standardized transmission protocols, and intermittent communication characteristic, wireless communications are extremely vulnerable to various attacks [2].

Some typical security threats and privacy risks in 5G-and-beyond are also shown in Figure 2.1, their descriptions are summarized as:

- Spoofing attacks: The objective of spoofing attacks is to generate and send malicious packets that seem legitimate in the systems. For example, the adversary may spoof the IP addresses of authorized devices in an IP-based IoT system, and then send malicious data with the spoofed IP addresses to gain access to the system [12].

- Eavesdropping attacks: Eavesdropping attacks are the acts of secretly or stealthily listening to the private conversation or communications of others without their consent [12]. An eavesdropping attack can be difficult to detect because the network transmissions will appear to be operating normally.

- False information/recommendation attacks: A malicious device may collude and provide false information/recommendations to isolate good devices while keeping malicious devices connected. The malicious device may keep complaining about a peer device and create the peer's negative reputation [65].

- Tampering attacks: This kind of attacks can be classified as device tampering and data tampering [66]. The device tampering can be easily performed especially when an IoT device is absent most of the time. It can be easily stolen without being noticed and then be used maliciously. The data tampering involves malicious modification of data, e.g., data stored in databases or data transiting between two devices.

- Sybil attacks: This kind of attacks are impersonation attacks, which can be simply prevented by explicitly binding an identity to participate in a system. A malicious device can use multiple network identities, which can affect topology maintenance and fault-tolerant schemes, such as multi-path routing [65].

- Denial-of-Service (DoS) attacks: They aim to overwhelm the network services by inundating them with requests, e.g., servers inundate with requests for services. A malicious node may block the normal use or management of communications facilities, for example, by causing excessive resource consumption [65].

2.2 Existing Solutions for Secure Communication and Their Challenges

This subsection presents some existing solutions for secure communications and their challenges, i.e., authentication, access control, trust management, and privacy protection.

2.2.1 Authentication

The existing solutions for authentication and their challenges are introduced in this subsection, including cryptographic techniques and physical layer authentication techniques.

Cryptographic Techniques

Although digital key-based cryptographic techniques [22, 23, 24] have been widely used both for communication security and authentication, they may fall short of the desired performance in many emerging scenarios. One fundamental weakness of the digital credentials based on conventional cryptography is that detecting compromised security keys cannot be readily achieved, since the inherent physical attributes of communication devices and users are disregarded [25]. Given the rapidly growing computational capability of devices, it is becoming more and more feasible to crack the security key from the intercepted signals of standardized and static security protocols. Furthermore, conventional cryptographic techniques also require appropriate key management procedures to generate, distribute, refresh, and revoke digital security keys, which may result in excessive latencies in large-scale networks. Indeed, this latency may become intolerable for delay-sensitive communications, such as networked control and vehicular communications. The computational overhead of digital key-based cryptographic methods is also particularly undesirable for devices, which have limited battery lifetime and computational capability, such as IoT sensors. For example, the group key agreement protocols require thousands of transmission times to exchange keys and to establish group keys among 5-client groups [26].

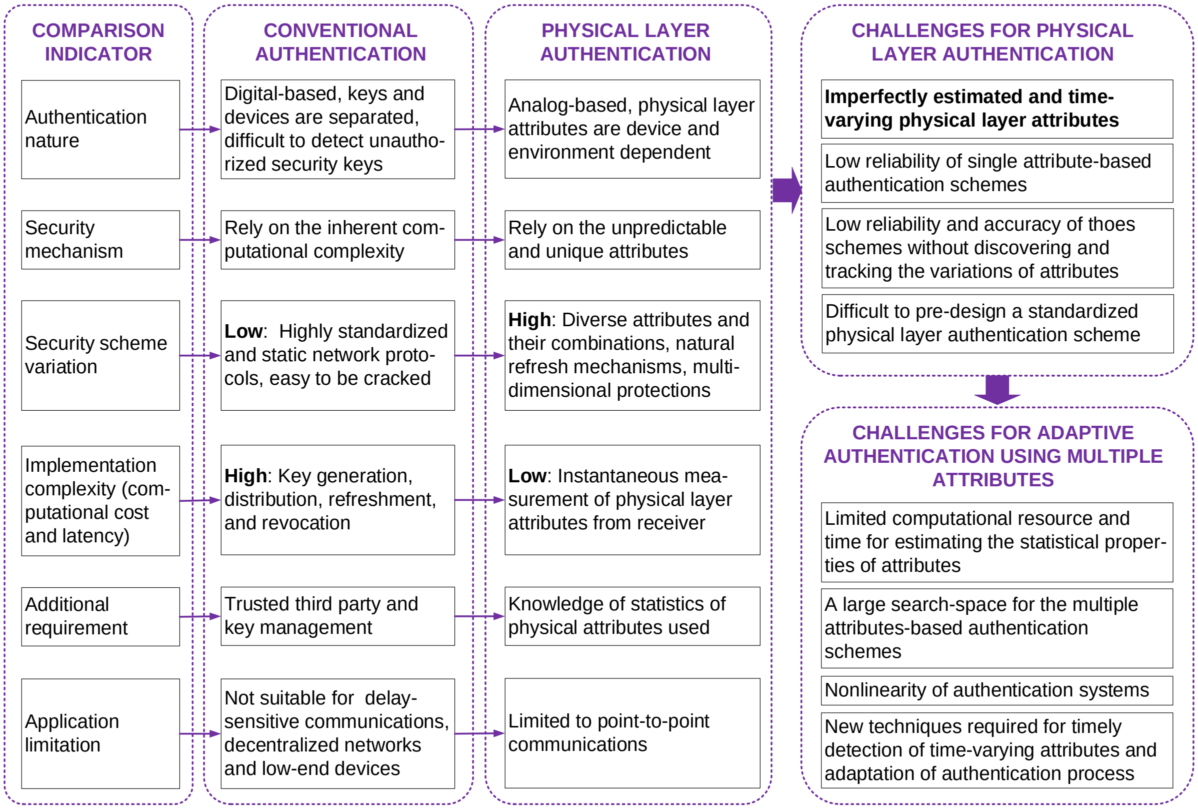
The authors of [27] developed a lightweight mutual authentication protocol based on the public key encryption for smart city applications, which strikes a balance between the efficiency and communication costs without sacrificing security. A scalable framework for lightweight authentication and hierarchical routing in data networking IoT is proposed in [28]. The authors of [29] proposed a two-factor lightweight privacy-preserving authentication scheme to enhance the security of vehicular ad-hoc network communications relying on the decentralized certificate authority and the biological passwords. However, these schemes also require many rounds for the key generation, refresh, and delivery, resulting in long time latency and high communication overhead. Furthermore, the key transmission process in security management procedures of the cryptographic techniques could lead to potential key leakage [30].

Physical Layer Authentication Techniques

Physical layer authentication techniques have attracted a lot of interests, which can be classified as key-based or keyless, according to whether a secret key shared between the transceiver is exploited for the physical layer authenticate or not [31].

In [32], the authentication signal is generated and added to the message signal with the assistance of a secrete key. The communication performance could be reduced in this scheme since the authentication signal appears as noise to the message signal and vice versa. The superimposed tag-based authentication schemes [33] transmit an additional authentication signal concurrently with the messages, but corrupt the entire data message and require additional complicated preprocessing, such as message symbol recovery through demodulation and decoding. The authors of [31] proposed an artificial-noise-aided physical layer phase challenge-response authentication scheme for orthogonal frequency division multiplexing (OFDM) transmission. In [34], a slope authentication method is developed at the physical layer to divide the transmitted signal into multiple groups, and to generate a tag based on a shared secrete key and pilot signal to mark the time index of each group for authentication. However, the above key-based physical layer authentication schemes require the procedure of generating keys and assistance from trusted third parties, resulting in long latency and high computation overhead.

The keyless physical layer authentication technique has been widely studied in the literature [31, 35, 36, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 48] due to its advantages including low computational requirement, low network overhead, and modest energy consumption. It focuses on exploiting the attributes of communication links and devices to protect legitimate communications from the spoofing attacks. Such analog-domain attributes directly relate to the communicating devices and corresponding physical environment, thus are difficult to impersonate and predict, e.g., channel impulse response (CIR) [35, 36], carrier frequency offset (CFO) [37, 38], received signal strength indicator (RSSI) [39], in-phase-quadrature-phase imbalance (IQI) [40], just to name a few. These attributes are time-varying and imperfectly estimated in practical networks because of the mobility of devices, dynamic channels with unpredictable interference conditions, estimation errors, and so on.



COMPARISON INDICATOR	CONVENTIONAL AUTHENTICATION	PHYSICAL LAYER AUTHENTICATION
Authentication nature	Digital-based, keys and devices are separated, difficult to detect unauthorized security keys	Analog-based, physical layer attributes are device and environment dependent
Security mechanism	Rely on the inherent computational complexity	Rely on the unpredictable and unique attributes
Security scheme variation	**Low**: Highly standardized and static network protocols, easy to be cracked	**High**: Diverse attributes and their combinations, natural refresh mechanisms, multi-dimensional protections
Implementation complexity (computational cost and latency)	**High**: Key generation, distribution, refreshment, and revocation	**Low**: Instantaneous measurement of physical layer attributes from receiver
Additional requirement	Trusted third party and key management	Knowledge of statistics of physical attributes used
Application limitation	Not suitable for delay-sensitive communications, decentralized networks and low-end devices	Limited to point-to-point communications

CHALLENGES FOR PHYSICAL LAYER AUTHENTICATION

- **Imperfectly estimated and time-varying physical layer attributes**
- Low reliability of single attribute-based authentication schemes
- Low reliability and accuracy of thoes schemes without discovering and tracking the variations of attributes
- Difficult to pre-design a standardized physical layer authentication scheme

CHALLENGES FOR ADAPTIVE AUTHENTICATION USING MULTIPLE ATTRIBUTES

- Limited computational resource and time for estimating the statistical properties of attributes
- A large search-space for the multiple attributes-based authentication schemes
- Nonlinearity of authentication systems
- New techniques required for timely detection of time-varying attributes and adaptation of authentication process

Figure 2.2: Comparison of cryptographic and physical authentication techniques.

A detailed comparison of conventional and physical authentication techniques is given in Figure 2.2.

Challenges for Existing Physical Layer Authentication Techniques

Although physical layer authentication has many advantages, it also faces many challenges. The main reason is that most of the existing physical layer authentication techniques rely on only a single attribute, as well as on static mechanisms while encountering the complex dynamic wireless environment of 5G-and-beyond wireless networks. As shown in Figure 2.2, the challenges for existing physical layer authentication techniques are summarized as follows.

- **Low reliability when using single attribute:** Performance of the single attribute-based physical layer authentication schemes suffers from the imperfect estimates and variations of the selected attribute [2]. Moreover, the limited range of specific attribute distribution may not be sufficient for differentiating transmitters all the time. This limits the performance of single attribute-based authentication schemes in many universal applications, such as mobile device security.

- **Difficulty in pre-designing a precise authentication model:** Most of the existing physical layer authentication schemes are model-based, as exemplified by [37, 49], which may be deteriorated when it is operated in a complex time-varying environment. More importantly, tremendous amounts of data and *a priori* knowledge are required for obtaining the accurate channel model, which are obviously undesirable for those mobile networks, such as unmanned aerial vehicle (UAV) networks and vehicular ad-hoc networks (VANETs). Hence, it is challenging to pre-design a precise authentication model for supporting new applications in 5G-and-beyond networks.

- **Impediment to continuous protection of legitimate devices:** Most of the existing authentication schemes are static in time and binary in nature, which means that the devices either pass or fail the authentication, thus leading to the one-time hard verification [37, 49]. Due to the intermittent communications between Alice and Bob, these schemes may be limited in detecting spoofer after the initial login and in addressing varying security risks.

- **Challenge of learning time-varying attributes:** Authentication performance of the existing static authentication schemes could be severely affected by the unpredictable variations of attributes due to the potential decorrelation at different time instants and device mobility. Hence, the variations of attributes increase the uncertainty for adversaries, but decrease the authentication accuracy of legitimate devices operating without learning the diverse attributes as well.

In addition, there are also some open issues for the adaptive authentication systems utilizing multiple physical layer attributes as follows:

- Limited computational resources for estimating the statistical properties of attributes for many IoT devices.
- Large search-space for finding the outcomes of authentication when multiple physical layer attributes are utilized.
- Nonlinear and non-convex characteristics of authentication systems.
- Timely detection of time-varying attributes and adaptation of the authentication process.

Due to these existing challenges, the authentication enhancement and efficient security provisioning are of paramount importance for 5G-and-beyond wireless networks.

2.2.2 Access Control

The access control mechanisms can be classified as encryption-based and encryption independent based on whether they use a particular encryption technique or are independent of the underlying encryption [147]. In the encryption-based approaches, the content providers encrypt their content before disseminating them into the network. Clients need to authenticate themselves and obtain the content decryption keys to be able to decrypt and consume the content. On the contrary, the encryption independent approaches provide access control frameworks that can use any encryption methods for performing access control.

The encryption-based approaches have been well studied in the literature [53, 54, 148]. A generalized hierarchical access control scheme named shared encryption-based construction is proposed in [53] by adding qualified users to the system via perfect secret sharing and symmetric encryption. This protocol defines alternative methods of accessing the system and allows the distribution of duties to different users. This paper also develops a secure key assignment scheme called threshold broadcast encryption-based construction. In [54], an attributed-based encryption mechanism is proposed for access control enforcement that uses either the key-policy or the ciphertext-policy based encryption models. The authors of [148] proposed a probabilistic structure for encryption-based access control. Publishers and clients are equipped with public-private key pairs and each client initially subscribes to a publisher by sending an interest. The publisher stores a record for each registered client and identifies the client's credentials.

Different from the encryption-based approaches, [149] proposes a trust-based approach for access control. During registration, a new client or publisher presents its credentials and attributes to the broker, thus trust is established. The publisher defines an access policy and submits it to its broker. In [50], a lightweight digital signature and access control scheme is developed for data networking. The access policies are enforced using generated tokens-metadata that indicate access levels. Two private tokens enable content access and integrity verification for each authorized entity. After receiving the entity's request for a token, the provider encrypts the token (generated by hashing a key vector) based on the requester's access level. In [51], an automated ConfigSynth framework is proposed to provide affordable and synthesizing precise network configuration. The proposed framework is further refined to provide improved security by developing a refinement mechanism. To prevent from international mobile subscriber identity downgrade attack with a fake LTE base station, a pseudonym-based solution and a mechanism to update LTE pseudonyms are proposed in [52].

2.2.3 Trust Management

Trust and reputation management systems can also be used in assessing the quality of received information, to provide network security services such as access control, authentication, malicious node detections, and secure resource sharing. According to [67, 68, 69, 150], definitions of trust and reputation are given respectively as: "A node A's trust in a node B is the subjective expectation of node A receiving positive outcomes from the interaction with node B in a specific context." and "Reputation is the global perception of a node's trustworthiness in a network." The concept of "Trust" originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [63]. The authors in [64] first introduced the term "Trust Management" and identified it as a separate component of security services in networks and clarified that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships." The concept of trust also has been attractive to communication and network protocol designers where trust relationships among participating nodes are critical in building cooperative and collaborative environments to optimize system objectives in terms of scalability, reconfigurability, and reliability, dependability, or security [65].

The trust management system usually contains multiple functional blocks: trust calculation, trust propagation, trust aggregation, and trust prediction. First of all, a trust value of the device/user will be calculated based on some metrics or recommendations. These trust values will be propagated in the network so that the trust can be established between devices which are not in immediate contact. While propagating the trust, trust values from multiple paths will be aggregated to get a combined trust value which can be stored in history. The stored trust value can be used in the trust predictions and this predicted trust value will be further used in the applications. The stored trust value can also be used in the trust computation in the form of feedback knowledge. Therefore, trust calculation, trust propagation, trust aggregation, and trust prediction blocks are closely interconnected in the trust management.

The authors in [70] proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks to effectively deal with selfish or malicious nodes. They considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. The authors of [71] proposed a 3-tier cloud-cloudlet device hierarchical trust-based service management protocol for large-scale mobile-cloud IoT systems. This protocol allows an IoT customer to report its service experiences and query its subjective service trust score toward an IoT service provider following a scalable report-and-query design. In [72], a trust management scheme is proposed for unattended wireless sensor networks to provide efficient and robust trust data storage and trust generation. For trust data storage, a geographic hash table is employed to identify storage nodes and to significantly decrease storage costs. The subjective logic-based consensus techniques are utilized in this work to mitigate trust fluctuations caused by environmental factors. To achieve accurate and energy-efficient trust evaluation in underwater acoustic sensor networks, an attack-resistant trust model is proposed in [73] based on multidimensional trust metrics, which mainly consists of three types of trust metrics, i.e., the link trust, data trust, and node trust.

2.2.4 Privacy Protection

In this subsection, privacy protection can be classified into three different categories, i.e., data privacy, location privacy, and identity privacy [55], which are summarized as follows.

- *Data privacy:* 5G-and-beyond networks allow users to utilize smart and data-intensive services, such as high-resolution streaming, healthcare [56], and smart metering [57], through the heterogeneous smart devices. To provide these services, the service providers may store and use private data of individuals without their permission. The stored data may be shared with other stakeholders so that they can analyze the data for their products. To mitigate such data privacy issues, service providers must provide clarification for the users not only how and where the individual's data have been stored, but also how and what purpose their data have been used. The authors in [58] argued that the standard formalization of differential privacy is stricter than that required by the intuitive privacy guarantee it seeks. In this work, several mechanisms to attain individual differential privacy are developed.

- *Location privacy:* More and more devices in 5G-and-beyond networks rely on ubiquitous location-based services [59]. Indeed, such services make users' life easier and more enjoyable but bring a plethora of privacy issues that of being continuously tracked as well. A scalable architecture is provided in [60] for protecting the location privacy from various privacy threats resulting from uncontrolled usage of location-based services. This architecture includes the development of a personalized location anonymization model and a suite of location perturbation algorithms. A flexible privacy personalization framework is used to support location k-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. This framework enables each mobile client to specify the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to accept when requesting k-anonymity-preserving location-based services.

- *Identity privacy:* It protects the identity-related information of a device/system/ user against attacks. As more and more devices are being connected to the network, it raises the probability of identity information leakage by adversaries [61]. The authors of [62] addressed the privacy risks of identity disclosures in sequential releases of a dynamic network. To prevent leakage of identity privacy, they proposed k^w-structural diversity anonymity, where k is an appreciated privacy level and w is a time period that an adversary can monitor a victim to collect the attack knowledge.

2.3 AI for Security, Trust, and Privacy Enhancement

2.3.1 Benefits of AI for Security, Trust, and Privacy

The artificial intelligence (AI) [74] is leveraged in this thesis to enhance security, trust, and privacy in 5G-and-beyond networks through learning, reasoning, and self-correction. Explicitly, AI techniques could be exploited at gateways and routers, and the abundant information contained in large-scale wireless communication systems could be utilized for learning and reasoning, thus achieving security enhancement and trust management based on learned knowledge. Moreover, through self-correction by AI techniques, the intelligent security provisioning and trust management may be accomplished to adapt to dynamic wireless environments. To be more specific, AI may contribute to the secure communications in 5G-and-beyond networks due to the following reasons.

- **Security management may be accelerated based on learned knowledge by AI.** In a large-scale communication system, the gateways and routers may undertake the AI management, such as data collection, training, and testing, thus the communication and computation overhead could be reduced at low-power devices. They also have abundant multi-domain information on communication channels, devices, environments, network connections, and application software. Such information could be intelligently utilized for security provisioning as well as for contributing to the learning and reasoning by AI techniques. More importantly, AI techniques may utilize historical information to facilitate security management. Hence, the continuous security process at devices could be accelerated as well as the security induced latency could be reduced based on learned knowledge by AI techniques.

- **AI provides real-time learning under limited statistical properties and unpredictable dynamics.** In the practical communication environment, it is more and more difficult to develop accurate statistical models for security enhancement. This is mainly because of the ubiquitous uncertainties and unpredictable dynamics as well as the limited computational resources and time for obtaining precise statistical properties. Those AI techniques providing online learning under limited statistical properties and unpredictable dynamics could conduce to the real-time detection of attacks and continuous protections for legitimate communications. Furthermore, different from the statistical hypothesis testing [75], which requires an accurate statistical model, the machine learning algorithms allow systems to become more accurate in predicting outcomes based on the training data.

- **Automatic management may be achieved with the help of AI techniques.** With the significant increasing requirements in 5G-and-beyond, automatic management helps to meet different goals, for example, quality of service (QoS), security enhancement, trust establishment, and privacy protection. This can be achieved based on the learning of the dynamic situations of the time-varying systems by AI techniques, thus the different goals can be automatically adjusted in the process of communications. More importantly, the objective-aware techniques can be designed utilizing AI to provide benefits for more efficient management in dynamic environments.

- **Privacy protection in security management may be achieved based on AI.** As the leaked private information of a device/user could be leveraged by attackers, leading to security risks and lack of trust, privacy protection in the security management process is extremely important. With the help of AI, intelligent security provisioning may be designed by utilizing the channel reciprocity [21] as well as by tracking the specific communication link-related, device-related, and biometric features without the transmission of private information. To be more specific, AI techniques may help in amplifying the channel reciprocity, so that highly similar information can be acquired on transceiver sides. Moreover, machine learning algorithms can track the specific features for continuous security management without the transmission of private information [2].

Therefore, through leveraging AI, new intelligent security provisioning and trust management schemes can be developed in large-scale 5G-and-beyond networks.

2.3.2 Categories of Machine Learning for Intelligent Management

The family of machine learning algorithms can be categorized based on their functionality and structure [1], yielding regression algorithms, decision tree algorithms, Bayesian algorithms, clustering algorithms, and artificial neural networks, just to name a few. In this subsection, machine learning techniques are clarified from two perspectives: parametric/non-parametric learning and supervised/unsupervised/reinforcement learning, as illustrated in Figure 2.3. The adjectives "parametric/non-parametric" indicate whether there are specific forms of training functions, while "supervised/unsupervised" indicate whether there are labeled samples in the database. The focus of reinforcement learning is finding a balance between exploration of uncharted territory and the exploitation of current knowledge. The basic concepts and typical examples of these machine learning techniques will be introduced, more importantly, their applications and possible requirements in designing intelligent security provisioning and trust management approaches will be discussed for different wireless communication scenarios.

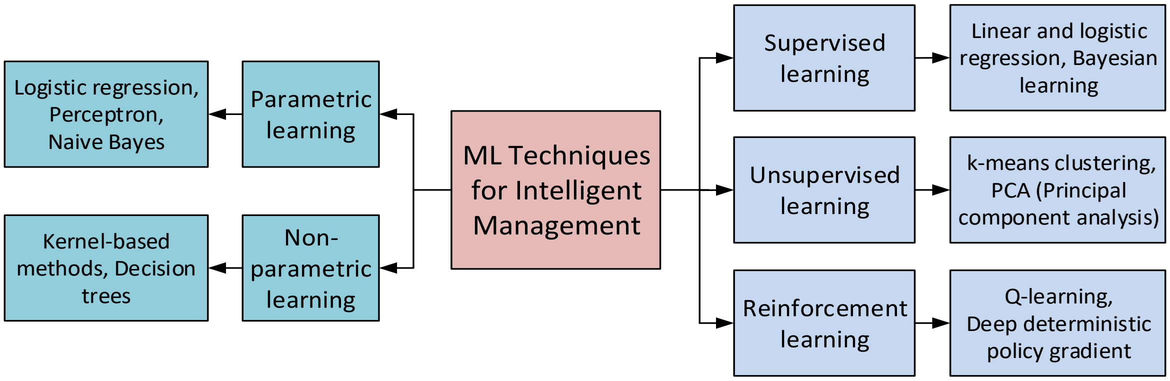

ML Techniques for Intelligent Management
Parametric learning
Logistic regression, Perceptron, Naive Bayes
Non-parametric learning
Kernel-based methods, Decision trees
Supervised learning
Linear and logistic regression, Bayesian learning
Unsupervised learning
k-means clustering, PCA (Principal component analysis)
Reinforcement learning
Q-learning, Deep deterministic policy gradient

Figure 2.3: Categories of machine learning (ML) techniques for intelligent security provisioning and trust management.

Parametric Learning Methods

The family of parametric learning methods has become mature in the literature, as exemplified by the logistic regression, linear discriminant analysis, perceptron, and naive Bayes, which require the specific form of training functions [76]. When the training functions related to the training samples (i.e., the collection of multi-dimensional information) are selected appropriately, the parametric learning methods could be more accurate, simpler, and require fewer training samples than the non-parametric learning methods.

In the intelligent physical layer authentication schemes, the parametric learning methods could model the communication link-related attributes independently based on the specific form of training functions, and the uncertainties caused by the complex time-varying environment may be circumvented. The communication overhead and complexity of training may be adjusted adaptively by opportunistically leveraging attributes. However, this kind of learning methods may be challenged in 5G-and-beyond wireless communication scenarios wherein the statistic properties and a priori knowledge of attributes are not at hand.

Non-Parametric Learning Methods

In contrast to parametric learning methods, the non-parametric learning methods [1, 2, 76] are not specified *a priori*, but are determined from the available data. Examples include kernel estimator, k-nearest neighbors, and decision trees, just to name a few. A kernel machine-based scheme for intelligent physical layer authentication process is proposed in [2]. The dimensionality of multiple attribute-based authentication systems is reduced by the kernel function and the resultant authentication process can be modeled as a linear system, thus decreasing the computation complexity of the authentication process, even though a large number of attributes are utilized. More importantly, the proposed kernel learning algorithm tracks the time-varying attributes to enhance security based on continuous device validation.

The non-parametric learning methods dynamically learn from the time-varying environments without requiring any assumptions concerning the training models. Beneficially, this provides higher flexibility for intelligent management, especially in those time-varying scenarios, where the computational resources and time available for obtaining the statistical properties of attributes and training functions are limited. However, compared with the parametric learning methods, they require more training data (i.e., collection of multi-dimensional information and/or their corresponding labels) and may result in overfitting.

Supervised Learning Techniques

The main difference between supervised and unsupervised learning algorithms is that supervised learning requires the prior knowledge of outputs for the corresponding inputs, while unsupervised learning algorithms do not need labeled outputs. Some supervised machine learning algorithms are studied in [76] for defending against the false data injection attacks, such as the perceptron, k-nearest neighbors, and support vector machines (SVM). In intelligent management, the choice between supervised or unsupervised machine learning algorithms typically depends on the problem and volume of training data at hand. A supervised learning algorithm is suitable when training data and corresponding outputs of a legitimate communication session are straightforward to obtain. More explicitly, the labeled outputs should be required near-instantaneously, so that the adaptation of the management process may be achieved in real-time. When labeled outputs are not at hand, fast labeling techniques may be helpful for the supervised learning-based intelligent management.

Unsupervised Learning Techniques

In exploring this kind of algorithms, the learner exclusively receives unlabeled training data and makes predictions for all unobserved points, as exemplified by the K-means clustering [1]. For instance, in physical layer authentication scenarios wherein the samples of a legitimate device (i.e., estimates of attributes) are much more than that of Spoofer, unsupervised learning algorithms may be introduced for intelligent authentication. It is reasonable since the spoofing attacks fully rely on the legitimate device's behaviors for better attacking performance, including the transmission protocols and attributes. Through applying unsupervised machine learning techniques for security enhancement and trust management, the time latency and energy consumption for labeling the outputs will be significantly decreased.

Reinforcement Learning Techniques

They do not require accurate inputs and outputs as well as precise parameter updates. A Q-learning-based authentication scheme is proposed in [78] depending on the received signal strength indicator of signals to achieve the optimal test threshold and to improve the authentication accuracy. However, it is also a static authentication scheme and maybe unsuitable when the available resources and time are limited for obtaining complete information, i.e., the environment and agent states as well as the immediate reward for each action of devices.

2.3.3 AI-based Security Provisioning

As shown in Figure 2.4, a design of machine learning-aided intelligent authentication approaches is introduced as an example by utilizing multi-dimensional attributes and by optimizing the holistic authentication process.

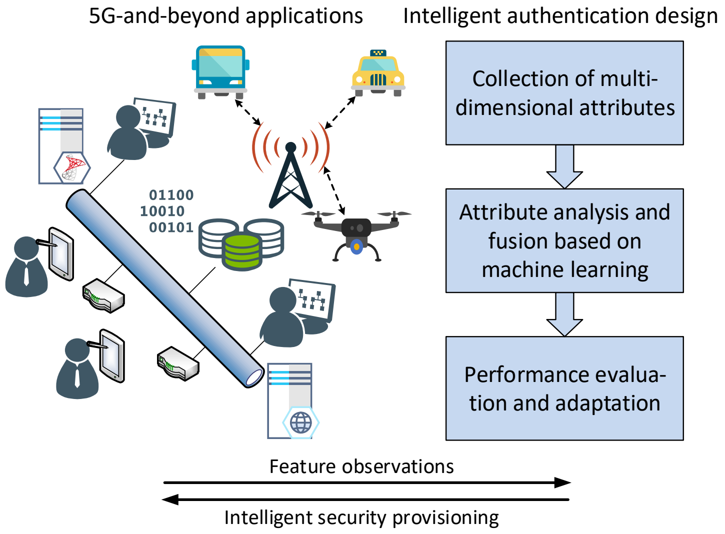

5G-and-beyond applications
Intelligent authentication design
Collection of multi-dimensional attributes
Attribute analysis and fusion based on machine learning
Performance evaluation and adaptation
01100
10010
00101
Feature observations
Intelligent security provisioning

Figure 2.4: Framework diagram of intelligent authentication design.

Phase I: The time-varying multi-dimensional attributes are collected for authentication, which may be estimated imperfectly having noises and measurement errors. Examples include the physical layer attributes, network selection in heterogeneous wireless networks, and mobility patterns. In a specific 5G-and-beyond wireless communication scenario, those attributes providing more information for authentication may be selected first. In detail, the independent attributes having a broader distribution range and a higher estimation accuracy could offer more information for distinguishing different transmitters. By utilizing multi-dimensional attributes as well as sharing the information among different layers and networks, the reliability of authentication will be improved. Explicitly, the design of intelligent authentication only relies on the estimation data of attributes without requiring a precise structure of the time-varying attributes, e.g., the channel model, resulting in model-free device validation.

Phase II: The multi-dimensional attributes can be fused for authentication based on machine learning techniques. An example is given in [2], which is a kernel learning-based physical layer authentication scheme. Considering the time-varying network conditions, such as the resource limitations and uncertainties, the attributes may be opportunistically selected for dealing with both communication overhead and security management concurrently. Furthermore, developing an appropriate machine learning algorithm and reducing the dimension of the authentication system will also benefit communication performance, thus cost-effective authentication will be achieved.

Phase III: The authentication for a legitimate device and a spoofer can be conducted based on the new collection of multi-dimensional attributes. To achieve this, the regression or classification model should be built based on the training data collected from them. Then the authentication performance can be evaluated, and the authentication process can be adapted to the complex time-varying environment by exploring machine learning to track the variations of multi-dimensional attributes. Hence, the continuous and situation-aware process is proposed for intelligent security provisioning in 5G-and-beyond applications.

2.4 Chapter Summary

This chapter firstly introduced the threats and risks in 5G-and-beyond networks as well as some existing solutions for secure communications, including authentication, access control, trust management, and privacy protection techniques. The challenges for the conventional techniques and the advantages of artificial intelligence were presented. Then, the machine learning paradigms for intelligent management were classified into parametric and non-parametric learning methods, as well as supervised, unsupervised, and reinforcement learning techniques. Based on the preliminaries provided in this chapter, new intelligent security provisioning and trust management schemes will be developed in the following chapters.

Chapter 3

Physical Layer Authentication as an Intelligent Process

Physical layer authentication techniques validate wireless transmitters by verifying the dynamic attributes of the associated physical communication links, devices, location, and environment. Performance of the existing physical layer authentication schemes could be severely affected by the imperfect estimates and the variations of the communication link attributes. The commonly adopted static hypothesis testing for physical layer authentication faces significant challenges in time-varying communication channels due to the changing propagation and interference conditions, which are typically unknown at the design stage. To circumvent this impediment, two multi-dimensional adaptive physical layer authentication schemes are proposed based on artificial intelligence (AI) techniques as an intelligent process in this chapter to learn and utilize the complex time-varying environment, and hence to improve the reliability and robustness of physical layer authentication. These two schemes are named as kernel learning-based authentication scheme and fuzzy learning-based authentication scheme.

3.1 Introduction

Due to the open broadcast nature of radio signal propagation, as well as owing to using standardized transmission schemes and intermittent communications, wireless communication systems are extremely vulnerable to interception and spoofing attacks. First of all, the open broadcast nature of wireless medium facilitates the reception of radio signals by any illegitimate receiver within the coverage of the transmitter [25]. Secondly, the standardized transmission and conventional security schemes of wireless networks make interception and eavesdropping fairly straightforward [79, 80]. Moreover, the "on-off" and sporadic transmissions of low cost wireless devices, especially the significantly growing number of Internet-of-Things (IoT) devices, provide abundant opportunities to adversaries for spoofing attacks. Therefore, the enhancement of authentication schemes is of paramount importance for wireless communication systems, especially in the light of the ongoing convergence between the wireless infrastructure and vertical industrial applications enabled by IoT.

Physical layer authentication technique provides an effective approach for authenticating a user (transmitter) by exploiting the physical layer attributes of its communication links. However, imperfect estimates and variations of the physical layer attributes are inevitable in practical wireless networks. These constitute challenges for the physical layer authentication, but beneficially, they provide unique distinguishing features. Having said that, their adequate estimation often imposes challenges on physical layer authentication, mainly due to time-varying channels, dynamic interference conditions, mobility of devices, non-symmetrical observations at the transmitter and receiver, as well as owing to the measurement errors, just to name a few.

To elaborate a little further on the challenges, the performance of the single-attribute-based physical layer authentication schemes [31, 36, 37, 38, 41, 42, 43, 44, 45, 46, 48] remains limited by the imperfect estimates of the specific attribute used. Moreover, the limited range of the specific attribute distribution may not be sufficiently wide-spread for differentiating the devices all the time. These estimations lead to low-reliability and low-robustness of physical layer authentication in conjunction with only a single attribute, especially in a hostile time-varying wireless communication environment.

Hence, multiple physical layer attributes may be taken into account for improving the authentication performance [30, 81], since it is more difficult for an adversary to succeed in predicting or imitating all the attributes based on the received signal. On the other hand, when the environment is time-variant, the performance of physical layer authentication could be severely affected by the unpredictable variations of attributes due to the potential decorrelation of the physical layer attributes observed at different time instants. Although the variations of attributes provide additional scope for improving the security mechanisms by increasing the uncertainty for the adversaries, at the same time also brings challenges for the legitimate users operating without discovering and tracking the variations of physical layer attributes.

In a nutshell, the main challenge is that a multiple varying attributes-based authentication scheme is capable of achieving high security in the presence of adversaries, but this increases the grade of challenge imposed on legitimate users as well. More importantly, variations of the physical layer attributes are typically unknown at the design stage and they are hard to predict, thus it is very difficult to pre-design a static physical layer authentication scheme. Hence the conception of adaptive physical layer authentication is extremely helpful for improving the validation performance, which can promptly adapt to the time-varying environment.

There are in general two classes of methodologies in the literature available for combining the multiple physical layer attributes for authentication. The first one is the nonparametric methods [96, 97, 98, 99, 100], which can be used for combining multiple attributes without a fixed form (structure) of the authentication model. The other one is the parametric methods, where the forms of system expression are given, as exemplified by the Gaussian function and polynomial function [101, 102, 103]. The details of these two classes of methodologies have been introduced in subsection 2.3.2.

3.1.1 Kernel Learning-based Authentication Scheme

When the statistical properties of the physical layer attributes are limited, designing near-instantaneously adaptive physical layer authentication based on multiple attributes is challenging due to the following reasons:

C1. Both the computational resources and the time available for estimating the statistical properties of the physical layer attributes are limited;

C2. New authentication schemes based on multiple attributes result in a large search-space, which may lead to both excessive complexity and non-convex property in optimization;

C3. In practical wireless communication, the typical authentication schemes rely on nonlinear techniques, as exemplified by the binary hypothesis tests of [42, 43, 44] and by the generalized likelihood ratio test of [82];

C4. Sophisticated near-instantaneously adaptive processing techniques are required for fast detection of time-varying physical layer attributes and the adaptation of the physical layer authentication process.

To overcome these difficulties, the kernel-based machine learning technique of [83, 84] is applied first for modeling the authentication problem in this chapter, which is a non-parametric learning method. Although the family of parametric learning methods has become mature in the literature [39, 87, 88, 89, 90, 91, 92], they usually rely on the assumption of knowing the distribution of samples (i.e., the estimates of physical layer attributes) together with the specific form of the authentication model (e.g., based on linear function or polynomial function). When the assumptions related to the samples' distribution are correct, the parametric methods are usually more accurate than the non-parametric methods. However, once the assumptions concerning the samples' distribution models become inaccurate, they have a much greater chance of failing. This dramatically limits the employment of parametric learning methods when they face challenge **C1**, since computing accurate distributions for multiple physical layer attributes in a complex time-varying environment is indeed time-consuming. In contrast to parametric learning methods, the non-parametric methods are not specified *a priori*, but are determined from the data available. Some examples are constituted by the classic k-nearest neighbors [93] and the decision tree based solutions [94]. However, these two non-parametric methods have a limited ability to deal with challenges **C2**-**C4**. To be specific, it is not easy to determine the most appropriate k-distance in the k-nearest neighbors method. In the decision tree method, the perturbation of collected data (e.g., by noise) will result in quite a different decision tree, thus leading to inaccurate authentication results.

The authors of [75] proposed a physical layer authentication scheme based on the extreme learning machine for improving the spoofing detection accuracy. However, this scheme assumes that all the multiple physical layer attributes obey the same statistical distribution functions, such as the Gaussian distributions, thus their performance is limited in the complex high-dynamic environments. Furthermore, a few other machine learning techniques are introduced for authentication in [77], such as Q-learning and neural network-based techniques, as well as some well-studied fusion methods, e.g., the Kalman filter of [37], fuzzy logic of [95], and Bayesian inference techniques of [75]. However, these methods may be limited in dealing with **C1-C4**. To be specific, the authors of [77] studied the test threshold of authentication based on the Q-learning technique instead of the variations of attributes in the time-varying environment encountered. The neural network-based method of [77] may improve the model accuracy by increasing the number of layers and neurons used, but at the cost of a higher complexity, which hence may not be suitable for near-instantaneous authentication. Moreover, the Kalman filter aided method of [37] is also model-based, relying on the assumption of having Gaussian distributed process noise, the fuzzy logic method of [95] requires tuning of the membership function, and the Bayesian inference method of [75] also requires a statistical model of the observed data, which are hence limited in dealling with challenge **C1**.

To overcome these challenges, a promising alternative approach of modeling the authentication process is to track multiple physical layer attributes based on the kernel learning [85, 86]. As a benefit, the kernel machine of [83, 84, 85, 86] is capable of reducing the dimensionality of the authentication problem based on multiple attributes. It models the authentication problem as a linear system without requiring the knowledge of the attributes' statistical properties. More importantly, the variations of attributes as well as of the environment may be tracked (learnt) by the kernel learning. Due to these compelling benefits, this chapter first proposes a novel authentication scheme based on the kernel learning technique as an intelligent process in the face of time-varying wireless communication scenarios to achieve reliable authentication through discovering the complex dynamic environment encountered and through tracking the variations of multiple physical layer attributes. Firstly, a multiple physical layer attribute fusion model based on the classic kernel machine is designed for modeling the authentication problem without requiring the knowledge of those attributes' statistical properties, which corresponds to **C1**. As for **C2** and **C3**, the authentication problem is cast from a high-dimensional search space to a single-dimensional space by using the classic Gaussian kernel, hence the resultant physical layer authentication can be considered as a linear system. Then an adaptive algorithm is proposed for tracking the variations of the physical layer attributes to achieve a reliable authentication performance, which is a solution for **C4**.

Specifically, the technical contributions of the proposed kernel learning-based physical layer authentication scheme are summarized as follows:

- A kernel machine-based model for determining the authentication attributes is designed without requiring the knowledge of their statistical properties, and the authentication system is cast from a high-dimensional space to a single-dimensional space. Then the resultant physical layer authentication process can be considered as a linear system, which is easier to train based on the estimates of the physical layer attributes and the observed authentication results. As a result of this transformation, the complexity of the designed multiple physical layer attribute fusion model can be dramatically reduced, despite considering a high number of physical layer attributes;

- The learning (training) objective of the physical layer authentication based on kernel machine can be formulated as a convex problem. An intelligent authentication process is proposed based on kernel least-mean-square for tracking the variations of the physical layer attributes to achieve a reliable authentication performance. By deriving the learning rules for both the system parameters and for the authentication system, the proposed intelligent authentication process becomes capable of adapting to time-varying environments. Therefore, a timely detection of the physical layer attributes and the adjustment of the authentication process can be achieved;

- Numerical performance and simulations results demonstrate that a larger number of physical layer attributes leads to a more pronounced authentication performance improvement without unduly degrading the convergence and training performance. The results also demonstrate the superiority of the kernel learning-based scheme over its non-adaptive benchmarker.

3.1.2 Fuzzy Learning-based Authentication Scheme

When some statistical properties of the physical layer attributes are available and intermittent availability of some attributes are considered, the fuzzy theory [104, 105, 106, 107, 108] is leveraged for combining multiple attributes. It is because fuzzy models or sets are mathematical means of representing vagueness and imprecise information, then make decisions based on the imprecise and non-numerical information. To be more specific, a fuzzy membership function is used as a generalization of the indicator function in classical sets and represents the degree of truth as an extension of valuation. Hence, it provides an effective method to combine multiple attribute and to deal with the imperfectness of attribute estimation for achieving accurate authentication. Furthermore, knowing that the fuzzy model using membership function is a parametric method, the authentication scheme based on fuzzy model can be seen as a compact approach. In a nutshell, through the fuzzy theory, the authentication system can be well modelled by using a specific expression to combine multiple attributes.

Compared with the parametric methods [101, 102, 103], more observed samples of the adopted attributes are required in building the authentication model by using the nonparametric methods, leading to a larger number of parameters in the authentication process to be determined. Although sufficient observations of the adopted physical layer attributes may be available in some networks, longer time for estimating attributes and larger memory space for storing them are required in leveraging such methodologies. In the parametric methods, given a fixed form of authentication model with only parameters to be determined, more information has already been involved in attribute combination, thus resulting in less parameters to be determined when compared to the nonparametric methods, hence demonstrating a compact approach.

More importantly, the adopted physical layer attributes in the authentication process are time-varying and their variations may be difficult to predict, due to the uncertainties and dynamics of communication environments, i.e., the estimation imperfectness, time-varying characteristic of attributes, and intermittent availability of some attributes. In the attribute estimation stage, the estimates of some attributes may not be available by the receiver at some moments because of the complex communication environment or the unreliable estimation components. These all lead to a low authentication performance of the schemes without an adaptive mechanism to overcome the uncertainties and dynamics, as exemplified by [35, 36, 37, 38, 39]. In detail, to achieve a reliable and robust authentication, an adaptive scheme is extremely helpful in near-instantaneously updating the system parameters, so that they will remain unknown to the adversaries.

In this chapter, a fuzzy theory-based adaptive authentication scheme is developed by utilizing multiple physical layer attributes to improve authentication performance in time-varying environments. First of all, a fuzzy model is designed for combining multiple physical layer attributes with imperfect estimation, which forms multi-dimensional protections for legitimate devices. In order to update system parameters to achieve adaptive authentication, the false alarm rate and misdetection rate of the fuzzy learning-based scheme are derived. Note that updating the system parameters is a non-convex optimization problem. To improve the efficiency of learning, system parameters in the proposed fuzzy multiple attribute combination model are divided into two classes, named linear parameters and nonlinear parameters. Then, a hybrid learning algorithm is proposed for near-instantaneously updating the system parameters, wherein the least-square estimator is applied for linear parameter update and the gradient decent is used for nonlinear parameters update.

Specifically, the technical contributions of the proposed adaptive fuzzy learning-based physical layer authentication scheme are summarized as follows:

- The designed fuzzy model relaxes the accuracy requirement of attribute estimation and provides an explicit expression of multiple physical layer attribute combination. Compared with the non-parametric methods, the proposed fuzzy multiple attribute combination model requires much less observed samples and less parameters to be determined in the authentication process due to the given form of system expression, leading to a compact approach;

- The proposed hybrid learning algorithm achieves reliable and robust authentication in time-varying environments. On one hand, the system parameters can be updated near-instantaneously by the adaptive learning algorithm. On the other hand, each attribute in the adaptive authentication model is independently taken into account, thus once some attributes are unavailable at some moments, the remaining attributes still contribute to the authentication model and make the model work, demonstrating a robust approach;

- Simulation results demonstrate the parameter update and authentication performance of the proposed fuzzy learning-based scheme in simulated urban scenario. Moreover, compared with some existing authentication schemes, the outperformance of the proposed fuzzy learning-based scheme in defending against the spoofing attacks is shown in dynamic environments.

The rest of this chapter is organized as follows. In Section 3.2, the system model used in this chapter is presented. In Section 3.3, the kernel learning-based physical layer authentication scheme is proposed. The fuzzy learning-based physical layer authentication scheme is developed in Section 3.4. Finally, Section 3.5 concludes this chapter.

Table 3.1: Notations of Chapter 3

Notations	Definitions
N	Number of physical layer attributes used for authentication.
$\boldsymbol{H}$	Estimates of multiple physical layer attributes.
$\mathcal{F}(\cdot)$	Intelligent adaptive function for physical layer authentication.
ν	Authentication threshold.
L	Number of observations for training.
$\boldsymbol{\alpha}$	Weight vector of Kernel machine.
μ	Step-size parameter of Kernel machine learning.
σ_κ	Kernel width.
e	Prediction error in the training process.
P_{FA}	False alarm rate.
P_{MD}	Misdetection rate.
Φ_0	The case that the signal is from Alice.
Φ_1	The case that the signal is from Eve.
$\widehat{\mu}$	Mean of Gaussian fuzzy function in fuzzy learning-based scheme.
$\widehat{\sigma}$	Variance of Gaussian fuzzy function in fuzzy learning-based scheme.
$\widehat{\alpha}$	Linear system parameter of fuzzy learning-based scheme.

Notations: In this chapter, scalars are denoted by italic letters, while vectors are respectively denoted by bold-face letters. False alarm (FA) represents an event when the receiver wrongly believes that the legitimate transmitter is an adversary, while misdetection (MD) is an event when the receiver wrongly identifies the adversary as a legitimate device. Table 3.1 shows the notations of this chapter.

3.2 System Model and Problem Formulation

As shown in Figure 3.1, a wireless network is considered, where Alice and Bob communicate with each other in the presence of an eavesdropper, i.e., Eve, who intends to intercept and impersonate Alice, and then to send spoofing signals to obtain illegal advantages. Bob's main objective is to uniquely and unambiguously identify the transmitter by physical layer authentication. The basic physical layer authentication aims for supporting this pair of legitimate devices by a reciprocal wireless link, while the device-dependent features can be used as a unique security signature.

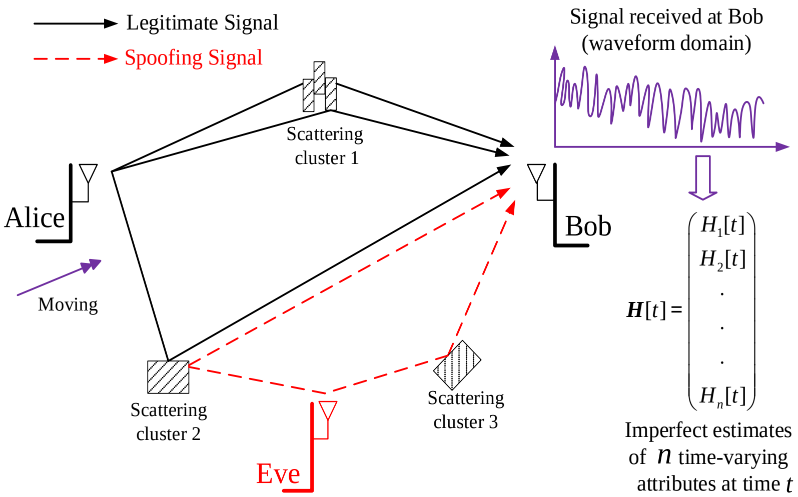


Figure 3.1: Adversarial system and physical layer authentication in a wireless network.

The number of physical layer attributes used for authentication is denoted as N and the estimates of multiple physical layer attributes are denoted as $\boldsymbol{H} = (H_1, H_2, ..., H_N)^{\mathrm{T}}$, where T represents the transposition of a vector. These physical layer attributes may include the channel state information (CSI), carrier frequency offset (CFO), received signal strength indicator (RSSI), round-trip time (RTT), in-phase-quadrature-phase imbalance (IQI), and so on. These unique channel and device features offer security guarantee by physical layer authentication.

A few important assumptions are stipulated for the authentication considered in this chapter, as follows:

Assumption 3.1. The physical signals transmitted between a pair of legitimate devices rapidly become decorrelated in space, time and frequency. This implies that it is hard for the attacker to observe and predict the channel state between legitimate devices if the attacker is at a third location, which is farther than a wavelength away from Alice and Bob;

Assumption 3.2. Both the wireless channels and the interference are time-varying, the devices are moving, and hence the wireless environment is dynamically changing. These all lead to unpredictable variations of the physical layer attributes;

Assumption 3.3. The estimates of the physical layer attributes are imperfect because the legitimate devices will suffer from different interferences in a dynamic propagation environment when the devices roam in different locations.

These assumptions characterize a practical scenario, but naturally, it will be more difficult to deal with these imperfectly estimated time-varying physical layer attributes.

The physical layer authentication comprises two phases, as described below.

Phase I: Alice broadcasts one or more messages to Bob at time t. From the received signal, Bob infers an imperfect estimate of the multiple attributes

$$\boldsymbol{H}_A^I[t] = (H_{A1}^I[t], H_{A2}^I[t], ..., H_{AN}^I[t])^{\mathrm{T}}, \tag{3.1}$$

which are associated with Alice. At the same time, Eve overhears the transmission.

Phase II: Either Alice or Eve transmits a message to Bob at time $t + \tau$. Then Bob obtains another imperfect estimate

$$\boldsymbol{H}^{II}[t+\tau] = (H_1^{II}[t+\tau], H_2^{II}[t+\tau], ..., H_N^{II}[t+\tau])^{\mathrm{T}}, \tag{3.2}$$

where τ represents the time interval between the two phases.

Bob should compare the estimate $\boldsymbol{H}^{II}[t+\tau]$ to the previous estimate $\boldsymbol{H}_A^I[t]$. If these two estimates are likely to be originated from the same channel realization and the same imperfect hardware, then the message at time $t + \tau$ is deemed to be coming from Alice.

Remark 3.1. As mentioned in the assumptions, the physical layer attributes are time-variant and imperfectly estimated. The objective of this chapter is to propose authentication schemes as an intelligent process relying on these physical layer attributes. The process aims for achieving reliable and robust authentication through discovering and learning the complex operating environment. Two physical layer authentication schemes will be proposed for specific communication scenarios, i.e., kernel learning-based scheme for the case that the properties of the attributes are not available and fuzzy learning-based scheme based on the known properties (which are not perfectly estimated).

An intelligent adaptive function $\mathcal{F}(\cdot)$ is conceived, which is used for fusing N independent physical layer attributes. Then the authentication process can be formulated relying on a threshold $\nu > 0$ as

$$\begin{cases} \Phi_0 : & |\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| \le \nu; \\ \Phi_1 : & |\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| > \nu, \end{cases} \tag{3.3}$$

where Φ_0 indicates that the signal is from Alice, while Φ_1 indicates that it is from Eve. Due to the variations and imperfect estimates of the physical layer attributes between Alice and Bob, both false alarms and misdetections are encountered. Therefore, the parameters in $\mathcal{F}(\cdot)$ should be promptly updated to achieve low false alarm rate and misdetection rate in a time-varying environment.

3.3 Kernel Learning-based Authentication Scheme

In order to improve the performance of the authentication schemes using multiple physical layer attributes, which are imperfectly estimated and time-varying, a kernel machine-based model is proposed for fusing multiple physical layer attributes without requiring the knowledge of their statical properties in the spirit of **C1**. Then, the dimension of the search-space is reduced from N to 1 with the aid of the developed kernel machine-based physical layer attribute fusion model and the authentication problem can be modeled by a linear system as detailed in this section (corresponding to **C2** and **C3**). Therefore, the complexity of the designed multiple physical layer attribute fusion model can be dramatically reduced, as well as the trade-off between the authentication false alarm and misdetection can be improved by utilizing multiple attributes.

3.3.1 Kernel Machine-based Multiple Physical Layer Attribute Fusion

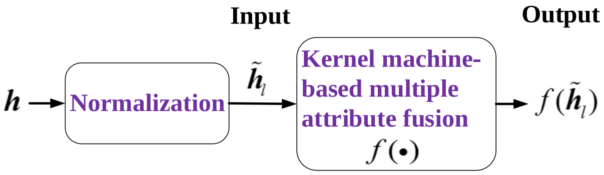

Input
Output
$\boldsymbol{h}$
Normalization
$\tilde{\boldsymbol{h}}_l$
Kernel machine-based multiple attribute fusion $f(\bullet)$
$f(\tilde{\boldsymbol{h}}_l)$

Figure 3.2: Kernel machine-based multiple physical layer attribute fusion.

In the kernel machine-based multiple attribute fusion, Bob will obtain an estimate $\boldsymbol{H}^{II}[t+\tau]$ of (3.2) at time $t+\tau$. Then, Bob will compare the estimate $\boldsymbol{H}^{II}[t+\tau]$ to the previous estimate at time t, namely for $\boldsymbol{H}_A^I[t]$ of (3.1). The difference between these two estimates is denoted as

$\boldsymbol{h} = (h_1, h_2, ..., h_N)^{\mathrm{T}}$, where each $h_n \in [a_n, b_n]$ is formulated as

$$h_n = H^I_{An}[t] - H^{II}_n[t + \tau],\ n = 1, 2, ..., N. \tag{3.4}$$

Since the different attributes exhibit quite different ranges and have different units, the normalization (see Figure 3.2) is required for scaling the attributes having different ranges to the same range for the ease of analysis and for the design of the kernel machine-based fusion. In the following, the attributes having ranges $[a_n, b_n], n = 1, 2, ..., N$, are normalized to $[-1, 1]$ by invoking

$$\widetilde{h}_n = \frac{2}{b_n - a_n}(h_n - \frac{a_n + b_n}{2}),\ n = 1, 2, ..., N. \tag{3.5}$$

It can be observed from (3.4) and (3.5) that these two equations are only used for normalizing the estimates of the attributes to the range of $[-1, 1]$, so that the rather diverse multiple physical layer attributes can be processed in the same range. In practical systems, only the approximate variation ranges of the attributes are required, which is reasonable because there always have *a priori* knowledge about the communication systems and environments before designing the authentication system.

Let us assume that a set of observations $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)^L_{l=1} \in [-1, 1]^N \times \{0, 1\}$ is given, which is used for training the authentication process, where $\widetilde{\boldsymbol{h}}_l = (\widetilde{h}_{1l}, \widetilde{h}_{2l}, ..., \widetilde{h}_{Nl})^{\mathrm{T}}$ is the lth estimate after the normalization, with each element $\widetilde{h}_{nl}$ defined in (3.5), and

$$\widehat{y}_l = \begin{cases} 1 & \Phi_0 \\ 0 & \Phi_1 \end{cases}. \tag{3.6}$$

As shown in Figure 3.2, the normalized estimates $\widetilde{\boldsymbol{h}}_l, l = 1, 2, ..., L$, are considered as the inputs of the kernel machine, and $f(\widetilde{\boldsymbol{h}}_l)$ represent the outputs of the kernel machine with the corresponding inputs given by $\widetilde{\boldsymbol{h}}_l \in [-1, 1]^N, l = 1, 2, ..., L$. Note that for the legitimate users, the training data of a legitimate communication session is relatively straightforward to obtain.

The task is then to infer the underlying mapping function $\widehat{y}_l = f(\widetilde{\boldsymbol{h}}_l)$ from the training data set (the samples) received $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)^L_{l=1} \in [-1, 1]^N \times \{0, 1\}$. In other words, the task in this section is to represent the authentication system $\widehat{y_l} = f(\widetilde{\boldsymbol{h}}_l)$, and to model the relationship between the estimates of multiple attributes and the corresponding authentication results. After this, it can be verified whether a transmitter is that of Alice or of Eve once a new normalized estimate $\overline{\boldsymbol{h}} = (\overline{h}_1, \overline{h}_2, ..., \overline{h}_N)^{\mathrm{T}}$ has been obtained. For example, in a continuous authentication session as defined in [48], once the transmitter accesses the system again or sends the messages to Bob continuously, Bob can infer the estimates of this transmitter's physical attributes, and then determine its normalized estimate through (3.5). This normalized estimate may be different from the previous normalized estimates $\widetilde{\boldsymbol{h}}_l, l = 1, 2, ..., L$, because of the time-varying environment or channels, which will be treated as the new normalized estimate of the attributes and be applied to the authentication to improve the security.

The kernel machine projects the N-dimensional input vector $\overline{\boldsymbol{h}} \in [-1, 1]^N$ into a potentially infinite-dimensional feature space $\mathcal{H}$ through a mapping $\varphi : [-1, 1]^N \to \mathcal{H}$. Note that the transformation from the input space into the feature space is nonlinear, and the dimensionality of the feature space is high enough. Since the linear model defined in feature space $\mathcal{H}$ satisfies the *universal approximation property* of [29], the authentication system can be expressed as

$$f(\overline{\boldsymbol{h}}) = \boldsymbol{w}^{\mathrm{T}}\varphi(\overline{\boldsymbol{h}}), \tag{3.7}$$

where $\boldsymbol{w}$ is the weight vector in the feature space $\mathcal{H}$. According to the *Representer Theorem* of [109, 110], the authentication system expression of (3.7) can be rewritten as

$$f(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}), \tag{3.8}$$

where $\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}})$ is a Mercer kernel [83]. The classic Gaussian kernel function of [83, 84, 85, 86] is adopted in this chapter, which has an excellent modelling capability and is numerically stable. The Gaussian kernel function used in the proposed authentication scheme is given by

$$\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \exp(\frac{-||\widetilde{\boldsymbol{h}}_l - \overline{\boldsymbol{h}}||^2}{2\sigma_\kappa^2}), \tag{3.9}$$

where σ_κ is the kernel width and should be chosen by the users. The Gaussian kernel function of (3.9) characterizes a similarity between the observed inputs $\widetilde{\boldsymbol{h}}_l$ and the new normalized estimate $\overline{\boldsymbol{h}}$.

From (3.7) and (3.8), the following relationship holds, i.e.,

$$\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}). \tag{3.10}$$

Remark 3.2. It is observed both from the kernel function of (3.9) and from the authentication system expression of (3.8) that the physical layer attributes are fused without any specific knowledge of their statistical properties, which corresponds to **C1**. As for **C2**, the search-space is transformed from being N-dimensional to single-dimensional by the developed multiple physical layer attribute fusion model.

Remark 3.3. In practical wireless networks, the authentication systems are usually nonlinear (see **C3**). By contrast, according to the proposed kernel machine-based physical layer attribute fusion model of (3.8), the authentication system is formulated as a linear system, since the expression of (3.8) relies on the linear weights $\alpha_l,\ l = 1, 2, ..., L$.

The estimates of the multiple physical layer attributes $\boldsymbol{H}$ are time-variant, which may lead to a low authentication performance without agile adaptation. Therefore, next subsection focuses on proposing adaptive learning procedures for promptly adjusting the authentication system of (3.8), which is the solution of **C4**.

3.3.2 Adaptive Authentication based on Kernel Learning

In this section, a learning procedure is proposed for adaptive authentication based on the kernel least-mean-square for promptly updating the parameters. This authentication process is based on learning from the observed samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$. Explicitly, the proposed learning procedure can be viewed as an intelligent process of learning the time-varying environment for updating the system parameters $\alpha_l,\ l = 1, 2, ..., L$, to achieve a reliable and robust authentication.

Given the samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$ observed, the N-dimensional input vector $\widetilde{\boldsymbol{h}}_l \in [-1, 1]^N$ is transformed into a kernel Hilbert space $\mathcal{H}$ through a mapping $\varphi : [-1, 1]^N \to \mathcal{H}$ according to (3.7). Therefore, a pair of sample sequences $\{\varphi(\widetilde{\boldsymbol{h}}_1), \varphi(\widetilde{\boldsymbol{h}}_2), ...\}$ and $\{\widehat{y}_1, \widehat{y}_2, ...\}$ is obtained. The weight vector $\boldsymbol{w}$ in (3.7) at iteration l should be updated for minimizing the cost function as follows

$$\min_{\boldsymbol{w}} \sum_{i=1}^{l} [\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_i)]^2. \tag{3.11}$$

Remark 3.4. It is observed from (3.11) that the learning (training) objective of the adaptive authentication process is formulated as a convex optimization problem.

The learning rules conceived for updating the authentication system of (3.8) are given as:
Proposition 3.1: The learning rule conceived for updating the weight vector $\boldsymbol{\alpha}[l]$ in the developed multiple physical layer attribute fusion model at iteration l can be expressed as

$$\boldsymbol{\alpha}[l] = \mu \times (e[1], e[2], ..., e[l])^{\mathrm{T}}, \tag{3.12}$$

where μ represents a step-size parameter. Furthermore, $e[l]$ is the prediction error computed as the difference between the desired observation of the transmitter and its prediction relying on the authentication system parameters $\boldsymbol{\alpha}[l-1]$, which is expressed as

$$e[l] = \widehat{y}_l - f(\widetilde{\boldsymbol{h}}_l)[l-1], \tag{3.13}$$

where

$$f(\widetilde{\boldsymbol{h}}_l)[l-1] = \sum_{i=1}^{l-1} \alpha_i[l-1] \kappa(\widetilde{\boldsymbol{h}}_i, \widetilde{\boldsymbol{h}}_l). \tag{3.14}$$

Furthermore, the learning rule conceived for adjusting the authentication system at iteration l is given by

$$f(\overline{\boldsymbol{h}})[l] = f(\overline{\boldsymbol{h}})[l-1] + \mu e[l] \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}). \tag{3.15}$$

Proof: Let

$$J(\boldsymbol{w}) = \sum_{i=1}^{l} [\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_i)]^2. \tag{3.16}$$

By invoking a step-size parameter μ, the learning rule for the parameter $\boldsymbol{w}$ can be derived by using the gradient. The partial derivative of the function $J(\boldsymbol{w})$ with respect to $\boldsymbol{w} = (w_1, w_2, ..., w_l)^{\mathrm{T}}$ is given by

$$\frac{\partial J(\boldsymbol{w})}{\partial \boldsymbol{w}} = -2\sum_{i=1}^{l} \varphi(\widetilde{\boldsymbol{h}}_i)[\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}}\varphi(\widetilde{\boldsymbol{h}}_i)], \tag{3.17}$$

and the instantaneous gradient at iteration l is

$$\frac{\partial J(\boldsymbol{w})}{\partial \boldsymbol{w}}[l] = -\varphi(\widetilde{\boldsymbol{h}}_l)[\widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}}\varphi(\widetilde{\boldsymbol{h}}_l)]. \tag{3.18}$$

According to the steepest descent algorithm, it has

$$\boldsymbol{w}[l] = \boldsymbol{w}[l-1] + \mu\varphi(\widetilde{\boldsymbol{h}}_l)[\widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}}\varphi(\widetilde{\boldsymbol{h}}_l)]. \tag{3.19}$$

Since $e[l]$ of (3.13) can also be expressed as

$$e[l] = \widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}}\varphi(\widetilde{\boldsymbol{h}}_l), \tag{3.20}$$

the repeated application of (3.19) through iterations becomes

$$\begin{aligned}\boldsymbol{w}[l] &= \boldsymbol{w}[l-1] + \mu\varphi(\widetilde{\boldsymbol{h}}_l)e[l] = \boldsymbol{w}[l-2] + \mu\varphi(\widetilde{\boldsymbol{h}}_{l-1})e[l-1] + \mu\varphi(\widetilde{\boldsymbol{h}}_l)e[l] \\ &= \cdots = \sum_{i=1}^{l} \mu\varphi(\widetilde{\boldsymbol{h}}_i)e[i];\ (\boldsymbol{w}[0] = 0).\end{aligned} \tag{3.21}$$

According to (3.7), (3.8) and (3.9), the authentication system can be derived as

$$f(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}}\varphi(\overline{\boldsymbol{h}}) = \boldsymbol{w}[L]^{\mathrm{T}}\varphi(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \mu e[l]\varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}}\varphi(\overline{\boldsymbol{h}}), \tag{3.22}$$

then the following equation holds

$$\alpha_l[l] = \mu e[l]. \tag{3.23}$$

Therefore, the parameter vector $\boldsymbol{\alpha}$ at iteration l, i.e., $\boldsymbol{\alpha}[l] = (\alpha_1[l], \alpha_2[l], ..., \alpha_l[l])^{\mathrm{T}}$, can be updated through (3.12). Then the authentication system at iteration l can be formulated as

$$\begin{aligned} f(\overline{\boldsymbol{h}})[l] = \sum_{i=1}^{l} \alpha_i \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) = \mu \sum_{i=1}^{l} e[i] \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) &= \mu \sum_{i=1}^{l-1} e[i] \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) + \mu e[l] \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) \\ &= f(\overline{\boldsymbol{h}})[l-1] + \mu e[l] \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}). \end{aligned} \tag{3.24}$$

Therefore, learning rule for adjusting the authentication system of (3.8) is expressed as (3.15). □

Algorithm 1 Intelligent authentication process based on the kernel learning

```
1. Initialization:
    $f[0] = 0$: initial value of authentication system
    $e[0] = 0$: initial value of prediction error
    $\alpha[0] = 0$: initial value of system parameter $\boldsymbol{\alpha}$
    $\mu$: step-size parameter of learning
    $\sigma_\kappa$: kernel width
    $\widetilde{\boldsymbol{h}}_1$: initial input, i.e., the normalized estimate of physical layer attributes
    $C = \{\widetilde{\boldsymbol{h}}_1\}$: initial set of input
    $\widehat{y}_1$: initial observation of the transmitter with the corresponding normalized estimate $\widetilde{\boldsymbol{h}}_1$
2. Iteration:
    2.1 while samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$ available do
    2.2     obtain the output of authentication system $f[l-1]$ at iteration $l-1$ via (3.8);
    2.3     calculate the prediction error $e[l]$ via (3.13);
    2.4     update weight vector $\boldsymbol{\alpha}[l]$ through (3.12);
    2.5     adjust the authentication system $f[l]$ via (3.15);
    2.6     update the input set as $C = C + \{\widetilde{\boldsymbol{h}}_l\}$;
    2.7     $l = l + 1$;
    2.8 end
```

According to Proposition 3.1, the intelligent authentication process based on the kernel least-mean-square is summarized at a glance in Algorithm 1.

Remark 3.5. In conclusion, the search space is transformed from being N-dimensional to single-dimensional (see Remark 3.2), the authentication is modeled as a linear system (see Remark 3.3), and the learning objective of the authentication is formulated as a convex problem (see Remark 3.4). Therefore, the complexity of the physical layer authentication scheme relying on multiple attributes is dramatically reduced. It is also observed from Algorithm 1 that the execution-time is on the order of $O(L)$, which makes Algorithm 1 an attractive solution.

The step-size parameter directly affects the convergence of the proposed authentication process, since increasing the step-size of learning will reduce the convergence time but may in fact lead to divergence. Therefore, the step-size parameter μ should be carefully decided.

Theorem 3.1: The proposed intelligent authentication process (see Algorithm 1) converges to a steady-state value, if the step-size parameter of learning μ satisfies

$$0 < \mu < \frac{L}{\sum_{l=1}^{L} \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_l)} = 1. \tag{3.25}$$

Proof: A practical convergence criterion is a convergence in the mean square error sense, which is formulated as

$$E[||e[l]||^2] \rightarrow \text{constant, as } l \rightarrow \infty, \tag{3.26}$$

where $E[\cdot]$ represents the expectation of $\cdot$. It was shown in [109, 112] that the least-mean-square criterion-based learning is convergent in the mean square, if μ satisfies

$$0 < \mu < \frac{1}{\beta_{max}}, \tag{3.27}$$

where β_{max} is the largest eigenvalue of the correlation matrix $\boldsymbol{\Theta}[L]$ given by

$$\boldsymbol{\Theta}[L] = [\varphi(\widetilde{\boldsymbol{h}}_1), \varphi(\widetilde{\boldsymbol{h}}_2), ..., \varphi(\widetilde{\boldsymbol{h}}_L)]_{N\times L}. \tag{3.28}$$

Since $\beta_{max} < \text{tr}(\boldsymbol{\Theta}[L])/L$, the following inequality is satisfied

$$0 < \mu < \frac{L}{\text{tr}(\boldsymbol{\Theta}[L])} = \frac{L}{\sum_{l=1}^{L} \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_l)} = 1, \tag{3.29}$$

where $\text{tr}(\boldsymbol{\Theta}[L])$ is the trace of the matrix $\boldsymbol{\Theta}[L]$. Therefore, the proposed intelligent authentication process (see Algorithm 1) converges to a steady-state value if the step-size parameter of learning μ satisfies (3.25). $\square$

Remark 3.6. Theorem 3.1 gives the upper bound of the step-size parameter μ in Algorithm 1, so that the proposed intelligent authentication process will converge to a steady state.

According to the proposed authentication system of (3.8), the false alarm rate and misdetection rate at instant L can be rewritten, respectively, as

$$P_{\mathrm{FA}} = P(|\sum_{l=1}^{L-1} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_L)| < \nu \mid \Phi_0) \tag{3.30}$$

and

$$P_{\mathrm{MD}} = P(|1 - \sum_{l=1}^{L-1} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_L)| \le \nu \mid \Phi_1), \tag{3.31}$$

where $\nu \in [0, 1)$.

In the face of the imperfect estimates of time-varying physical layer attributes, they are divided into two parts: the time-varying part $\overline{\boldsymbol{H}}$ that is the real value of physical layer attributes used, and part $\triangle \boldsymbol{H}$ that is the bias of estimated attributes. Then the estimates $\boldsymbol{H}_A^I[l - \tau_l]$ and $\boldsymbol{H}^{II}[l]$ can be written, respectively, as

$$\boldsymbol{H}_A^I[l - \tau_l] = \overline{\boldsymbol{H}}_A^I[l - \tau_l] + \triangle \boldsymbol{H}_A^I[l - \tau_l] \tag{3.32}$$

and

$$\boldsymbol{H}^{II}[l] = \overline{\boldsymbol{H}}^{II}[l] + \triangle \boldsymbol{H}^{II}[l], \tag{3.33}$$

where τ_l is the time interval between Phase I and Phase II of the physical layer authentication at iteration $l, l = 1, 2, ..., L$. Furthermore, $\boldsymbol{\upsilon}(\tau_l) = (\upsilon_{1l}, \upsilon_{2l}, ..., \upsilon_{Nl})^{\mathrm{T}}$ represents the variations of part $\overline{\boldsymbol{H}}_A^I$ during the time interval τ_l, which can be expressed as

$$\boldsymbol{\upsilon}(\tau_l) = \overline{\boldsymbol{H}}_A^{II}[l] - \overline{\boldsymbol{H}}_A^I[l - \tau_l]. \tag{3.34}$$

Given the distributions of part $\triangle \boldsymbol{H}$ of the multiple physical layer attributes, the false alarm rate and misdetection rate of the proposed scheme are calculated as the following theorems.

Theorem 3.2: The false alarm rate expression of the kernel learning-based scheme at iteration L is given by

$$P_{\mathrm{FA}} = F_{Y_1} * F_{Y_2} * \cdots * F_{Y_{L-1}}(\nu) - F_{Y_1} * F_{Y_2} * \cdots * F_{Y_{L-1}}(-\nu), \tag{3.35}$$

where $Y_l = \alpha_l \exp(-\sum_{n=1}^{N}(\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2/2\sigma_\kappa^2)$, $l = 1, 2, ..., L-1$, $\widetilde{h}_{nL}^{\Phi_0}$ is shown in (3.36), F represents the cumulative distribution function, and $*$ represents the convolution.

Proof: According to (3.5), (3.32), (3.33), and (3.34), $\widetilde{\boldsymbol{h}}_L = (\widetilde{h}_{1L}, \widetilde{h}_{2L}, ..., \widetilde{h}_{NL})^{\mathrm{T}}$ in case of Φ_0 is calculated as

$$\widetilde{h}_{nL}^{\Phi_0} = \frac{2}{b_n - a_n}(\upsilon_n(\tau_L) + \triangle H_{An}^{I}[L - \tau_L] - \triangle H_{An}^{II}[L] - \frac{a_n + b_n}{2}),\ n = 1, 2, ..., N, \tag{3.36}$$

where τ_L is the time interval between Phase I and Phase II of the proposed physical layer authentication scheme at iteration L. Given the distributions of $\triangle H_{An}^{I}$ and $\triangle H_{An}^{II}$ of each physical layer attribute, the probability of density function of $\widetilde{h}_{nL}^{\Phi_0}$ can be obtained. Let $Y_l = \alpha_l \exp(\frac{-\sum_{n=1}^{N}(\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2}{2\sigma_\kappa^2})$, the false alarm rate at iteration L is calculated as

$$\begin{aligned} P_{\mathrm{FA}} = P(|\sum_{l=1}^{L-1} \alpha_l \exp(\frac{-\sum_{n=1}^{N}(\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2}{2\sigma_\kappa^2})| < \nu) &= P(\sum_{l=1}^{L-1} Y_l < \nu) - P(\sum_{l=1}^{L-1} Y_l \leq -\nu) \\ &= F_{\sum_{l=1}^{L-1} Y_l}(\nu) - F_{\sum_{l=1}^{L-1} Y_l}(-\nu). \end{aligned} \tag{3.37}$$

Therefore, the false alarm rate expression of the kernel learning-based scheme at iteration L is shown in (3.35). □

Theorem 3.3: The misdetection rate expression of the kernel learning-based scheme at iteration L is expressed as

$$P_{\mathrm{MD}} = F_{Z_1} * F_{Z_2} * \cdots * F_{Z_{L-1}}(\nu + 1) - F_{Z_1} * F_{Z_2} * \cdots * F_{Z_{L-1}}(1 - \nu), \tag{3.38}$$

where $Z_l = \alpha_l \exp(-\sum_{n=1}^{N}(\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_1})^2/2\sigma_\kappa^2)$, $l = 1, 2, ..., L-1$, and $\widetilde{h}_{nL}^{\Phi_1}$ is shown in (3.39).

Proof: According to (3.5), (3.32), and (3.33), $\widetilde{\boldsymbol{h}}_L = (\widetilde{h}_{1L}, \widetilde{h}_{2L}, ..., \widetilde{h}_{NL})^{\mathrm{T}}$ in case Φ_1 is formulated as

$$\widetilde{h}_{nL}^{\Phi_1} = \frac{2}{b_n - a_n}(\overline{H}_{An}^{I}[L - \tau_L] - \overline{H}_{En}^{II}[L] + \triangle H_{An}^{I}[L - \tau_L] - \triangle H_{En}^{II}[L] - \frac{a_n + b_n}{2}). \tag{3.39}$$

Given the distributions of $\triangle H_{An}^{I}$ and $\triangle H_{En}^{II}$ of each physical layer attribute, the probability of density function of $\widetilde{h}_{nL}^{\Phi_1}$ can be obtained. Upon letting $Z_l = \alpha_l \exp(\frac{-\sum_{n=1}^{N}(\widetilde{h}_{nl}-\widetilde{h}_{nL}^{\Phi_1})^2}{2\sigma_\kappa^2})$, the misdetection rate at iteration L yields

$$\begin{aligned} P_{\mathrm{MD}} = P(|1-\sum_{l=1}^{L-1}\alpha_l \exp(\frac{-\sum_{n=1}^{N}(\widetilde{h}_{nl}-\widetilde{h}_{nL}^{\Phi_1})^2}{2\sigma_\kappa^2})| \leq \nu) &= P(\sum_{l=1}^{L-1} Z_l \leq \nu+1) - P(\sum_{l=1}^{L-1} Z_l < 1-\nu) \\ &= F_{\sum_{l=1}^{L-1} Z_l}(\nu+1) - F_{\sum_{l=1}^{L-1} Z_l}(1-\nu). \qquad (3.40) \end{aligned}$$

Therefore, the misdetection rate expression of the kernel learning-based scheme at iteration L is given by (3.38). □

Remark 3.7. It can be observed from Theorem 3.2 and Theorem 3.3 that the false alarm rate and misdetection rate of the kernel learning-based scheme depend on both the number of physical layer attributes N and on the variations of the attributes $\boldsymbol{v}$. The kernel learning-based scheme tracks the variations of the attributes and promptly adjusts the authentication system, so that a compelling false alarm rate vs. misdetection rate trade-off will be achieved.

3.3.3 Simulation Results

In this subsection, the proposed kernel learning-based scheme is implemented using multiple physical layer attributes. First of all, three physical layer attributes, namely the carrier frequency offset (CFO), channel impulse response (CIR), and received signal strength indicator (RSSI) are considered to confirm the viability of the proposed intelligent authentication process. Specifically, a communication system having a measurement center frequency of 2.5 GHz, measurement bandwidth of 10 MHz, coherence bandwidth of 0.99, normalized time correlation of 0.99 and sampling time of 50 ms is considered. The transmitted signal is passed through a randomly generated 12-tap multipath fading channel having an exponential power delay profile. The relative velocity between Alice and Bob is assumed to be around 20 km/h, and the initial distance between Alice and Bob is 5 m. Then the CFO of an individual transmitter can be approximated as a zero-mean Gaussian variable [37, 116], and the standard deviation of the CFO variation is $\triangle_{\mathrm{CFO}} \approx 2.35 \times 10^{-7}$. The CFO estimation range is $[-78.125, 78.125)$ kHz [37]. Furthermore, according to [82], an autoregressive model of order 1 (AR-1) is used for characterizing the temporal amplitude fluctuation $\text{Amp}_k[t]$ of the kth-tap in the multipath fading channel. Therefore, the variation of CIR can be given as $\upsilon_{\text{CIR}} = \sum_{k=1}^{12} \text{Amp}_k[t] \exp(-j4.99\pi k)$, and the per-tone signal-to-noise ratio (SNR) is in the channel measurements range of $[-12.8, 14.2)$ dB with a median value of 6.4 dB, if the transmit power is 10 mW [82]. Finally, according to [117], the RSSI can be given as $PL[\text{dB}] = 75 + 36.1 \log(\text{d}/10)$, where PL is the path loss, and d represents the direct transmission distance between the transmitter and Bob. The direct transmission distance between the transmitter and Bob is assumed to be in the range of $[0, 100]$ m.

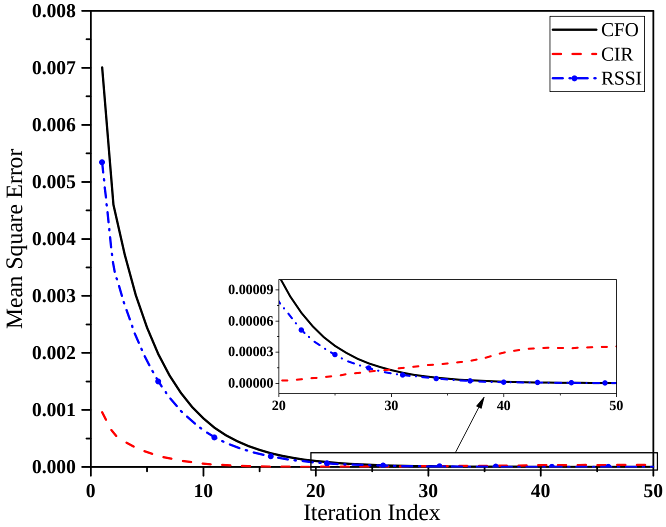


Figure 3.3: Training performance of the kernel learning-based scheme (Algorithm 1) relying on the CFO, CIR and RSSI triplet.

Given 300 samples of the CFO, CIR and RSSI of Alice, i.e., $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{300} \in [-1, 1]^3 \times \{0, 1\}$, where $\widehat{y}_l = 1$, Figure 3.3 shows the training performance of the kernel learning-based scheme (Algorithm 1) relying on the CFO, CIR and RSSI triplet. The step-size parameter of Algorithm 1 is set to $\mu = 0.1$. It is observed from Figure 3.3 that the mean square errors $E[||e[l]||^2]$ of all the strategies are significantly reduced, as the iteration index increases from 0 to 50. Furthermore, the mean square error $E[||e[l]||^2]$ of each strategy reaches its steady-state value after 30 iterations. Figure 3.3 shows that the CIR estimation performs better than both the CFO and RSSI estimation in the training performance at the beginning, but its training performance becomes the worst after 30 iterations. The reason for this trend is that the deviation of CIR estimation is lower than that of the CFO and RSSI, while its variation is the highest.

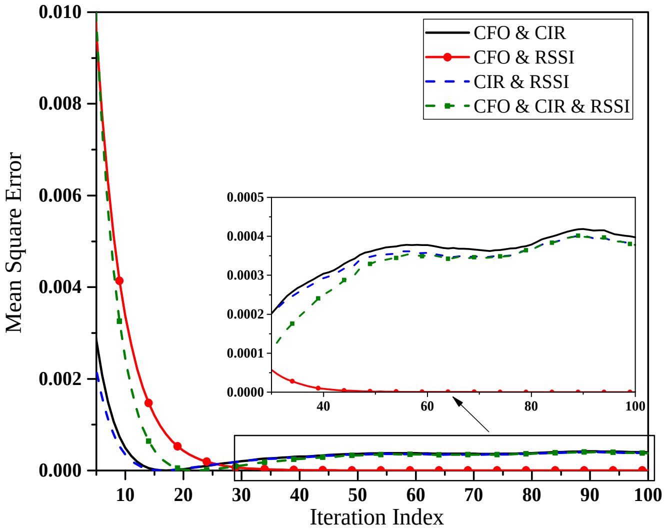


Figure 3.4: Training performance of the kernel learning-based scheme (Algorithm 1) relying on 2 attributes and 3 attributes.

Figure 3.4 characterizes the training performance of the kernel learning-based scheme (see Algorithm 1) relying on multiple attributes. Four cases are considered, namely the CFO & CIR, the CFO & RSSI, the CIR & RSSI, and finally the CFO & CIR & RSSI scenarios. It is observed from Figure 3.4 that the proposed intelligent authentication process relying on the CFO & RSSI pair has the worst training performance before 30 iterations, while that relying on the CIR & RSSI pair has the lowest mean square error. The reason for this trend is that the mean square error of the proposed intelligent authentication process relying on the CIR is lower than that of the CFO and RSSI before 30 iterations seen in Figure 3.5, which adversely affects the training performance in this communication scenario. Additionally, the mean square error of the proposed intelligent authentication process relying on the CFO & RSSI pair is the lowest after 30 iterations, because both the CFO and RSSI are more reliable than the CIR in the authentication process. Furthermore, it is also shown in Figure 3.4 that the training performance of the proposed intelligent authentication process relying on the CFO & CIR & RSSI triplet is worse than that of the CFO & RSSI pair after 30 iterations, while it is better than that of the CFO & CIR pair and CIR & RSSI pair. This is because the training performance of the kernel learning-based scheme depends on both the specific attributes and on the number of physical layer attributes.

Figure 3.5 considers the case that Eve can intercept and imitate the CFO of Alice, which

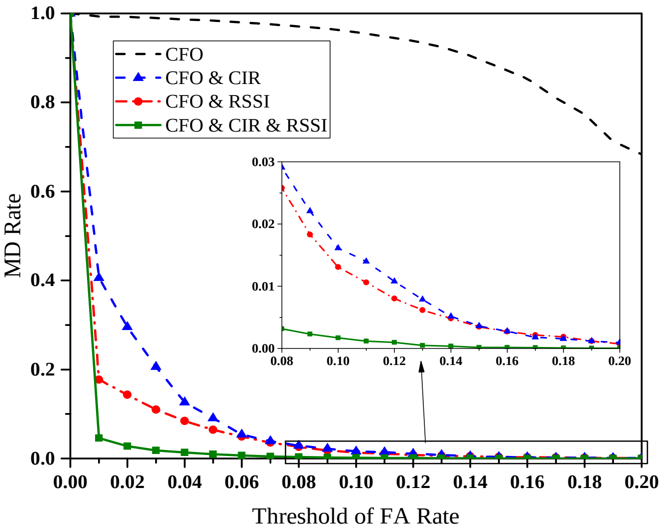


Figure 3.5: Authentication performance of the kernel learning-based scheme relying on the CFO, CFO & CIR, CFO & RSSI, and CFO & CIR & RSSI scenarios.

characterizes the authentication performance of the kernel learning-based scheme relying on the CFO, CFO & CIR, CFO & RSSI, and finally the CFO & CIR & RSSI scenarios. In other words, Eve intercepts and impersonates the CFO of Alice to obtain unintended advantages from Bob in this case. It is observed from Figure 3.5 that the kernel learning-based scheme relying on the CFO & CIR & RSSI has the best authentication performance, while that only relying on the CFO performs worst. The reason for this trend is that Bob can better identify the transmitter by using CIR and RSSI, although Eve imitates the CFO of Alice in the CFO & CIR & RSSI scenario. On the other hand, Bob suffers from a high misdetection rate in the CFO scenario, since the CFO of Alice is impersonated by Eve. It is also shown in Figure 3.5 that there is a small difference between the authentication performance of the kernel learning-based scheme relying on the CFO & CIR pair and that of the CFO & RSSI pair; and the authentication performances of these two attributes scenarios are better than that of a single-attribute scenario (i.e., CFO). This is because Bob can identify the adversary by using CIR or RSSI in the CFO & CIR or the CFO & RSSI scenarios. Therefore, the increasing number of physical layer attributes is expected to lead to a higher authentication performance in the kernel learning-based scheme.

Figure 3.6 considers the scenario when Eve can intercept and impersonate both the CFO and CIR of Alice. It is observed from Figure 3.6 that the authentication performance of the

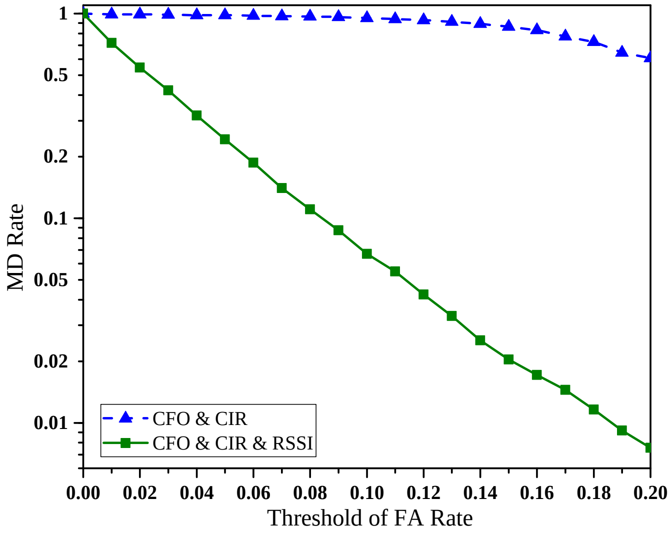


Figure 3.6: Authentication performance of the kernel learning-based scheme relying on the CFO & CIR and CFO & CIR & RSSI scenarios.

kernel learning-based scheme relying on the CFO & CIR & RSSI triplet is better than that of the CFO & CIR pair. The reason for this trend is that Bob can identify the adversary using the RSSI in the CFO & CIR & RSSI scenario, although Eve imitates both the CFO and CIR of Alice. Both Figure 3.5 and Figure 3.6 confirm that increasing the number of physical layer attributes leads to a better authentication performance, since it is more difficult for an adversary to succeed in predicting or imitating all the attributes based on the received signal.

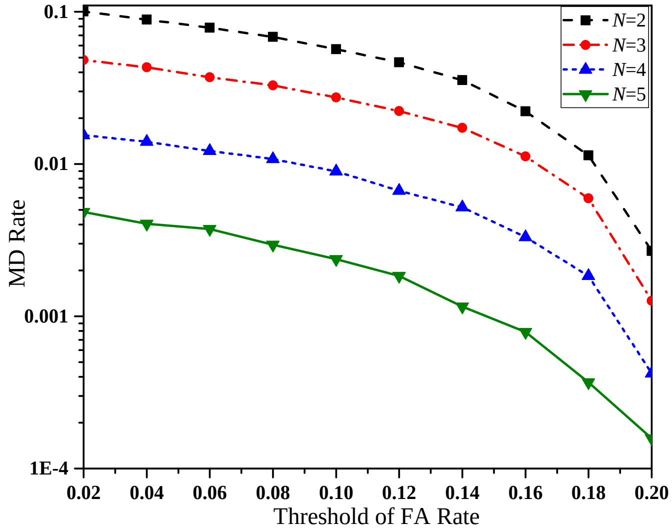


Figure 3.7: Authentication performance comparison results of the kernel learning-based scheme with different numbers of attributes.

Figure 3.7 characterizes the influence of the number of physical layer attributes N on the authentication performance, which quantifies the MD rate vs. the threshold of FA rate for different numbers of physical layer attributes, namely for $N = 2$, $N = 3$, $N = 4$ and $N = 5$. It can be observed that the MD rates are reduced in all cases as the threshold δ of FA rate increases from 0 to 0.2, because there is an inevitable FA-and-MD trade-off. One can also observe from Figure 3.7 that a larger number of attributes leads to a more obvious security performance improvement. This trend demonstrates the validity of authentication performance analysis. In a nutshell, by using more physical layer attributes, the kernel learning-based scheme achieves a better authentication performance, indicating the presence of a FA-and-MD trade-off, because the proposed scheme can readily fuse multiple physical layer attributes and control the authentication system to track the variations of multiple attributes. On the same note, the attackers find it more difficult to predict and imitate a larger number of attributes from a received signal.

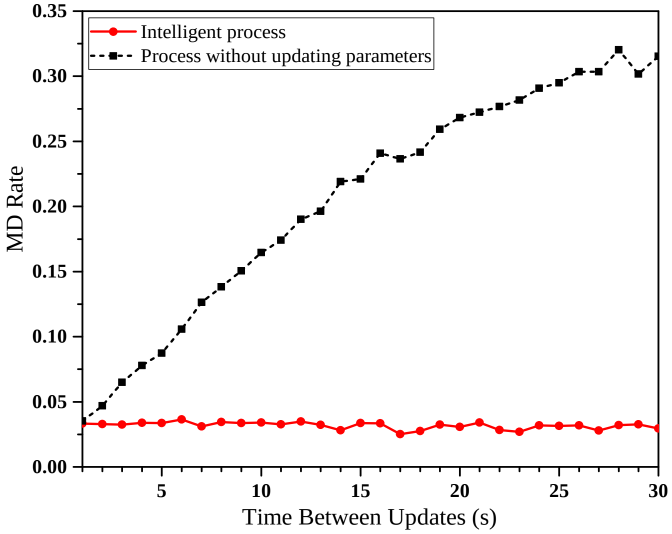


Figure 3.8: Comparison results between the kernel learning-based scheme and the process without updating system parameters relying on CFO & CIR & RSSI.

In Figure 3.8, the variations on the CFO, CIR and RSSI are imposed for comparing the kernel learning-based scheme and the authentication process operating without updating the system parameters. The threshold of the false alarm rate is 0.02. Then it can be observed from Figure 3.8 that upon increasing the time between updates, the MD rate of the proposed intelligent process remains robust, tending to around 0.035, while that of the process operating without updating the system parameters increases dramatically from about 0.035 to almost

0.35. This demonstrates that without an adaptive scheme, the authentication performance will be dramatically reduced in time-varying environments. Therefore, the kernel learning-based scheme performs better than the static scheme operating without updating the parameters.

3.4 Fuzzy Learning-based Authentication Scheme

In order to improve the authentication performance by utilizing multiple attributes when some statistical properties of the physical layer attributes are available and intermittent availability of some attributes are considered, a fuzzy theory-based model is designed to combine multiple physical layer attributes. By using fuzzy theory [104, 105, 106, 107], the effects of their imperfectness can be mitigated and the authentication accuracy can be improved.

Following the normalization of (3.4) and (3.5), each set $[a_n, b_n]$ is uniformed into specific set $[-1, 1]$ through

$$h'_n[t] = \frac{2}{b_n - a_n}(H_n[t+1] - H_{An}[t] - \frac{a_n + b_n}{2}),\ n = 1, 2, ..., N. \tag{3.41}$$

In this equation, $\tau = 1$.

The fuzzy membership function is explored to combine the multiple attributes, which is a generalization of the indicator function in classical sets [106]. Some typical examples of fuzzy membership function are given as the Gaussian function, triangle function, and trapezoid function. In this chapter, the fuzzy membership function is designed as the Gaussian function with means $\widehat{\mu}_n$ and variances $\widehat{\sigma}^2_n$, i.e.,

$$u_{[-1,1]}(h'_n[t]) = \exp(\frac{-(h'_n[t] - \widehat{\mu}_n)^2}{2\widehat{\sigma}^2_n}). \tag{3.42}$$

For different physical layer attributes, $\widehat{\mu}_n$ and $\widehat{\sigma}^2_n$, $n = 1, 2, ..., N$, experience different values and control the developed fuzzy multiple attribute combination model. The expression (3.42) is the fuzzy membership function for combing multiple physical layer attributes rather than describing the Gaussian noises of attributes' estimates.

Without loss of generality, through using product inference engine and center average defuzzifier [113], the fuzzy multiple attribute combination model is designed as

$$\begin{array}{ccl} \text{Inputs} & \rightarrow & \text{Outputs} \\ \boldsymbol{h}'[t] & \rightarrow & y[t] = \sum_{n=1}^{N} \widehat{\alpha}_n u_{[-1,1]}(h'_n[t]), \end{array} \tag{3.43}$$

where $\boldsymbol{h}'[t] = (h'_1[t], h'_2[t], ..., h'_N[t])^{\mathrm{T}}$, and $\widehat{\alpha}_n$ are system parameters, which adjust the weights of multiples physical layer attributes. Therefore, the designed fuzzy multiple attribute combination model can well control the different contributions of attributes on the authentication accuracy.

Remark 3.8. The fuzzy function of (3.42) describes the form of model expression using Gaussian function, which is a parametric method. It can also be observed from (3.42) that each attribute is independently taken into account. Hence, although some attributes are unavailable at some moments, the remaining attributes still contribute to the authentication and make the model applicable, thus the fuzzy learning-based scheme comes to a robust approach. Moreover, the robustness of the developed fuzzy authentication model can be improved by increasing the number of attributes N.

Through the designed fuzzy multiple attribute combination model, a real-valued output $y[t]$ can be obtained from (3.42) at time t. Then the physical layer authentication process is turned into a fuzzy authentication process as

$$\begin{cases} \Phi_0: & \nu \le y[t] \le 1; \\ \Phi_1: & 0 < y[t] < \nu. \end{cases} \tag{3.44}$$

The false alarm rate and misdetection rate of the designed fuzzy model at time t can be formulated based on the fuzzy authentication process of (3.43) as

$$P_{\mathrm{FA}}[t] = P(0 < y[t] < \nu \mid \Phi_0), \tag{3.45}$$

and

$$P_{\mathrm{MD}}[t] = P(\nu \le y[t] \le 1 \mid \Phi_1). \tag{3.46}$$

In the following, it is assumed that the estimate deviations $\triangle\boldsymbol{H}$, which can be seen as the noises of estimates, are zero-mean complex Gaussian random variables with variances $\boldsymbol{\varrho}^2 = (\varrho_1^2, \varrho_2^2, ..., \varrho_N^2)^{\mathrm{T}}$, denoted as $\triangle\boldsymbol{H} \sim \aleph(0, \boldsymbol{\varrho}^2)$, and are independently distributed. Note that only the noises of attribute estimates are assumed to be the zero-mean complex Gaussian random variables. The multiple physical layer attributes can follow different distributions.

Upon denoting $X_n[t] = (h'_n[t] - \widehat{\mu}_n)/\varrho'_n$, it obeys Gaussian random distribution, which can be expressed as $X_n[t] \sim \aleph(\overline{\mu}'_n[t], 1)$, where $\varrho'^2_n = 4(\varrho^2_{An} + \varrho^2_n)/(b_n - a_n)^2$ and $\overline{\mu}'_n[t] = 2(\overline{H}_n[t+1] - \overline{H}_{An}[t+1] + \upsilon_n[t] - \widehat{\mu}_n)/(\varrho'_n(b_n - a_n))$. Note that the X_n at time instant t is Gaussian random variable, but X_n at different time instants does not obey Gaussian random distribution, since the mean $\overline{\mu}'_n[t]$ is time-varying. Therefore, each $X^2_n[t]$ obeys the noncentral chi-squared distribution, which can be expressed as $X^2_n[t] \sim \mathscr{X}^2_n(1, \lambda_n[t])$. It has two parameters: the number of degrees of freedom, namely for 1, and the noncentrality parameter $\lambda_n[t]$, satisfying $\lambda_n[t] = \overline{\mu}'^2_n[t]$. Using the relationship between the central and noncentral chi-squared distributions, the probability density function (PDF) and the cumulative distribution function (CDF) of variable $X^2_n[t]$ can be given as

$$f_{X^2_n[t]}(x; 1, \lambda_n[t]) = \frac{1}{2}\exp(-\frac{x + \lambda_n[t]}{2})(\frac{x}{\lambda_n[t]})^{-\frac{1}{4}} I_{-\frac{1}{2}}(\sqrt{\lambda_n[t]x}), \tag{3.47}$$

and

$$P_{X^2_n[t]}(x; 1, \lambda_n[t]) = \exp(-\frac{\lambda_n[t]}{2}) \sum_{j=1}^{\infty} \frac{(\lambda_n[t]/2)^j}{j!} Q(x; 1 + 2j), \tag{3.48}$$

respectively. $I_{-\frac{1}{2}}(\sqrt{\lambda_n[t]x})$ is a modified Bessel function of the first kind given by

$$I_{-\frac{1}{2}}(\sqrt{\lambda_n[t]x}) = (\frac{\sqrt{\lambda_n[t]x}}{2})^{-\frac{1}{2}} \sum_{j=0}^{\infty} \frac{(\lambda_n[t]x/4)^j}{j!\Gamma(j + 1/2)}.$$

Moreover, $Q(x; 1 + 2j)$ is the CDF of the central chi-squared distribution with 1 degree of freedom shown as

$$Q(x; 1 + 2j) = \frac{\Upsilon((1 + 2j)/2, x/2)}{\Gamma((1 + 2j)/2)}, \tag{3.49}$$

where $\Upsilon(\cdot)$ is the lower incomplete Gamma function, and $\Gamma(\cdot)$ represents the Gamma function.

Then, the output of the developed fuzzy multiple attribute combination model y of (3.43) at time t can be rewritten as

$$y[t] = \sum_{n=1}^{N} \widehat{\alpha}_n[t] \exp(-\frac{\varrho_n'^2}{2\widehat{\sigma}_n^2[t]} X_n^2[t]). \tag{3.50}$$

The following theorem can be obtained:

Theorem 3.4: The false alarm rate and misdetection rate of the designed fuzzy multiple attribute combination model can be given, respectively, by

$$P_{\text{FA}}[t] = P(0 < Y[t] < \nu) = \overbrace{\int \cdots \int}^{N}_{C_1} \prod_{n=1}^{N} f_{\xi_n[t]}(x_n) dx_1 \cdots dx_N \tag{3.51}$$

and

$$P_{\text{MD}}[t] = P(\nu \leq Z[t] \leq 1) = \overbrace{\int \cdots \int}^{N}_{C_2} \prod_{n=1}^{N} f_{\varsigma_n[t]}(x_n) dx_1 \cdots dx_N, \tag{3.52}$$

where

$$Y[t] = \sum_{n=1}^{N} \xi_n[t],\ \xi_n[t] = \widehat{\alpha}_n[t] \exp(-\frac{\varrho_n'^2}{2\widehat{\sigma}_n^2[t]} X^2_{n,\lambda_n^{\text{FA}}[t]}),\ \lambda_n^{\text{FA}}[t] = (\frac{2(\upsilon_n[t] - \widehat{\mu}_n[t])}{\varrho_n'(b_n - a_n)})^2. \tag{3.53}$$

$f_{\xi_n[t]}(x_n)$ and $F_{\xi_n[t]}(x_n)$ are the PDF and CDF of variable $\xi_n[t]$, respectively, which are given as

$$F_{\xi_n[t]}(x_n) = 1 - P_{X_n^2[t]}(-\frac{2\widehat{\sigma}_n^2[t]}{\varrho_n'^2} \ln(\frac{x_n}{\widehat{\alpha}_n[t]}); 1, \lambda_n^{\text{FA}}[t]) = \int_{-\infty}^{x_n} f_{\xi_n[t]}(\tau) d\tau. \tag{3.54}$$

Moreover,

$$\begin{aligned} Z[t] &= \sum_{n=1}^{N} \varsigma_n[t],\ \varsigma_n[t] = \widehat{\alpha}_n[t] \exp(-\frac{\varrho_n'^2}{2\widehat{\sigma}_n^2[t]} X^2_{n,\lambda_n^{\text{MD}}[t]}), \\ \lambda_n^{\text{MD}}[t] &= (\frac{2(\overline{H}_{En}[t] - \overline{H}_{An}[t] + \upsilon_n[t] - \widehat{\mu}_n)}{\varrho_n'(b_n - a_n)})^2. \end{aligned} \tag{3.55}$$

$f_{\varsigma_n[t]}(x_n)$ and $F_{\varsigma_n[t]}(x_n)$ represent the PDF and CDF of variable $\varsigma_n[t]$, which are given as

$$F_{\varsigma_n[t]}(x_n) = 1 - P_{X_n^2[t]}(-\frac{2\widehat{\sigma}_n^2[t]}{\varrho_n'^2}\ln(\frac{x_n}{\widehat{\alpha}_n[t]}); 1, \lambda_n^{\mathrm{MD}}[t]) = \int_{-\infty}^{x_n} f_{\varsigma_n[t]}(\tau)d\tau. \tag{3.56}$$

Furthermore, $\prod$ represents the product of a sequence. C_1 and C_2 are denoted as the domains of multiple integral in (3.51) and (3.52), respectively, which satisfy $0 < Y[t] < \nu$ and $\nu \leq Z[t] \leq 1$.

Proof: According to (3.50), the probability of occurrence $P_{\mathrm{FA}}[t]$ of (3.45) can be calculated as

$$\begin{aligned} P(0 < y[t] < \nu \mid \Phi_0) &= P(0 < \sum_{n=1}^{N} \widehat{\alpha}_n[t] \exp(-\frac{\varrho_n'^2}{2\widehat{\sigma}_n^2[t]} X_n^2[t]) < \nu \mid \Phi_0) \\ &= P(0 < \sum_{n=1}^{N} \xi_n[t] < \nu). \end{aligned} \tag{3.57}$$

Note that $X^2_{n,\lambda_n^{\mathrm{FA}}}[t]$ obeys the noncentral chi-squared distribution with 1 degree of freedom and $\lambda_n^{\mathrm{FA}}[t]$ in the case of Φ_0. Therefore, the CDF of variable ξ_n can be shown in (3.54), and the false alarm rate of the proposed scheme is expressed as (3.51). Furthermore, $P_{\mathrm{MD}}[t]$ of (3.46) is given by

$$\begin{aligned} P(\nu \leq y[t] \leq 1 \mid \Phi_1) &= P(\nu \leq \sum_{n=1}^{N} \widehat{\alpha}_n[t] \exp(-\frac{\varrho_n'^2}{2\widehat{\sigma}_n^2[t]} X_n^2[t]) \leq 1 \mid \Phi_1) \\ &= P(\nu \leq \sum_{n=1}^{N} \varsigma_n[t] \leq 1). \end{aligned} \tag{3.58}$$

Note that $X^2_{n,\lambda_n^{\mathrm{MD}}}[t]$ obeys the noncentral chi-squared distribution with 1 degree of freedom and $\lambda_n^{\mathrm{MD}}[t]$ in the case of Φ_1, and its CDF is shown in (3.56). Therefore, the misdetection rate of the fuzzy learning-based authentication scheme is expressed as (3.52). □

Remark 3.9. It is observed from Theorem 3.4 that the false alarm rate depends on the variations of Alice's attributes $\upsilon_n[t]$, $n = 1, 2, ..., N$. Therefore, without updating the system parameters, namely for $\widehat{\sigma}_n^2$, $\widehat{\mu}_n$ and $\widehat{\alpha}_n$ in (3.50), the designed fuzzy multiple attribute combination model will result in low authentication accuracy in the time-varying environment. In next section, a hybrid learning algorithm will be proposed for updating these system parameters.

3.4.1 Multi-Dimensional Adaptive Authentication Architecture

In this section, an optimization problem based on the expressions of false alarm rate and misdetection rate and a multi-dimensional adaptive authentication architecture are designed. Then, a hybrid learning algorithm is proposed to describe and update the system parameters of the designed fuzzy multiple attribute combination model. The hybrid learning algorithm focuses on updating the system parameters to solve the designed optimization problem, which describes the false alarm vs. misdetection trade-off, thus reliable authentication in the time-varying environment can be achieved.

As discussed above, the authentication performance of the designed fuzzy multiple attribute combination model can be improved by well deciding and updating the parameters $\widehat{\mu}_n$, $\widehat{\sigma}^2_n$ and $\widehat{\alpha}_n$ in (3.50). Due to the inevitable trade-off between false alarm and misdetection [2, 114], the authentication optimization problem is designed as

$$\begin{aligned} &\min_{(\widehat{\mu}_n,\widehat{\sigma}^2_n,\widehat{\alpha}_n,\nu),n=1,2,\ldots,N} \quad P_{\mathrm{FA}}, \\ &\text{s.t. } P_{\mathrm{MD}} \leq \delta, \end{aligned} \tag{3.59}$$

where δ represents the threshold of misdetection rate. Given a δ, the threshold of authentication in (3.3), namely for ν, can be determined by letting $P_{\mathrm{MD}} = \delta$. Then, the threshold ν is fixed in the subsequent authentication process, and the proposed scheme focuses on improving the authentication accuracy through tracking the variations of the adopted physical layer attributes of Alice and updating system parameters near-instantaneously.

In order to study and update the system parameters (i.e., $\widehat{\mu}_n$, $\widehat{\sigma}^2_n$ and $\widehat{\alpha}_n$) near-instantaneously, the fuzzy combination model of (3.43) is described as a multi-dimensional adaptive authentication architecture with these parameters in Figure 3.9. In this adaptive architecture, each input-output behavior is determined by a collection of modifiable parameters. The multi-dimensional adaptive authentication architecture can be expressed as follows:

Step 1: The inputs of multi-dimensional adaptive authentication architecture are denoted as $\boldsymbol{h'}[t] = (h'_1[t], h'_2[t], ..., h'_N[t])^{\mathrm{T}}$ with each element is designed in (3.41). Then a degree of membership value $u_{[-1,1]}(h'_n[t])$ of (3.42) can be obtained.

Step 2: By multiplying the parameter $\widehat{\alpha}_n$ with the output $u_{[-1,1]}(h'_n[t])$ of Step 1, the $\widehat{\alpha}_n u_{[-1,1]}(h'_n[t])$

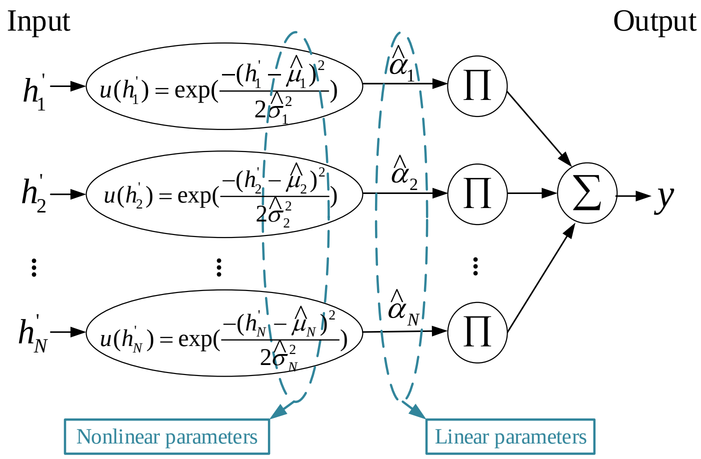

Input
Output
h_1'
$u(h_1') = \exp(\frac{-(h_1' - \hat{\mu}_1)^2}{2\hat{\sigma}_1^2})$
$\hat{\alpha}_1$
h_2'
$u(h_2') = \exp(\frac{-(h_2' - \hat{\mu}_2)^2}{2\hat{\sigma}_2^2})$
$\hat{\alpha}_2$
h_N'
$u(h_N') = \exp(\frac{-(h_N' - \hat{\mu}_N)^2}{2\hat{\sigma}_N^2})$
$\hat{\alpha}_N$
Π
Σ
y
Nonlinear parameters
Linear parameters

Figure 3.9: Multi-dimensional adaptive authentication architecture with linear parameters $\widehat{\alpha}_n$ and nonlinear parameters $\widehat{\mu}_n, \widehat{\sigma}_n^2$.

can be obtained.

Step 3: The overall output of the multi-dimensional adaptive authentication architecture is the summation of outputs of Step 2, which can be written as

$$y[t] = \widehat{\alpha}_1 \exp(\frac{-(h_1'[t] - \widehat{\mu}_1)^2}{2\widehat{\sigma}_1^2}) + \widehat{\alpha}_2 \exp(\frac{-(h_2'[t] - \widehat{\mu}_2)^2}{2\widehat{\sigma}_2^2}) + \cdots + \widehat{\alpha}_N \exp(\frac{-(h_N'[t] - \widehat{\mu}_N)^2}{2\widehat{\sigma}_N^2}). \quad (3.60)$$

As shown in Figure 3.9, the multi-dimensional adaptive authentication architecture is feed-forward, since the output of each step propagates from the input side (left) to the output side (right) unanimously. Besides, it is shown in (3.60) that the output of multi-dimensional adaptive authentication architecture is linear in $\widehat{\alpha}_n$, while it is nonlinear in $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$. Therefore, $\widehat{\alpha}_n$ are called as linear parameters, while $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$ are named as nonlinear parameters.

3.4.2 Hybrid Learning for Parameters Update

In this subsection, a hybrid learning algorithm is designed by combining the gradient descent and the least-square estimator for fast updating the system parameters.

Gradient Descent for Nonlinear Parameter Update

Given weights $\widehat{\alpha}_n, n = 1, 2, ...N$, the Gradient descent is applied to update the nonlinear parameters $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, thereby to solve the optimization problem of (3.59), which can be expressed as

$$\widehat{\mu}_n[k+1] = \widehat{\mu}_n[k] - \epsilon \frac{\partial P_{\text{FA}}}{\partial \widehat{\mu}_n}|_k \tag{3.61}$$

and

$$\widehat{\sigma}_n^2[k+1] = \widehat{\sigma}_n^2[k] - \epsilon \frac{\partial P_{\text{FA}}}{\partial \widehat{\sigma}_n^2}|_k, \tag{3.62}$$

where ϵ represents the step size of Gradient descent. $\partial P_{\text{FA}}/\partial\widehat{\mu}_n$ and $\partial P_{\text{FA}}/\partial\widehat{\sigma}_n^2$ are the first order partial derivatives of P_{FA} with respect to $\widehat{\mu}_n$ and that with respect to $\widehat{\sigma}_n^2$, respectively. Again, given the physical layer attributes adopted and attribute observations of Alice, the closed-from expression of P_{FA} can be obtained. Hence, the gradients in (3.61) and (3.62) can be derived.

Least-Square Estimator for Linear Parameter Update

Given the non-linear parameters $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, the least-square estimator is applied to update the weights $\widehat{\alpha}_n$ in (3.60). Consider that a set of Alice's observations $\{(\boldsymbol{h}'_l, \widehat{y}_l), l = 1, 2, ..., L\}$ is given, which is used for training the weights $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_1, \widehat{\alpha}_2, ..., \widehat{\alpha}_N)^{\text{T}}$ in the least-square estimator. Then, using the matrix notation, the following equation holds

$$\widehat{\boldsymbol{y}} = \boldsymbol{y} + \boldsymbol{e} = \boldsymbol{U}\widehat{\boldsymbol{\alpha}} + \boldsymbol{e}, \tag{3.63}$$

where $\widehat{\boldsymbol{y}} = (\widehat{y}_1, \widehat{y}_2, ..., \widehat{y}_L)^{\text{T}}$ are the observations for training, while $\boldsymbol{y} = (y_1, y_2, ..., y_L)^{\text{T}}$ represent the outputs of the fuzzy learning-based scheme with the corresponding inputs $\boldsymbol{h}'_l, l = 1, 2, ..., L$. Moreover, $\boldsymbol{e} = \widehat{\boldsymbol{y}} - \boldsymbol{y}$ represent the errors between the observations and outputs of the fuzzy learning-based scheme, and

$$\boldsymbol{U} = \begin{bmatrix} u_{[-1,1]}(h'_{11}) & \cdots & u_{[-1,1]}(h'_{N1}) \\ \vdots & \ddots & \vdots \\ u_{[-1,1]}(h'_{1L}) & \cdots & u_{[-1,1]}(h'_{NL}) \end{bmatrix}_{L\times N}. \tag{3.64}$$

Instead of finding the exact solution for (3.59), the proposed fuzzy learning-based scheme aims at searching for optimal linear parameters, i.e., $\widehat{\alpha}_n^*$, for minimizing the sum of squared error, which is given by

$$E(\widehat{\boldsymbol{\alpha}}) = \sum_{l=1}^{L} \gamma^{L-l} e_l^2 = \sum_{l=1}^{L} \gamma^{L-l} (\widehat{y}_l - y_l)^2 = (\widehat{\boldsymbol{y}} - \boldsymbol{U}\widehat{\boldsymbol{\alpha}})^{\mathrm{T}} \boldsymbol{\gamma} (\widehat{\boldsymbol{y}} - \boldsymbol{U}\widehat{\boldsymbol{\alpha}}), \tag{3.65}$$

where the $\gamma \in [0, 1]$ is forgetting factor to place the heavier emphasis on more recent data and

$$\boldsymbol{\gamma} = \begin{bmatrix} \gamma^{L-1} & 0 & \cdots & 0 \\ 0 & \gamma^{L-2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma^0 \end{bmatrix}_{L \times L} . \tag{3.66}$$

The utilization of forgetting factor γ in the proposed hybrid learning algorithm can decrease the influence of historical samples in the authentication system gently due to the decorrelation of physical layer attributes in the time-varying environment. According to [115], the closed-form of solution for minimizing $E(\widehat{\boldsymbol{\alpha}})$ of (3.65) can be obtained as

$$\widehat{\boldsymbol{\alpha}}^*[L] = (\boldsymbol{U}^{\mathrm{T}} \boldsymbol{\gamma} \boldsymbol{U})^{-1} \boldsymbol{U}^{\mathrm{T}} \boldsymbol{\gamma} \widehat{\boldsymbol{y}}. \tag{3.67}$$

Hence, given non-linear parameters $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, (3.67) provides an optimal linear parameter $\widehat{\boldsymbol{\alpha}}^*$ for multi-dimensional adaptive authentication.

Remark 3.10. If estimate of an attribute, i.e., H_n, cannot be obtained at some moments, $\widehat{\alpha}_n = 0$ is set directly, and update the other linear parameters via (3.67). Since each attribute in the authentication model (3.43) is independently taken into account, the parameter update for each attribute is also independent. This demonstrates the benefit of the proposed solution compared with the nonparametric methods [2], that is, once some attributes are unavailable at some moments, the remaining attributes will still contribute to the authentication model and make the model work, leading to a robust authentication performance.

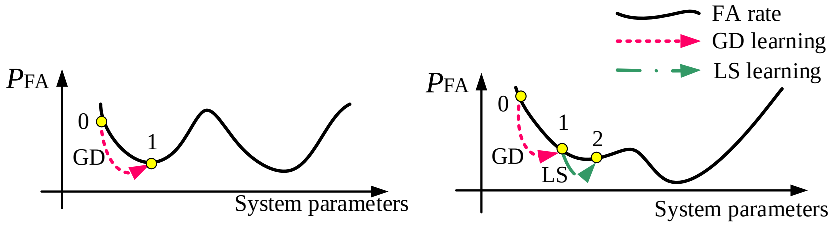
Hybrid Learning Algorithm

In order to improve the convergence performance of parameters updating, the gradient descent and least-square estimator presented above is combined, named as hybrid learning. The hybrid learning is implemented in a batch mode, each learning epoch is composed of forward pass and backward pass [115]. Given a threshold ν and a set of observations $\{(\boldsymbol{h}'_l, \widehat{y}_l), l = 1, 2, ..., L\}$, the weights $\widehat{\alpha}_n$ are updated according to (3.67) in the forward pass. After the weights $\widehat{\alpha}_n$ are identified, the $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$ can be updated via (3.61) and (3.62), respectively, in the backward pass. Then, the threshold ν is updated by letting $P_{\mathrm{MD}} = \delta$ with the updated parameters $(\widehat{\mu}_n^*, \widehat{\sigma}_n^{*2}, \widehat{\alpha}_n^*)$. As a conclusion, the proposed hybrid learning algorithm can be summarized in Algorithm 2.

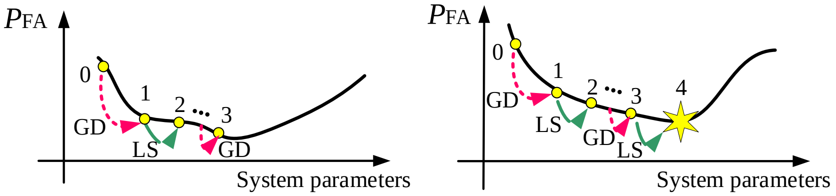
Algorithm 2 Hybrid learning for multi-dimensional adaptive authentication

```
    Given N physical layer attributes adopted, Alice's observations $\boldsymbol{h}'_l, l = 1, 2, ..., L$, step size
of Gradient descent $\epsilon$, initial parameters $\widehat{\alpha}_n[0], \widehat{\mu}_n[0], \widehat{\sigma}_n^2[0]$, and $\nu[0]$.
1. Iteration: $t = 1, 2, ...L$
    Gradient descent:
    1.1 obtain $(\widehat{\mu}_n^*[t], \widehat{\sigma}_n^{*2}[t])$ through updating means $\widehat{\mu}_n[k+1]$ and variances $\widehat{\sigma}_n^2[k+1]$ via
        (3.61) and (3.62), respectively, until $|\widehat{\mu}_n[k] - \widehat{\mu}_n[k-1]| < \varepsilon_1 \& |\widehat{\sigma}_n^2[k] - \widehat{\sigma}_n^2[k-1]| < \varepsilon_2$;
    1.2 update $P_{\mathrm{FA}}(\widehat{\mu}_n^*[t], \widehat{\sigma}_n^{*2}[t])$ via (3.51);
    Least square estimator:
    1.3 if the estimate of attribute $n$ is unvailable
    1.4     set $\widehat{\alpha}_n[t] = 0$;
    1.5 else
    1.6     obtain optimal weights $\widehat{\alpha}_n^*[t]$ through (3.67) and update $P_{\mathrm{FA}}(\widehat{\alpha}_n^*[t])$ via (3.51);
    1.7 end if
    1.8 update threshold $\nu$ by letting $P_{\mathrm{MD}}(\widehat{\mu}_n^*[t], \widehat{\sigma}_n^{*2}[t], \widehat{\alpha}_n^*[t]) = \delta$;
2. Multi-dimensional adaptive authentication: $t = L + 1$
    2.1 obtain new physical layer attribute estimate of authenticating transmitter $\boldsymbol{H}[t]$;
    2.2 predict authentication result using parameters $(\widehat{\mu}_n^*[L], \widehat{\sigma}_n^{*2}[L], \widehat{\alpha}_n^*[L])$ via (3.44):
        Alice/Eve;
    2.3 update parameters via Step 1 by renewing observation set to $\{(\boldsymbol{h}'_l, \widehat{y}_l), l = 1, ..., L + 1\}$;
```

Figure 3.10 characterizes the hybrid learning process of parameter update in the fuzzy learning-based scheme. Since the optimization problem of (3.59) is nonconvex, there may exist several minimal points and saddle points, as shown in Figure 3.10 (a). Given the initial values of linear parameters, the nonlinear parameters $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$ are updated by using gradient descent (GD) to achieve the point 1. Then based on the fixed $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, the least-square (LS) estimator is used to find an optimal weights $\widehat{\alpha}_n^*$ according to (3.67), achieving to point 2. Continuing this process, the point 4 can be found as shown in Figure 3.10 (d). Note that the false alarm rate of the proposed scheme is changing during the hybrid learning process. Therefore, through the proposed hybrid learning algorithm (see Algorithm 2), most of the minimal points and saddle points can be avoided, achieving better convergence performance.



(a) Nonlinear parameters update (b) Linear parameters update



(c) Nonlinear parameters update (d) Linear parameters update

Figure 3.10: Schematic diagram of the proposed hybrid learning process.

Remark 3.11. Given fixed $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, the weights $\widehat{\alpha}_n^*$ of (3.67) are the optimal values $\widehat{\alpha}_n$ in the weights space because of the squared error measure used. Therefore, by proposing the hybrid learning procedure (see Algorithm 2), the dimension of the search space is reduced, and the time needed to reach convergence is substantially decreased.

3.4.3 Convergence Analysis of Fuzzy Learning-based Scheme

This subsection analyzes the convergence of Algorithm 2 to show the performance of the proposed fuzzy learning-based authentication scheme. A general case is considered that at least one physical layer attribute adopted in the proposed scheme is dynamic. Then the following results can be obtained:

Theorem 3.5: If $\boldsymbol{\upsilon}[t] \neq \mathbf{0}$ satisfies, the proposed fuzzy learning-based authentication scheme with parameters $\widehat{\boldsymbol{\alpha}}[t]$, $\widehat{\boldsymbol{\mu}}[t]$, and $\widehat{\boldsymbol{\sigma}}^2[t]$ in Algorithm 2 performs better than that with parameters $\widehat{\boldsymbol{\alpha}}[t-1]$, $\widehat{\boldsymbol{\mu}}[t-1]$, and $\widehat{\boldsymbol{\sigma}}^2[t-1]$ at time instant t.

Proof: Given $\widehat{\boldsymbol{\alpha}}[t-1]$, $\widehat{\boldsymbol{\mu}}[t-1]$, and $\widehat{\boldsymbol{\sigma}}^2[t-1]$ at time instant $t-1$, the least-square estimator $\widehat{\boldsymbol{\alpha}}^*[t]$ of (3.67) can be obtained, which minimizes the sum of squared error for real-value authentication of (3.65) with a new observation $\widehat{y}[t]$. Therefore, for the given $\widehat{\boldsymbol{\mu}}[t-1]$ and $\widehat{\boldsymbol{\sigma}}^2[t-1]$, the sum of squared error for real-value authentication of (3.65) with parameters $\widehat{\boldsymbol{\alpha}}^*[t]$ is smaller than that parameters $\widehat{\boldsymbol{\alpha}}[t-1]$.

Then, given parameters $\widehat{\boldsymbol{\alpha}}^*[t]$, by setting $P_{\mathrm{MD}} = \delta$ in optimization problem (3.59), the nonlinear parameters $\widehat{\mu}_n[t]$ and $\widehat{\sigma}_n^2[t]$ can be updated via (3.61) and (3.62). Then it can be observed from Algorithm 2 as well as equations (3.61) and (3.62) that if the step size ϵ small enough, the following inequation satisfies

$$P_{\mathrm{FA}}(\widehat{\boldsymbol{\mu}}[t-1], \widehat{\sigma}_n^2[t-1]) > P_{\mathrm{FA}}(\widehat{\boldsymbol{\mu}}[t], \widehat{\sigma}_n^2[t]). \tag{3.68}$$

Therefore, the results of Theorem 3.5 are proved. □

Remark 3.12. Theorem 3.5 shows that Algorithm 2 achieves a reliable authentication performance in the time-varying environment. The reason is that the fuzzy learning-based physical layer authentication scheme promptly adjusts the authentication system to adapt the dynamic environment, so that a compelling false alarm rate vs. misdetection rate trade-off is achieved.

Remark 3.13. The proposed hybrid learning algorithm (i.e., Algorithm 2) combines the gradient descent and least-square estimator to update the system parameters for multi-dimensional adaptive authentication. On one hand, the false alarm rate P_{FA} is continuous, and satisfies Lipschitz condition with constant $J > 0$ in an arbitrary bounded subset of real numbers. Hence, if gradient descent is ran for k iterations with a fixed step size $\epsilon \leq 1/J$, gradient descent is guaranteed to converge with convergence rate $O(1/k)$. On the other hand, given the matrix $\boldsymbol{U}$ and closed-form of solution (3.67), the complexity of least-square estimator is $O(N^2 L)$.

3.4.4 Simulation Results

In order to show the performance of the proposed fuzzy learning-based scheme, case study and simulation results are provided in this section. Firstly, the proposed scheme is validated in a simulated urban scenario by utilizing carrier frequency offset (CFO), channel impulse response (CIR), received signal strength indicator (RSSI), and in-phase and quadrature imbalance (IQI). The parameter design and convergence performance of Algorithm 2 are demonstrated. Then, the fuzzy learning-based scheme is validated in a simulated indoor office scenario to show its performance. The comparison results between the fuzzy learning-based scheme and some existing schemes are presented, i.e., the optimal weights-based scheme and neural network-based scheme, demonstrating the superior permanence of the fuzzy learning-based scheme.

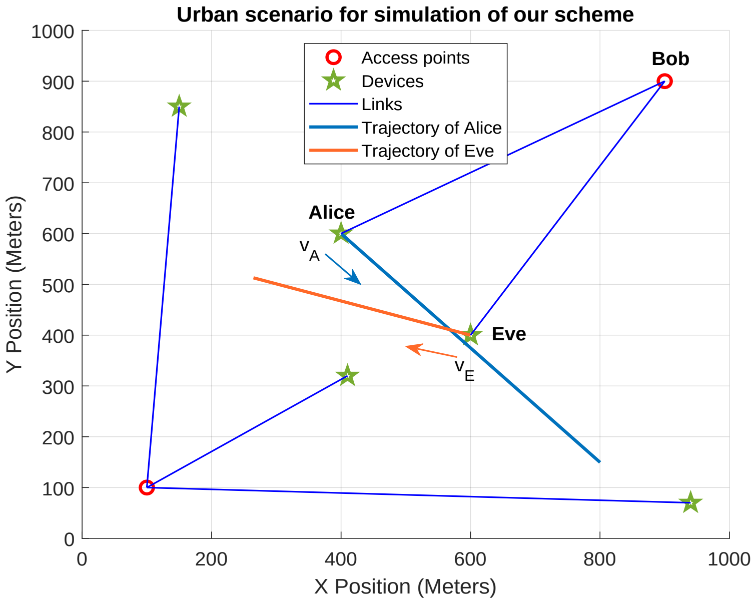


Figure 3.11: An urban scenario in the simulation.

Table 3.2: Simulation parameters of Chapter 3

Variable	Value	Variable	Value
Initial position of Alice	[400; 600] m	Position of Bob	[900; 900] m
Initial position of Eve	[600; 400] m	Antenna number of Alice/Eve	4
Antenna number of Bob	8	Antenna height	1 m
Velocity of Alice	[8; -9] m/s	Velocity of Eve	[-6.72; 2.26] m/s
Center frequency f_c	5 GHz	Sampling rate	20 MHz
Range	1000 m × 1000 m	SNR	20 dB

In this subsection, the proposed scheme is studied in an urban scenario, where its system topology is given in Figure 3.11. The locations of Alice, Bob and Eve, as well as the velocities of both Alice and Eve (denoted as v_A and v_E, respectively) are shown in this figure. The simulation parameters in this case study are given in Table 3.2. Specifically, the multipath channel model in this urban scenario is formulated as

$$H_{IR}(\tau;t) = \sum_{\kappa=1}^{K} A_\kappa(t)\delta(\tau - \kappa\Delta\tau), \tag{3.69}$$

where K is the number of multipath propagation paths, $\kappa\Delta\tau$ and A_κ represent the delay and complex amplitude of κ-th multipath component, respectively. Moreover, according to [118], the path loss model is given as

$$PL = 22.7\log_{10}(d[m]) + 41 + 20\log_{10}(\frac{f_c[GHz]}{5}), \tag{3.70}$$

where d is the distance between the transceiver.

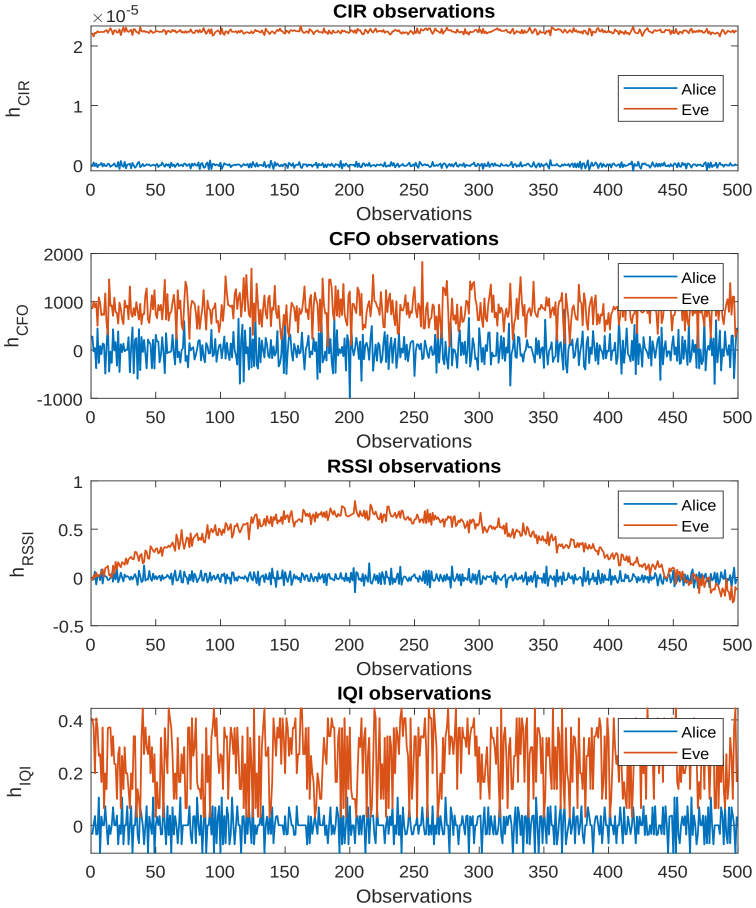


Figure 3.12: Variation measurements of CFO, CIR, RSSI, and IQI of Alice and Eve for simulation.

Given simulation parameters in Table 3.2, observations of CIR, CFO, RSSI, and IQI of both Alice and Eve can be obtained, where their variation measurements are shown in Figure 3.12. In the proposed scheme, 12 system parameters should be determined, namely for weights $\widehat{\alpha}_n$, means $\widehat{\mu}_n$ and widths $\widehat{\sigma}_n^2$, $n = 1, 2, 3, 4$ corresponding to CIR, CFO, RSSI, and IQI, respectively. Figure 3.13 characterizes the parameter design and update of the fuzzy learning-based scheme by Algorithm 2 with respect to weights $\widehat{\alpha}_n$, means $\widehat{\mu}_n$ and widths $\widehat{\sigma}_n^2$, $n = 1, 2, 3, 4$. The parameters are updated for each observation, and only 1 iteration is needed in the least square learning process. In this figure, 10 observations are used for training at the beginning of parameter design and authentication. It is shown in Figure 3.13 that with the increasing authentication time, the parameters are updated according to the variations of physical layer attributes. More importantly, Figure 3.13 demonstrates the compact characteristic of the proposed scheme in dealing with the dynamics of physical layer attributes due to only 10 observations used for learning and 12 system parameters to be determined in the case of utilizing 4 attributes. Figure

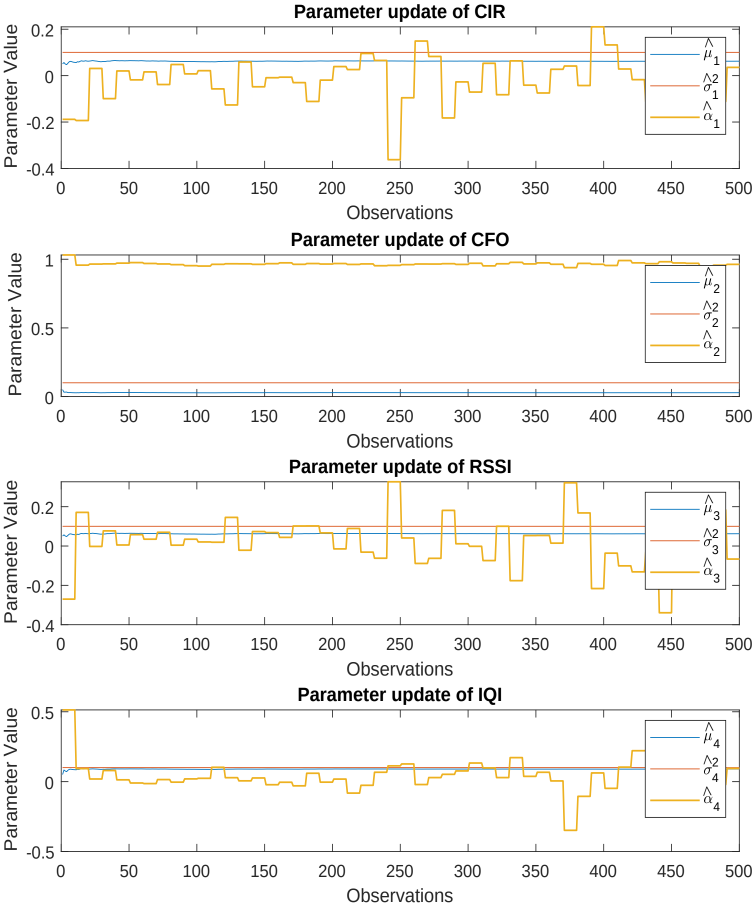


Figure 3.13: Parameter design and update by Algorithm 2.

3.14 characteristics the convergence of the proposed hybrid learning algorithm for 11-th observation, which is the convergence performance of the developed gradient descent for nonlinear parameter update in Algorithm 2. It is observed from Figure 3.14 that only about 50 iterations are needed for identifying a new attribute estimate of the transmitter with the learned system parameters (based on 10 observations).

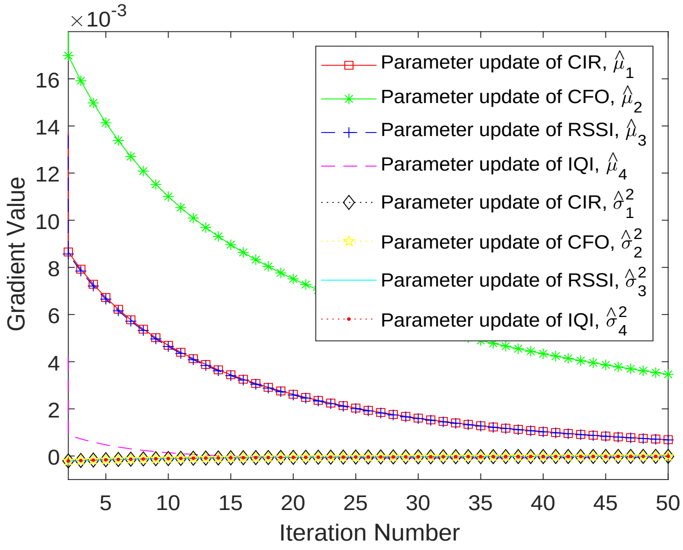


Figure 3.14: Convergence performance of Algorithm 2 for 11-th observation in Figure 3.13.

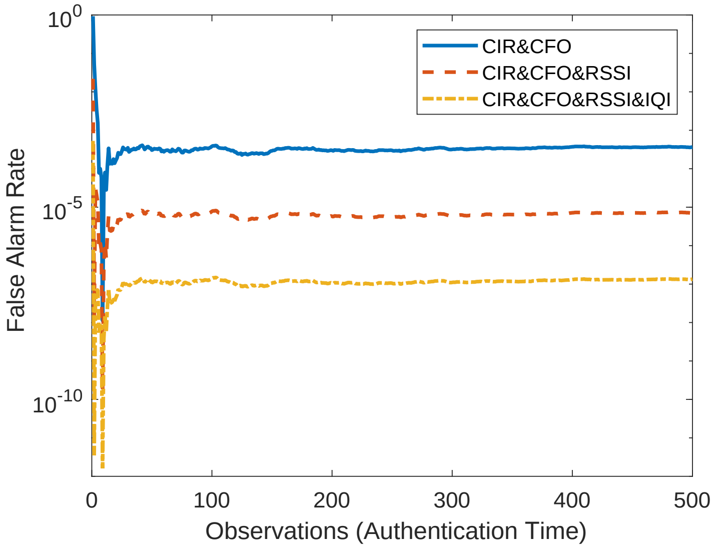


Figure 3.15: False alarm rate of the fuzzy learning-based scheme by different numbers of attributes.

Considering the utilization of different numbers of physical layer attributes, the authentication performance of the proposed scheme is characterized in Figure 3.15. Its system parameters of the proposed scheme in different cases, i.e., CIR & CFO, CIR & CFO & RSSI, and CIR & CFO & RSSI & IQI, are updated similarly as Figure 3.13. One can observe from Figure 3.15 that a larger number of attributes used leads to a more obvious improvement in authentication performance of the fuzzy learning-based scheme. The reason for this trend is that it is extremely unlikely for an adversary to predict or imitate all the attributes from the received signals. Moreover, reliable and robust authentication can be achieved by utilizing multiple attributes because of their different contributions on authentication and more information considered for identifying the transmitter. Therefore, utilization of multiple attributes for authentication schemes is extremely helpful to provide high uncertainty for the adversaries as well as high-dimensional protections for the legitimate devices.

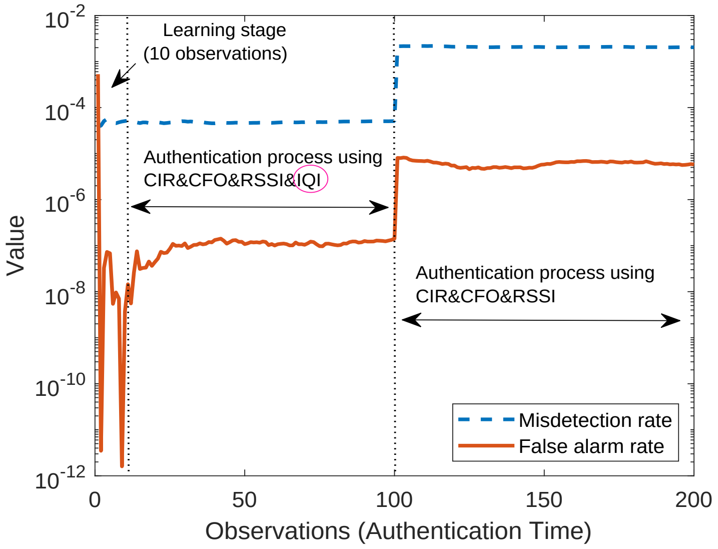


Figure 3.16: Robust performance of the fuzzy learning-based scheme.

Figure 3.16 characterizes the robust performance of the fuzzy learning-based scheme. Explicitly, 10 attribute observations are used for learning at the beginning of authentication. The adaptive authentication process is performed relying on four attributes, i.e., CIR & CFO & RSSI & IQI, during 11-100th authentication time instant. Then, the IQI is unavailable at the receiver from 101-th observation. It is observed from Figure 3.16 that once some of the adopted attributes are unavailable, the remaining attributes still contribute to the authentication model and make the model work, demonstrating the robustness of the fuzzy learning-based scheme in the complex time-varying environment.

Figure 3.17 characterizes the comparison results of the fuzzy learning-based (FL) scheme and the optimal weight-based (OW) scheme [114] in different cases, namely for CIR & CFO & RSSI & IQI and CIR & CFO & RSSI. It is observed from Figure 3.17 that with the increasing

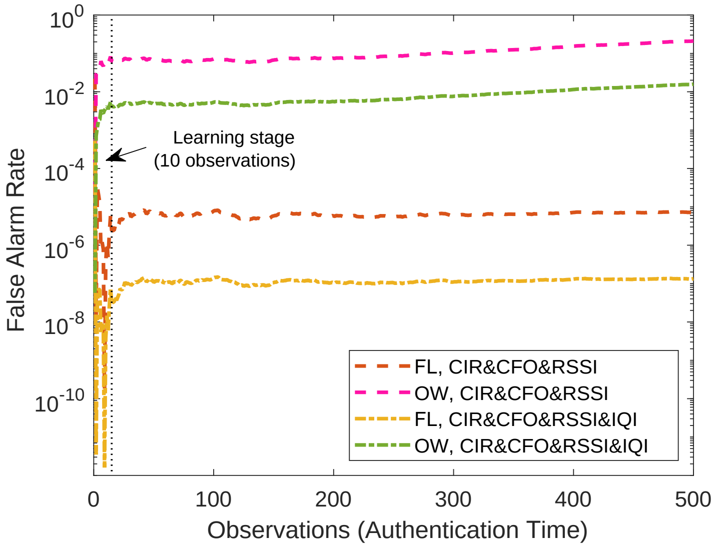


Figure 3.17: Comparison results of the fuzzy learning-based scheme and the optimal weight-based scheme of [114].

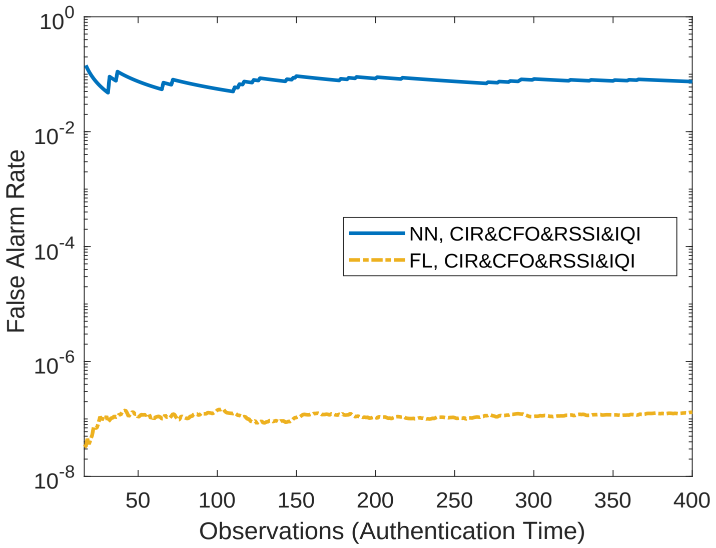


Figure 3.18: Comparison results of the fuzzy learning-based scheme and the neural network-based scheme of [119].

authentication time, the false alarm rate values of the fuzzy learning-based scheme in both cases keep stable, while that of the optimal weights-based scheme dramatically increase. The reason for this trend is that the optimal weights-based scheme is a static scheme and cannot update the system parameters according to the variations of physical layer attributes, thus cannot adapt to the dynamic environment. This also supports the results of Theorem 3.5. These all indicate that the proposed scheme performs better than the weights-based authentication scheme of [114]. As a conclusion, the results of Figure 3.15-3.17 characterize the benefits of the fuzzy learning-based scheme based on both multiple physical layer attributes and adaptive scheme.

Figure 3.18 characterizes the comparison results of the fuzzy learning-based (FL) scheme and a three-layer neural network-based (NN) scheme having 10 neurons for each layer [119]. It is observed from Figure 3.18 that the proposed scheme performs much better than the neural network-based scheme. Furthermore, the neural network-based scheme requires observations of the Spoofer for training, which limits its application in practical networks. Specifically, the fuzzy learning-based scheme straightforwardly utilizes the physical properties of the attributes in the fuzzy learning-based authentication process (see Figure 3.9), while the neural network cannot provide such information in the training process analytically and explicitly.

3.5 Chapter Summary

In this chapter, a kernel learning-based physical layer authentication scheme was proposed for combining the multiple physical layer attributes and for modelling the authentication as a linear system. Through the kernel machine-based multiple attribute fusion model, the number of dimensions of the search-space was reduced from N to 1, and the learning objective was formulated as a convex problem. Therefore, its complexity was substantially reduced. Then, by conceiving an adaptive authentication process relying on the kernel machine-based multiple attribute fusion model, the process advocated readily accommodated a time-varying environment by discovering and learning this complex dynamic environment. Both the convergence performance and the authentication performance of the proposed intelligent authentication process were theoretically analyzed and numerically validated. The simulation results showed that the authentication performance can be dramatically improved by increasing the number of physical layer attributes exploited by the proposed intelligent authentication process. Moreover, the proposed scheme has a much better authentication performance in a time-varying environment than its non-adaptive counterpart.

Then, a fuzzy learning-based physical layer authentication scheme was developed to improve the authentication performance from a robust and compact perspective. A fuzzy model was designed to combine the multiple physical layer attributes, which can efficiently mitigate the imperfectness of estimated attributes. By proposing an adaptive hybrid learning algorithm, i.e., the combination of least-square estimator and gradient method, the system parameters can be updated in real-time to adapt to the time-varying environment. Both the convergence performance and authentication performance of the proposed multi-dimensional adaptive authentication scheme were theoretically analyzed and validated in different simulation scenarios. It was demonstrated that the proposed scheme has much better authentication performance than some exiting schemes, such as the optimal weights-based scheme and neural network-based scheme.

In next chapter, the trust management will be explored for mitigating the risks of misdetection of authentication utilizing physical layer attributes. To be more specific, an adaptive trust management-based scheme will be proposed to achieve soft authentication and progressive authorization. The trust relationship between the transmitter and receiver will be established by validating the physical layer attributes. Moreover, the trust management will provide an efficient metric and method for multiple-level access control.

Chapter 4

Adaptive Trust Management for Soft and Progressive Security

Conventional authentication mechanisms routinely used for validating communication devices are facing significant challenges. This is mainly due to their reliance on both ‘spoofable’ digital credentials and static binary characteristic, and inevitable misdetection in physical layer authentication using time-varying attributes, leading to the cascading risks of security and trust. To circumvent these impediments and further reduce the effects of inevitable wrong decision of physical layer authentication, an adaptive trust management-based soft authentication and progressive authorization scheme is proposed in this chapter by intelligently exploiting the time-varying communication link-related attribute of the transmitter to improve wireless security. First of all, the trust relationship between the transmitter and receiver is established based on the evaluation of selected physical layer attribute for fast authentication and multiple-level authorization. Through the designed trust model, the transmitter is authorized by the specific level of services/resources corresponding to its trust level, so that soft security is achieved. To dynamically update the trust level of the transmitter, an online conformal prediction-based adaptive trust adjustment algorithm is proposed relying on the real-time validation of its attribute estimates at the receiver, thus resulting in progressive authorization. The performance of the proposed scheme is theoretically analyzed in terms of its individual risk and individual satisfaction. Simulation results demonstrate that the proposed scheme significantly improves the security performance and robustness in time-varying environments, and performs better than the static binary authentication scheme and existing physical layer authentication benchmarker.

4.1 Introduction

Due to the broadcast nature of radio signal propagation, owing to the intermittent nature of communications and the complex dynamic network environments encountered, wireless communications are vulnerable to spoofing attacks [4, 2, 79]. A spoofer may intercept the transmissions between legitimate devices and imitate them to obtain illegal benefits from networks/ systems, while counterfeiting authorized identities for fraud or other malicious purposes.

Although key-based cryptographic techniques [22, 23, 120, 121] have been widely used for authentication, they face increasing challenges in securing wireless communications. Differentiating devices with the aid of digital credentials cannot be readily achieved when the diverse attributes of communication devices are disregarded, thus leading to a high risk of undetected spoofing attacks [25]. Furthermore, the conventional key-based cryptographic techniques are static in time and binary in nature, where the devices either pass the security check or fail by a one-time authentication. These security schemes cannot help in detecting/preventing spoofers after the initial authentication has been completed. Although repeated authentication may theoretically be achieved with the aid of key-based cryptographic techniques by repeatedly logging into the server/system, the excessive latencies and computational overhead are particularly undesirable for delay-sensitive communications as well as for devices having limited battery lifetime and computational capability, such as the IoT devices [4, 2, 79].

Physical layer security techniques [25, 30, 37, 43, 48, 122, 123, 124] provide alternative authentication methods relying on the uniquely random link-related attributes, as exemplified by the channel impulse response (CIR) [2], carrier frequency offset (CFO) [37], and received signal strength (RSS) [25], just to name a few, which are difficult for malicious devices to impersonate and predict. Although they have obvious advantages including the low computational requirement, low network overhead and modest energy consumption, most of the physical layer authentication schemes based on the classic hypothesis test are also static in the time-domain, as exemplified by [43, 37, 30, 48]. Hence, they tend to be unsuitable for providing continuous identification. A kernel learning-based physical layer authentication scheme is proposed in [2] and Chapter 3 through tracking multiple time-varying attributes to provide lasting protection for legitimate links. However, the above schemes constitute binary admit/reject solutions as well as rely on separate authentication and authorization, hence resulting in latent loopholes for spoofing attacks because of the potential misdetection events in the physical layer authentication. Once an adversary passed the authentication by spoofing a legitimate device, the corresponding information/services/resources in the system will be leaked to this adversary. Furthermore, these binary-type solutions fail to provide differentiated levels of access control.

To overcome these challenges, the concept of *soft authentication and progressive authorization* is extremely beneficial for holistic system optimization in dynamic communication environments. The soft security solution provides a fast authentication and multiple-level authorization, while the progressive approach achieves continuous identification to enhance the security by multiple-step validation of the physical layer attribute observations. Through such a scheme, the threats and uncertainties caused by adversaries as well as the cascading risks in security and trust can be evaluated and controlled in real-time. In achieving this, the decision-making in a high layer is also required for modeling the soft authentication and progressive authorization as well as for security enhancement.

Trust management processes symbolic representations of the trustworthiness in support of a decision-making process, which has been widely studied in dealing with security problem-s in the literature [9, 125, 126, 127, 128, 129, 130, 131, 132]. However, conventional trust management approaches are usually used for modeling the trust relationships among authenticated users/devices for supporting cooperations in wireless networks. This chapter focuses on proposing an adaptive trust management approach by evaluating the attribute estimation of the transmitter to establish the trust relationship between transceiver for authentication and to provide metric for authorization. Through exploring the adaptive trust management, this radical solution provides fast authentication and dynamic multiple-level authorization, thus resulting in soft and progressive security. More importantly, the trust management-based scheme moves further away from the classical mechanisms, since it quests a holistic system design of unified authentication and authorization based on the continuous evaluation of time-varying physical layer attribute, which requires new wireless radio technologies. Hence, the machine learning techniques [4, 2] are studied in this chapter for adaptive trust management through classifying the time-varying attribute estimates of the transmitter.

In the unsupervised machine learning techniques of [133, 134, 135, 136], an assumption is usually made for the classification between normal and abnormal events that normal events are those that occur frequently and anomalous events occur rarely. This leads to a high false alarm rate in physical layer authentication, since those rare attribute observations may be deemed to be from the Spoofer. Therefore, the family of supervised learning techniques is invoked for the classification of the time-varying physical layer attribute estimates, which may be from legitimate devices and (or) adversaries. However, most of the existing supervised machine learning techniques have a limited capability to update the trustworthiness of an authenticating transmitter because of the lack of information on how close their predictions are to the real observations. Hence, the conformal prediction technique of [137, 138, 139] is explored in this chapter, where a valid measurement of each individual prediction is provided along with a confidence value based on the learning algorithms. More importantly, by invoking the online machine learning technique of [140, 141], the associated real-time classification results can be used for adaptive trust management, thus improving the security performance in time-varying communication scenarios.

In a nutshell, the proposed online conformal prediction-based adaptive trust management approach provides differentiated levels of continuous protection for legitimate communications. Such approach evaluates the trustworthiness of an authenticating transmitter using its physical layer attribute dynamically, thereafter the corresponding level of services/resources is authorized to the transmitter according to its trust level. Furthermore, it integrates authentication and authorization for achieving seamless and holistic system optimization, thus leaving fewer loopholes open for spoofing attacks.

Specifically, the contributions of this chapter are summarized as follows:

- To achieve the soft security, a trust model is designed for evaluating the trustworthiness of an authenticating transmitter relying on physical layer attribute without requiring its statistical properties. This model achieves fast authentication and provides a metric for multiple-level authorization to deal with the threats caused by adversaries and to control the risks of being attacked;

- An online conformal prediction-based adaptive trust adjustment algorithm is proposed for real-time validation of transmitter and for dynamically updating the trust model developed. Therefore, the proposed scheme becomes capable of adapting to time-varying environments for security enhancement;

- Simulation results demonstrate that the proposed scheme describes a soft access control and continuous procedure of authentication, thereby providing reliable adaptive protection for legitimate communication links. The superiority of the proposed scheme is demonstrated over the static binary authentication scheme and an exiting physical layer authentication scheme.

The rest of this chapter is organized as follows. In Section 4.2, the system model used in this chapter is presented. In Section 4.3, the online conformal prediction-based adaptive trust management scheme is proposed for achieving soft authentication and progressive authorization using physical layer attribute. The security performance analysis of the proposed scheme is also presented in Section 4.3, while the simulation results are discussed in Section

Table 4.1: Notations of Chapter 4

Notations	Definitions
H_A	Attribute estimate collected from Alice.
H_O	Attribute estimate collected from Alice or the Spoofer.
$\mathcal{F}$	Trust value of relationship $\{Bob : Transmitter, Alice\}$.
N	Number of authorization levels.
R_{ind}	Individual risk of the proposed scheme.
S_{ind}	Individual satisfaction of the proposed scheme.
Ψ_0	Scenario that the transmitter is the Spoofer.
Ψ_1	Scenario that the transmitter is Alice.
Γ	Conformal predictor.
y	Label of an attribute estimate.
Z	Set of training samples in conformal predictor.
Y	Predicted set of conformal predictor.
ϵ	Significance level of conformal predictor.
$1-\epsilon$	Confidence level on the predicted set Y.
e	Error made by the conformal predictor.
A	Nonconformity measure function.
α	Nonconformity score.
p	p-value of the conformal predictor.
L	Number of training samples.

4.4. Finally, Section 4.5 concludes the chapter.

Notations: In this chapter, scalars are denoted by italic letters, while vectors are respectively denoted by bold-face letters. Table 4.1 shows the notations of this chapter.

4.2 System Model and Problem Formulation

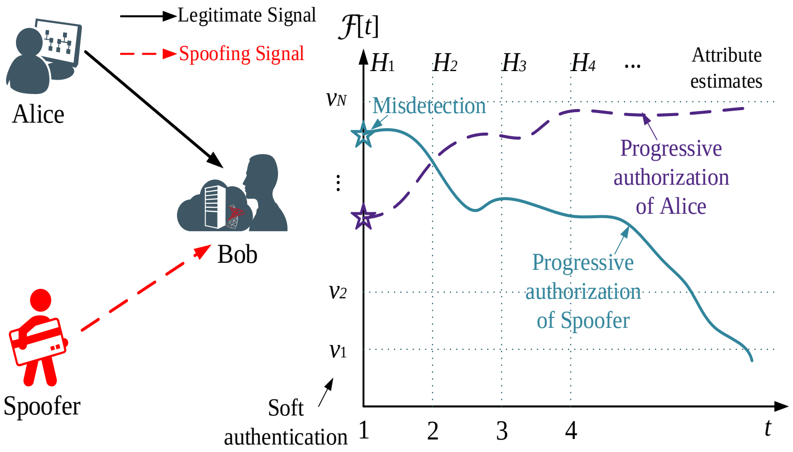


Figure 4.1: Soft authentication and progressive authorization system between Alice and Bob using a physical layer attribute continuously.

As shown in Figure 4.1, the attack model in a time-varying environment is characterized, where Alice and Bob represent a pair of legitimate devices and aim for communicating in the presence of a Spoofer, who tries to impersonate Alice and hence to access the system. More explicitly, the Spoofer not only tries to intercept Alice's transmission, but also to imitate her for obtaining illegal benefits from Bob. The Spoofer also tries to counterfeit authorized identities for fraud or other malicious purposes. The aggregated spoofing channel (i.e., the physical channel spanning from the Spoofer to Bob, as well as the hardware and analog components involved) is assumed to be independent of the main channel between Alice and Bob. Therefore, it is hard for the Spoofer to predict and clone Alice's physical layer attributes, such as her CIR, CFO, and RSS. In this chapter, only one physical layer attribute is utilized for authentication and authorization.

At the beginning of communication between Alice and Bob, existing security schemes have been used to establish initial authentication between them explicitly. Indeed, it is reasonable to expect that the devices have to be registered before joining the communication system, which is a basic prerequisite of physical layer authentication schemes [43, 37, 30, 48]. L estimates of the selected physical layer attribute of Alice can be obtained during the established initial authentication phase, which are denoted as

$$H_{A1}, H_{A2}, ..., H_{AL}, \tag{4.1}$$

where each H_{Al} represents an attribute estimate collected from Alice, $l \in \{1, 2, ..., L\}$ is an estimation time index, and L is the number of estimates during the established initial authentication phase. The major objective of physical layer authentication is to verify that the information received is from a legitimate device (i.e., Alice) by exploiting the difference between the estimates $H_{A1}, H_{A2}, ..., H_{AL}$ and new estimates of the selected attribute arriving from the transmitter (i.e., Alice or the Spoofer) during the subsequent communication stages. The new attribute estimates are denoted as H_{Ot}, explicitly showing the time instants of physical layer authentication $t = 1, 2, 3, ...$ Due to the dynamic nature of the environment encountered, the attribute estimates H_{Ot} are likely to be time-varying. Explicitly, the new attribute estimates H_{Ot} may have arrived from Alice or the Spoofer, and the validation of these estimates has to identify whether they are from Alice or the Spoofer. Moreover, the physical layer authentication starts at time instant $t = 1$ by identifying the estimate H_{O1}, which is arranged to be the $(L + 1)$-st attribute estimate, because L estimates of Alice have been collected during the initial authentication phase. Then, the physical layer authentication at time instant $t = 1$ is formulated as

$$\Delta H_{O1} = f(H_{A1}, H_{A2}, ..., H_{AL}, H_{O1}), \tag{4.2}$$

where $f(\cdot)$ represents a function that quantifies the difference between the estimates H_{A1}, H_{A2}, ..., H_{AL} and H_{O1}. The nonconformity measure of [143] will be applied in the proposed scheme for characterizing this difference. If the difference ΔH_{Ot} is small enough, the signal is deemed to be coming from Alice, otherwise, from the Spoofer. It is assumed that the attribute estimation noises of Alice and the Spoofer are independent and identically distributed, which may caused by the measurement errors, channel noises, interferences in the wireless communication environment, and so on.

In order to achieve security enhancement, this chapter focuses on proposing a novel adaptive trust management approach for achieving soft authentication and progressive authorization in dynamic communication environments. To be more specific, the proposed soft security solution provides prompt authentication and multiple-level authorization, while the progressive approach enhances the security by multiple-step validation of the time-varying physical layer attribute considered. The varying threats and uncertainties caused by the Spoofer and the cascading risks in security can be evaluated and controlled in real-time by the proposed scheme. Furthermore, various levels of protection can be provided for legitimate communications.

The trust relationship between the transmitter (i.e., Alice or the Spoofer) and Bob is characterized for the sake of evaluating the trustworthiness of the transmitter as follows:

Definition 4.1: The trust level of the relationship $\{Bob : Transmitter, Alice\}$ at time t is defined as the probability that the transmitter is deemed to be Alice in Bob's point of view by identifying the selected physical layer attribute, which is represented as

$$\mathcal{F}[t] = \Pr\{Bob : Transmitter, Alice\} \in [0, 1]. \tag{4.3}$$

It can be observed from Definition 4.1 that Bob has full trust in the transmitter when $\mathcal{F}[t] = 1$, and Bob totally distrusts the transmitter if $\mathcal{F}[t] = 0$. Then the new concept of multiple-level authorization is developed, where N classes of security services/resources are defined, denoted as $\{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$. The multiple-level authorization classes satisfy $\Phi_0 \subset \Phi_1 \subset ... \subset \Phi_{N-1}$, where Φ_{N-1} represents the highest level of authorization, while Φ_1 is the lowest one. Moreover, Φ_0 represents failed authentication and access denial for Bob. The proposed soft authentication and progressive authorization scheme can be formulated as

$$\begin{cases} \Phi_0 : & \mathcal{F}[t] \in [v_0, v_1] \\ \Phi_1 : & \mathcal{F}[t] \in (v_1, v_2] \\ & \vdots \\ \Phi_{N-1} : & \mathcal{F}[t] \in (v_{N-1}, v_N] \end{cases}, \tag{4.4}$$

where the thresholds satisfy $0 = v_0 < v_1 < v_2 < \cdots < v_{N-1} < v_N = 1$.

As shown in Figure 4.1, upon assuming the estimation range of the selected physical layer attribute as $[-a, a]$, the soft authentication and progressive authorization process is designed based on the trust level $\mathcal{F}[t]$ by evaluating the estimates of the selected attribute H_{Ot} as follows:

Soft authentication: The initial trust level of the relationship $\{Bob : Transmitter, Alice\}$ is set relying on the physical layer attribute estimate H_{O1} at time instant $t = 1$ according to the authentication of (4.2) as

$$\mathcal{F}[1] = 1 - \Delta H_{O1}. \tag{4.5}$$

If the initial trust level satisfies $\mathcal{F}[1] \in (\nu_n, \nu_{n+1}]$, the transmitter is allowed to access the services/resources associated with n-th level of authorization, namely at Φ_n, $n \in \{0, 1, ..., N-1\}$. In contrast to the conventional hypothesis testing-based authentication schemes [43, 37, 30, 48], the proposed soft authentication solution does not require any knowledge of the statical properties of the attribute selected and neither does it require the derivation of optimal thresholds for hypothesis testing. These simplifications lead to prompt authentication via (4.4), but the lack of having an optimal threshold may lead to an increased misdetection rate during the soft authentication of (4.5). Fortunately, both the multiple-level authorization and following progressive authorization designed for the proposed scheme are capable of enhancing the security by authorizing the corresponding class of security services and resources according to the trust level $\mathcal{F}$ as well as through the multiple-step validation of the physical layer attribute selected.

Progressive authorization: Given estimates of the selected physical layer attribute $H_{Ot} \in [-a, a]$ at time instants $t = 2, 3, 4, ...$, the trust level $\mathcal{F}$ should be updated to control the individual risk and individual satisfaction, which is formulated as

$$\mathcal{F}(H_{Ot}, \mathcal{F}[t-1]) : \ [-a, a] \times [0, 1] \quad \rightarrow \quad [0, 1], \tag{4.6}$$

where the individual risk and individual satisfaction are given in Definitions 4.2 and 4.3, respectively. The proposed progressive solution provides security enhancement by validating the transmitter continuously for ensuring that the security risks caused by inevitable misdetection during the soft authentication can be evaluated by the proposed trust management approach as well as carefully controlled by the judicious adjustment of the authorization level via (4.4).

Upon denoting the scenarios when the signal is from the Spoofer and from Alice by Ψ_0 and Ψ_1, respectively, the individual risk and individual satisfaction of the proposed scheme is defined as:

Definition 4.2: The individual risk level of the proposed soft authentication and progressive authorization scheme at time t is formulated as

$$R_{\text{ind}}[t] = \sum_{n=1}^{N-1} r_n \cdot \Pr(\mathcal{F}[t] \in (\nu_n, \nu_{n+1}] \mid \Psi_0), \tag{4.7}$$

where r_n is Bob's degree of loss or damage, if the system assigns the authorization level Φ_n to the Spoofer.

Definition 4.3: The individual satisfaction level of the proposed soft authentication and progressive authorization scheme at time t is given by

$$S_{\text{ind}}[t] = \sum_{n=1}^{N-1} s_n \cdot \Pr(\mathcal{F}[t] \in (\nu_n, \nu_{n+1}] \mid \Psi_1), \tag{4.8}$$

where s_n denotes Alice's degree of satisfaction at the authorization level Φ_n.

According to Definitions 4.2 and 4.3, the individual risk quantifies the potential loss of Bob if the Spoofer is granted authentication, while the individual satisfaction level quantifies the utility of services/resources granted to Alice by Bob. Note that $P_{\text{MD}} = R_{\text{ind}}$ and $P_{\text{FA}} = 1 - S_{\text{ind}}$ satisfy in the conventional binary authentication associated with $N = 2$ and $r_1 = s_1 = 1$, where P_{MD} and P_{FA} represent the misdetection rate and false alarm rate, respectively. Furthermore, it is observed from (4.7) and (4.8) that there is a trade-off between the individual risk and individual satisfaction level associated with the thresholds $\nu_1, \nu_2, ..., \nu_{N-1}$. If the thresholds are set too low, Bob will suffer from a higher individual risk, because the Spoofer may more easily succeed in imitating Alice and accessing a higher authorization level, but Alice will access more valuable services/resources to achieve a higher level of individual satisfaction. By contrast, if they are set too high, the proposed scheme may suffer from a low individual satisfaction level because of the lower authorization level Alice has, although Bob will experience a lower risk level. In the specific communication scenarios requiring high-security protection, the thresholds of the proposed scheme can be increased for reducing the risk caused by the Spoofer during the soft authentication stage.

Remark 4.1. The designed trust model provides an efficient metric for multiple-level authorization and for coping with the uncertainty and uncontrollability caused by the Spoofer. In contrast to the conventional physical layer authentication schemes [43, 37, 30], which minimize the misdetection rate while guaranteeing the false alarm rate, the proposes scheme focuses on enhancing security by updating the trust level $\mathcal{F}[t]$ based on the validation of the attribute estimates H_{Ot} continuously. Hence, an adaptive trust adjustment algorithm will be proposed to achieve soft authentication and progressive authentication in next section.

4.3 Proposed Adaptive Trust Management Scheme

In order to adaptively update the trust level $\mathcal{F}$ for soft authentication and progressive authorization, the online conformal prediction technique is explored for classifying the new collected estimates of the physical layer attribute used, i.e., $H_{Ot}, t = 1, 2, 3, ...$, which are time-varying and imperfectly estimated. Through developing an adaptive trust adjustment algorithm based on the confidence of prediction results, security enhancement can be achieved by multiple-step validation of the selected attribute and by appropriately adjusting authorization level in real-time.

4.3.1 Conformal Predictor for Classification of Attribute Estimates

To classify the new attribute estimates, the conformal prediction technique is explored in this subsection, which is a method conceived for providing valid measures of confidence for individual predictions by machine learning algorithms [142]. One of the main advantages of a conformal predictor is that it can guarantee that the probability of making erroneous predictions is the same as a pre-defined significance level (apart from some statistical fluctuations) [138]. The initial training set is denoted as $\{z_1, z_2, ..., z_L\} = \{(H_{A1}, 1), (H_{A2}, 1), ..., (H_{AL}, 1)\}$. In general, each training sample z_l contains an attribute estimate in the set $[-a, a]$ and a label of $y_l \in \{0, 1\}$. The label '0' indicates that the attribute estimate is from the Spoofer, while label '1' indicates that it is from Alice. The set of training inputs is denoted by $\mathcal{Z} = [-a, a] \times \{0, 1\}$.

Given a new sample having the observed attribute H_{O1} and a defined *significance level* of

$\epsilon \in [0, 1]$, a conformal predictor outputs a predicted set of $Y^{\epsilon}_{L+1} \subseteq \{0, 1\}$ for the unknown label y_{L+1}. Note that H_{O1} is arranged to be $L + 1$-th attribute estimate because of the L estimates of Alice collected during the initial authentication phase. The complementary value of $(1 - \epsilon)$ is called *confidence level*. It will always consider nested prediction sets $Y^{\epsilon_1}_{L+1} \subseteq Y^{\epsilon_2}_{L+1}$ when $\epsilon_1 \geq \epsilon_2$. The conformal predictor is formulated as a measurable function

$$\begin{aligned} \Gamma : \quad & \mathcal{Z}^* \times [-a, a] \times [0, 1] && \rightarrow && \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} \\ & z_1, z_2, ..., z_L,\ H_{O1},\ \epsilon && \rightarrow && Y^{\epsilon}_{L+1}, \end{aligned} \tag{4.9}$$

where $(z_1, z_2, ..., z_L) \in \mathcal{Z}^*$.

The predicted set is valid at the specified significance level ϵ in the sense that the probability of an error satisfies

$$\Pr(y_{L+1} \notin Y^{\epsilon}_{L+1}) \leq \epsilon, \tag{4.10}$$

under the randomness assumption [142]. That is to say, it has more than $(1 - \epsilon)$ confidence in the predicted set Y^{ϵ}_{L+1}. For example, in the case of $\epsilon = 0.1$, the probability that a prediction set includes the true label is at least 90%. Whether Γ makes an error on the $L + 1$-th trial can be represented by 1 and by 0 in case of no error as

$$e^{\epsilon}_{L+1} = \begin{cases} 1, \text{ if } y_{L+1} \notin Y^{\epsilon}_{L+1} \\ 0, \text{ otherwise} \end{cases} . \tag{4.11}$$

The basic idea of conformal prediction is to estimate the p-value for $y \in \{0, 1\}$, denoted as p_y, and to exclude those labels from the predicted set, which satisfy $p_y < \epsilon$. This p-value indicates how different a sample is from a set of training samples, and the higher the p-value, the better this sample fits the group of other samples. In order to obtain the p-value, the nonconformity measure of [143] is applied for estimate H_{O1} as

$$A_{L+1} : \mathcal{Z}^* \times \mathcal{Z} \rightarrow \mathfrak{R}. \tag{4.12}$$

Then the nonconformity score, which measures how different a sample z_l is from other samples in the set $\{z_1, z_2, ..., z_L, z_{L+1}\}$ [143], can be defined as

$$\alpha_l : A_{L+1}(\{z_1, z_2, ..., z_{l-1}, z_{l+1}, ..., z_L, z_{L+1}\}, z_l) \tag{4.13}$$

for each sample z_l in $\{z_1, z_2, ..., z_L, z_{L+1}\}$. It can be observed from (4.13) that z_{L+1} depends on an unknown y_{L+1}, so that the nonconformity score α_l relies on a variable $y \in \{0, 1\}$, which is a possible label for the new observation of the selected physical layer attribute H_{O1}. The nonconformity scores are based on the output of a classical underlying predictor, as exemplified by the ridge regression technique of [144], the k-nearest neighbours method of [145] and the autoregressive moving average solution of [146].

Then the p-value of z_{L+1} with different y in set $\{0, 1\}$ can be estimated as the ratio of the nonconformity scores $\alpha_1, \alpha_2, ..., \alpha_L$ that are at least as large as α_{L+1}, which is given as

$$p_{y,L+1} = \frac{|\{l = 1, 2, ..., L : \alpha_l \geq \alpha_{L+1}\}|}{L}, \tag{4.14}$$

where $|\cdot|$ represents the number of samples in the set $\{z_1, z_2, ..., z_L\}$ satisfying $\alpha_l \geq \alpha_{L+1}$ [142]. The predicted set is formed by estimating the p-value for each sample having a nonconformity score, and by adding those samples associated with p-value$\geq \epsilon$, which is formulated as

$$Y^{\epsilon}_{L+1} = \{y : y \in \{0, 1\}, p_{y,L+1} \geq \epsilon\}. \tag{4.15}$$

Remark 4.2. Given the conformal predictor developed, the estimates of the selected physical layer attribute can be classified. Then the trust level $\mathcal{F}[t]$ can be adaptively adjusted depending on the classification results and the confidence level $(1 - \epsilon)$ in real-time for progressive authorization, which will be explored in next subsection.

4.3.2 Adaptive Trust Adjustment based on Online Machine Learning

In order to dynamically update the trust level $\mathcal{F}$ based on the validation results of estimates $H_{Ot}, t = 1, 2, 3, ...$ in this subsection, an online conformal prediction-based adaptive trust adjustment algorithm is proposed. In online learning, the samples $z_{L+t} = (H_{Ot}, y_{L+t}), t = 1, 2, 3, ...,$

are presented one by one. The attribute estimate H_{Ot} is observed and its label y_{L+t} is predicted for each time, and then it moves on to the next attribute estimate. After obtaining the label of each physical layer attribute estimate, the training set $\{z_1, z_2, ..., z_L\}$ is updated by incorporating it and its label, as well as by removing the decorrelated historical training estimates. This is because the physical layer attribute used may become gradually uncorrelated after a period of time. Hence, the training set is also time-varying for maintaining its capability of adapting to the dynamic environment. Note that the attribute estimate at time instant t, namely H_{Ot}, is arranged to represent the $(L+t)$-th trial in the online conformal predictor due to having L initial training samples used at the beginning of physical layer authentication.

This algorithm focuses on validating the collected attribute estimates of the transmitter, i.e., $H_{Ot}, t = 1, 2, 3, ...$, thereby to dynamically update the trust level $\mathcal{F}$ relying on the real-time classification results of H_{Ot}, so that progressive authentication associated with multiple-level authorization can be achieved. To be more specific, according to Definition 4.1, if Bob observes that the attribute estimate H_{Ot} is classified to be from Alice, the trust level $\mathcal{F}$ will be increased, otherwise, it will be decreased. In this way, the designed trust model becomes robust even if an inaccurate classification occurs during the learning process. At the same time, the risk of a misdetection taking place during the soft authentication stage can be controlled by authorizing the corresponding class of security services/resources according to the trust level $\mathcal{F}[t]$ and by multiple-step validation.

According to the results in [142], the confidence predictor Γ is exactly valid if for each ϵ, $e_1^\epsilon, e_2^\epsilon, ...$ is a sequence of independent Bernoulli-distributed random variables. Unfortunately, the notion of exact validity is vacuous for confidence predictors, since no-confidence predictor is exactly valid [142]. A modification of conformal predictors is developed in [143], named smooth conformal predictor Γ^{sm}, by redefining p-value as

$$p_{y,L+t}^{\text{sm}} = \frac{|\{l : \alpha_l > \alpha_{L+t}\}| + \eta\, |\{l : \alpha_l = \alpha_{L+t}\}|}{L+t-1}, \tag{4.16}$$

where l ranges over $\{1, 2, ..., L+t-1\}$ and η is generated randomly from the uniform distribution on $[0, 1]$. Then, the following Lemma can be obtained:

Lemma 4.1 [143]: Given any significance level ϵ, the output of the smooth conformal predictor

Γ^{sm} satisfies

$$\lim_{t\to\infty} \wp_t = 1 - \epsilon, \tag{4.17}$$

where $\wp_t$ is denoted as the prediction accuracy of the proposed online conformal predictor at time instant t. It is formulated as

$$\wp_t = \frac{\mid \{i = 1, 2, ..., t-1 : e_i^{\epsilon} = 0\} \mid}{t-1}. \tag{4.18}$$

Based on the above analysis, the validation result of the online conformal predictor at time instant t associated with dynamically updating the trust level $\mathcal{F}$ is designed as

$$\theta_t = \begin{cases} -(1-\epsilon), & \text{if } Y_{L+t}^{\epsilon} = \{0\} \\ 1-\epsilon, & \text{if } Y_{L+t}^{\epsilon} = \{1\} \\ 0, & \text{otherwise} \end{cases} . \tag{4.19}$$

In this equation, $(1-\epsilon)$ represents the confidence in the prediction set $Y_{L+t}^{\epsilon} = \{1\}$, namely that the attribute estimate collected is from Alice at time instant t. By contrast, $-(1-\epsilon)$ quantizes the opposite of the confidence in the prediction set $Y_{L+t}^{\epsilon} = \{0\}$, namely that the collected attribute estimate is deemed to be from the Spoofer at time instant t. The validation result for updating the trust level $\mathcal{F}[t]$ is set as $\theta_t = 0$ in the cases of $Y_{L+t}^{\epsilon} = \{0, 1\}$ and $Y_{L+t}^{\epsilon} = \emptyset$, since the prediction results are invalid for authentication and authorization. It is plausible that if $Y_{L+t}^{\epsilon} = \{0, 1\}$ or $Y_{L+t}^{\epsilon} = \emptyset$, it shifts to other confidence levels, especially to specific confidence levels ϵ for which Y_{L+t}^{ϵ} is a singleton. Although the empirical error rate of the online conformal predictor approaches ϵ in the wireless communication scenarios, the validation result in (4.19) is set according to the confidence concerning the prediction results. This is because the proposed scheme requires multiple-step validation of the transmitter, thus resulting in a robust performance as a benefit of the progressive authorization process.

Then the trust level $\mathcal{F}$ at time instant t can be obtained by Definition 4.1 and (4.6), which is updated as

$$\mathcal{F}[t] = \frac{\rho\mathcal{F}[t-1]+\theta_t}{\rho+1} = \frac{\rho^{t-1}\mathcal{F}[1]+\sum_{i=2}^{t}\rho^{t-i}(\rho+1)^{i-2}\theta_i}{(\rho+1)^{t-1}}, \tag{4.20}$$

where $\rho \in (0,1]$ is the forgetting factor. Note that the forgetting factor should be chosen according to the specific application scenario. Upon using this forgetting factor in the trust management, the closer validation results will have a higher influence on the trust level $\mathcal{F}$. It is observed from (4.20) that $(1-\epsilon) \in [0,1]$, $-(1-\epsilon) \in [-1,0]$, $\mathcal{F}[1] \in [0,1]$, and $\mathcal{F}[t-1] \in [0,1]$. Upon setting $\mathcal{F}[t] \leq 0$ to 0, $\mathcal{F}[t] \in [0,1]$ satisfies. In summary, the developed adaptive trust adjustment procedure conceived for soft authentication and progressive authorization is summarized in Algorithm 3.

Algorithm 3 Online conformal prediction-based adaptive trust adjustment

```
Given initial training set $\{z_1, z_2, ..., z_L\}$ and significance level $\epsilon$;
1. Soft authentication:
1.1 obtain the initial trust level $\mathcal{F}[1]$ via (4.5);
1.2 if $\mathcal{F}[1] \in (\nu_n, \nu_{n+1}]$, $n \in \{1, 2, ..., N-1\}$
1.3     authorize this transmitter with $\Phi_n$ and go to Step 2;
1.4 else
1.5     authenticate this transmitter as the Spoofer and go to Step 3;
1.6 end if
2. Progressive authorization:
2.1 update training set by $\{z_1, z_2, ..., z_L\} + (H_{O1}, y_{L+1}) - z_1$;
2.2 for authentication time instants $t = 2, 3, 4, ...$
2.3     collect new physical layer attribute estimate $H_{Ot}$;
2.4     obtain value $p^{\mathrm{sm}}_{y,L+t}$ and predicted set $Y^{\epsilon}_{L+t}$ via (4.16) and (4.15), respectively;
2.5     obtain validation result $\theta_t$ via (4.19), and then update trust level $\mathcal{F}[t]$ via (4.20);
2.6     if $\mathcal{F}[t] \in (\nu_n, \nu_{n+1}]$, $n \in \{1, 2, ..., N-1\}$
2.7         authorize this transmitter with $\Phi_n$;
2.8     else
2.9         terminate the communication with this transmitter and go to Step 3;
2.10    end if
2.11    update training set as $\{z_t, z_{t+1}, ..., z_{L+t-1}\} + (H_{Ot}, y_{L+t}) - z_t$;
2.12 end for
3. END
```

Remark 4.3. In Algorithm 3, Bob authenticates the transmitter (Alice or the Spoofer) through an adaptive process based on the classification of the physical layer attribute estimates. Once the transmitter is believed to be the Spoofer, i.e., its trust level $\mathcal{F}$ is lower than ν_1, the communication session will be terminated by Bob, otherwise, the proposed scheme will be operated until the end of their communications. This algorithm describes a soft authentication and progressive authorization process, which supports prompt connection and enhanced security for legitimate devices.

4.3.3 Security Performance Analysis

According to Algorithm 3 and the proposed scheme, the following theorems can be formulated:
Theorem 4.1: In the case of $v_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $s_n = r_n, n = 1, 2, ..., N-1$, the individual risk and individual satisfaction of the proposed scheme at time instant t satisfy

$$\wp[t]R_{\text{ind}}[t] = (1 - \wp[t])S_{\text{ind}}[t]. \tag{4.21}$$

Proof: According to Definitions 4.2 and 4.3, and the proposed adaptive trust adjustment approach of (4.20), the individual risk and individual satisfaction at time instant t can be expressed, respectively, as

$$\begin{aligned} R_{\text{ind}}[t] &= \sum_{n=1}^{N-1} r_n \cdot \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-\theta_t}{\rho}, \frac{v_{n+1}(\rho+1)-\theta_t}{\rho}] \mid \Psi_0) \\ &= \sum_{n=1}^{N-1} r_n \cdot \{\Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)+1-\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)+1-\epsilon}{\rho}])\wp[t] \\ &\quad + \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}])(1-\wp[t])\}, \end{aligned} \tag{4.22}$$

and

$$\begin{aligned} S_{\text{ind}}[t] &= \sum_{n=1}^{N-1} s_n \cdot \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-\theta_t}{\rho}, \frac{v_{n+1}(\rho+1)-\theta_t}{\rho}] \mid \Psi_1) \\ &= \sum_{n=1}^{N-1} s_n \cdot \{\Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}])\wp[t] \\ &\quad + \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)+1-\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)+1-\epsilon}{\rho}])(1-\wp[t])\}. \end{aligned} \tag{4.23}$$

Given the condition $v_1 \geq (\rho+\epsilon-1)/(\rho+1)$, the following equation can be obtained

$$\Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)+1-\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)+1-\epsilon}{\rho}]) = 0,$$

since $0 < v_1 < v_2 < \cdots < v_N = 1$ and $(v_n(\rho+1)+1-\epsilon)/\rho \geq 1$. Then the individual risk and individual satisfaction at time instant t can be rewritten as

$$R_{\text{ind}}[t] = (1-\wp[t]) \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \qquad (4.24)$$

and

$$S_{\text{ind}}[t] = \wp[t] \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \qquad (4.25)$$

under the condition of $s_n = r_n$. Therefore, the individual risk and individual satisfaction of the proposed scheme at time instant t satisfy (4.21). □

Theorem 4.2: In the proposed soft authentication and progressive authorization scheme, the individual risk at time instant t satisfies

$$(1-\wp[t])R_{\text{ind}}[t-1] \leq R_{\text{ind}}[t] < 1-\wp[t] \qquad (4.26)$$

under the condition $v_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $v_{N-1} \leq 1-\epsilon$.

Proof: According to Definition 4.2 and the proposed adaptive trust adjustment approach of (4.20) as well as the results of Theorem 4.1, the individual risk at time instant t can be expressed as

$$R_{\text{ind}}[t] = (1-\wp[t]) \sum_{n=1}^{N-1} r_n \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \qquad (4.27)$$

under the conditions $v_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $v_{N-1} \leq 1-\epsilon$. Then the following results can be obtained

$$\frac{v_n(\rho+1)-(1-\epsilon)}{\rho} \leq v_n, \; n = 1, 2, ..., N-1, \qquad (4.28)$$

$$\Pr(\mathcal{F}[t-1] \in (\frac{v_{N-1}(\rho+1)-1+\epsilon}{\rho}, \frac{(\rho+1)-1+\epsilon}{\rho}]) \geq \Pr(\mathcal{F}[t-1] \in (v_{N-1}, 1]). \quad (4.29)$$

Hence, the following result holds

$$R_{\text{ind}}[t] \geq (1 - \wp[t])R_{\text{ind}}[t-1]. \quad (4.30)$$

Furthermore, due to

$$\sum_{n=1}^{N-1} \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \leq 1, \quad (4.31)$$

the following results are obtained

$$(1-\wp[t]) \sum_{n=1}^{N-1} r_n \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) < (1-\wp[t]). \quad (4.32)$$

Hence, the individual risk at time instant t satisfies (4.26) in the proposed scheme. □

Theorem 4.3: In the proposed soft authentication and progressive authorization scheme, the individual satisfaction at time instant t obeys

$$\wp[t]S_{\text{ind}}[t-1] \leq S_{\text{ind}}[t] < \wp[t] \quad (4.33)$$

under the condition $v_1 \geq (\rho + \epsilon - 1)/(\rho + 1)$ and $v_{N-1} \leq 1 - \epsilon$.

Proof: Similar to the proof of Theorem 4.2, given the conditions $v_1 \geq (\rho + \epsilon - 1)/(\rho + 1)$ and $v_{N-1} < 1 - \epsilon$, the individual satisfaction at time instant t is shown in (4.23). Based on the results of (4.25) and (4.29), as well as $0 \leq s_1 < s_2 < \cdots < s_{N-1} \leq 1$, the following result is obtained

$$S_{\text{ind}}[t] \geq \wp[t]S_{\text{ind}}[t-1]. \quad (4.34)$$

Given the result of (4.31), the following inequality is satisfied

$$\wp[t] \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{v_n(\rho+1)-1+\epsilon}{\rho}, \frac{v_{n+1}(\rho+1)-1+\epsilon}{\rho}]) < \wp[t]. \quad (4.35)$$

Hence, the individual satisfaction of the proposed scheme at time instant t satisfies (4.33). □

Corollary 4.1: When t is large enough, the individual risk and individual satisfaction of the proposed scheme at time instant t satisfy

$$(1-\epsilon)R_{\text{ind}}[t] \approx \epsilon S_{\text{ind}}[t], \tag{4.36}$$

under conditions $v_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $s_n = r_n, n = 1, 2, ..., N-1$.

Proof: According to Lemma 4.1, when t is large enough, the empirical prediction accuracy of the online conformal predictor obeys

$$\wp_t \approx 1-\epsilon \tag{4.37}$$

according to (4.17). Hence, the result of Corollary 4.1 can be obtained. □

It can be observed from Theorems 4.1-4.3 that the individual satisfaction and individual risk of the proposed scheme depend both on the dynamic trust level $\mathcal{F}[t]$ as well as on the prediction accuracy $\wp[t]$, which rely on the real-time validation results of the selected time-varying attribute. One can be observed from Theorems 4.2 and 4.3 that the proposed scheme evaluates the physical layer attribute used, thereby promptly adjusting the trust model, so that the individual risk can be dramatically reduced within a short time. Given the specific distribution of the attribute estimates used in the proposed scheme, the closed-form expressions of the $R_{\text{ind}}[t]$ and of the $S_{\text{ind}}[t]$ can be obtained.

Case study: In order to characterize the performance of the proposed scheme, a special case is studied assuming that the specific physical layer attribute of Alice and that of the Spoofer obey the classic Gaussian distribution with means of μ_1 and μ_2 as well as with variances of σ_1^2 and σ_2^2, respectively, and setting $N = 3$ and $\rho = 1$. Then the following results can be obtained:

Corollary 4.2: The closed-form expressions of the individual risk and individual satisfaction of the proposed scheme at time instant $t = 1$ can be formulated, respectively, as

$$R_{\text{ind}}[1] = \frac{r_1}{\sqrt{\pi}}\Big[\int_{\frac{\mu_1-\mu_2+2a(1-v_2)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2+2a(1-v_1)}{\sigma_2\sqrt{2}}} e^{-x^2}\mathrm{d}x + \int_{\frac{\mu_1-\mu_2-2a(1-v_1)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2-2a(1-v_2)}{\sigma_2\sqrt{2}}} e^{-x^2}\mathrm{d}x\Big] + \frac{r_2}{\sqrt{\pi}}\int_{\frac{\mu_1-\mu_2-2a(1-v_2)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2+2a(1-v_2)}{\sigma_2\sqrt{2}}} e^{-x^2}\mathrm{d}x \tag{4.38}$$

and

$$S_{\text{ind}}[1] = s_1[\text{erf}(\frac{\sqrt{2}a(1-v_1)}{\sigma_1}) - \text{erf}(\frac{\sqrt{2}a(1-v_2)}{\sigma_1})] + s_2\text{erf}(\frac{\sqrt{2}a(1-v_2)}{\sigma_1}), \tag{4.39}$$

where erf(·) is the error function.

Proof: In this case study, it is assumed that the attribute observations of Alice and that of Spoofer obey Gaussian distribution with means μ_1 and μ_2 and variances σ_1^2 and σ_2^2, respectively, as well as set $N = 3$ and $\rho = 1$. $\mathcal{F}[1] = |H_A - H_{O1}|/2a$ is formulated, where H_A is the average of $H_{A1}, H_{A2}, ..., H_{AL}$, and $|H_A - H_1|/2a$ normalizes the range of difference ΔH_{O1} in (4.2) to the limited set $[0, 1]$. Then the individual risk and individual satisfaction at time instant $t = 1$ can be given as (4.40) and (4.41), respectively.

$$\begin{aligned}
&R_{\text{ind}}[1] = r_1\Pr(\mathcal{F}[1] \in (v_1, v_2] \mid \Psi_0) + r_2\Pr(\mathcal{F}[1] \in (v_2, 1] \mid \Psi_0)\\
&= r_1\Pr(|H_A - H_{O1}| \in [2a(1-v_2), 2a(1-v_1)) \mid \Psi_0) + r_2\Pr(|H_A - H_{O1}| \in [0, 2a(1-v_2)) \mid \Psi_0)\\
&= \frac{1}{2}r_1[\text{erf}(\frac{H_A + 2a(1-v_1) - \mu_2}{\sigma_2\sqrt{2}}) - \text{erf}(\frac{H_A + 2a(1-v_2) - \mu_2}{\sigma_2\sqrt{2}}) + \text{erf}(\frac{H_A - 2a(1-v_2) - \mu_2}{\sigma_2\sqrt{2}})\\
&-\text{erf}(\frac{H_A - 2a(1-v_1) - \mu_2}{\sigma_2\sqrt{2}})] + \frac{1}{2}r_2[\text{erf}(\frac{H_A + 2a(1-v_2) - \mu_2}{\sigma_2\sqrt{2}}) - \text{erf}(\frac{H_A - 2a(1-v_2) - \mu_2}{\sigma_2\sqrt{2}})]\\
&= \frac{1}{2}r_1[\text{erf}(\frac{\mu_1 - \mu_2 + 2a(1-v_1)}{\sigma_2\sqrt{2}}) - \text{erf}(\frac{\mu_1 - \mu_2 + 2a(1-v_2)}{\sigma_2\sqrt{2}}) + \text{erf}(\frac{\mu_1 - \mu_2 - 2a(1-v_2)}{\sigma_2\sqrt{2}})\\
&-\text{erf}(\frac{\mu_1 - \mu_2 - 2a(1-v_1)}{\sigma_2\sqrt{2}})] + \frac{1}{2}r_2[\text{erf}(\frac{\mu_1 - \mu_2 + 2a(1-v_2)}{\sigma_2\sqrt{2}}) - \text{erf}(\frac{\mu_1 - \mu_2 - 2a(1-v_2)}{\sigma_2\sqrt{2}})].
\end{aligned} \tag{4.40}$$

$$\begin{aligned}
&S_{\text{ind}}[1] = s_1\Pr(\mathcal{F}[1] \in (v_1, v_2] \mid \Psi_1) + s_2\Pr(\mathcal{F}[1] \in (v_2, 1] \mid \Psi_1)\\
&= s_1\Pr(|H_A - H_{O1}| \in [2a(1-v_2), 2a(1-v_1)) \mid \Psi_1) + s_2\Pr(|H_A - H_{O1}| \in [0, 2a(1-v_2)) \mid \Psi_1)\\
&= \frac{1}{2}s_1[\text{erf}(\frac{H_A + 2a(1-v_1) - \mu_1}{\sigma_1\sqrt{2}}) - \text{erf}(\frac{H_A + 2a(1-v_2) - \mu_1}{\sigma_1\sqrt{2}}) + \text{erf}(\frac{H_A - 2a(1-v_2) - \mu_1}{\sigma_1\sqrt{2}})\\
&-\text{erf}(\frac{H_A - 2a(1-v_1) - \mu_1}{\sigma_1\sqrt{2}})] + \frac{1}{2}s_2[\text{erf}(\frac{H_A + 2a(1-v_2) - \mu_1}{\sigma_1\sqrt{2}}) - \text{erf}(\frac{H_A - 2a(1-v_2) - \mu_1}{\sigma_1\sqrt{2}})]\\
&= s_1[\text{erf}(\frac{2a(1-v_1)}{\sigma_1\sqrt{2}}) - \text{erf}(\frac{2a(1-v_2)}{\sigma_1\sqrt{2}})] + s_2\text{erf}(\frac{2a(1-v_2)}{\sigma_1\sqrt{2}}).
\end{aligned} \tag{4.41}$$

Therefore, the closed-forms of individual risk and individual satisfaction of the proposed scheme at time instant $t = 1$ are shown in (4.38) and (4.39), respectively. □

Corollary 4.3: The closed-form expressions of the individual risk and individual satisfaction of the proposed scheme at time instant $t = 2, 3, 4, ...$ can be obtained based on the results of Corollary 4.2, respectively, as

$$\begin{aligned} R_{\text{ind}}[t] &= r_1(1 - \wp[t])\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2v_2 - 1 + \epsilon]) \\ &\quad + r_2(1 - \wp[t])\Pr(\mathcal{F}[t-1] \in (2v_2 - 1 + \epsilon, 1]) \end{aligned} \tag{4.42}$$

and

$$\begin{aligned} S_{\text{ind}}[t] &= s_1\wp[t]\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2v_2 - 1 + \epsilon]) \\ &\quad + s_2\wp[t]\Pr(\mathcal{F}[t-1] \in (2v_2 - 1 + \epsilon, 1]) \end{aligned} \tag{4.43}$$

under condition $v_1 \geq \epsilon/2$.

Proof: In this case study, the individual risk and individual satisfaction at time instant $t = 2, 3, 4, ...$ can be obtained based on the results of Theorems 4.1-4.3 and Corollary 4.2 as

$$\begin{aligned} R_{\text{ind}}[t] &= \sum_{n=1}^{2} r_n \Pr(\frac{\mathcal{F}[t-1] + \theta_t}{2} \in (v_n, v_{n+1}] \mid \Psi_0) \\ &= (1 - \wp[t])r_1\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2v_2 - 1 + \epsilon]) \\ &\quad + (1 - \wp[t])r_2\Pr(\mathcal{F}[t-1] \in (2v_2 - 1 + \epsilon, 1]) \\ &\quad + \wp[t]r_1\Pr(\mathcal{F}[t-1] \in (2v_1 + 1 - \epsilon, 2v_2 + 1 - \epsilon]) \\ &\quad + \wp[t]r_2\Pr(\mathcal{F}[t-1] \in (2v_2 + 1 - \epsilon, 3 - \epsilon]) \end{aligned} \tag{4.44}$$

and

$$\begin{aligned} S_{\text{ind}}[t] &= \sum_{n=1}^{2} s_n \Pr(\frac{\mathcal{F}[t-1] + \theta_t}{2} \in (v_n, v_{n+1}] \mid \Psi_1) \\ &= \wp[t]s_1\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2v_2 - 1 + \epsilon]) \\ &\quad + \wp[t]s_2\Pr(\mathcal{F}[t-1] \in (2v_2 - 1 + \epsilon, 1]) \\ &\quad + (1 - \wp[t])s_1\Pr(\mathcal{F}[t-1] \in (2v_1 + 1 - \epsilon, 2v_2 + 1 - \epsilon]) \\ &\quad + (1 - \wp[t])s_2\Pr(\mathcal{F}[t-1] \in (2v_2 + 1 - \epsilon, 3 - \epsilon]). \end{aligned} \tag{4.45}$$

According to the derived $R_{\text{ind}}[1]$ and $S_{\text{ind}}[1]$ in (4.40) and (4.41), respectively, the individual risk and individual satisfaction of the proposed scheme at time instant $t = 2, 3, 4, ...$ are given as (4.42) and (4.43), respectively, under condition $v_1 \geq \epsilon/2$. $\square$

Corollary 4.4: Based on the results of Corollaries 4.2 and 4.3, the solution of the following problem does exist.

$$\begin{aligned}(v_1, v_2) &= \arg\max S_{\text{ind}}[t], \\ \text{s.t. } R_{\text{ind}}[t] &\leq \delta, 0 < v_1 < v_2 < 1,\end{aligned} \tag{4.46}$$

where δ denotes maximum tolerate individual risk invoked for controlling the risk in the proposed soft authentication and progressive authorization process.

Proof: Given the problem of (4.46), maximum $S_{\text{ind}}[t]$ can only be achieved when $R_{\text{ind}}[t] = \delta$, since there is a trade-off between the individual risk and individual satisfaction associated with the thresholds v_1, v_2. Hence, the following results can be obtained as

$$\begin{aligned}&(1 - \wp[t])r_1\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2v_2 - 1 + \epsilon]) \\ &\quad +(1 - \wp[t])r_2\Pr(\mathcal{F}[t-1] \in (2v_2 - 1 + \epsilon, 1]) = \delta \\ &\Rightarrow v_2 = g(v_1),\end{aligned} \tag{4.47}$$

where $g(\cdot)$ is the function of v_2 in terms of v_1. Then the problem of (4.46) can be rewritten as

$$\begin{aligned}v_1 &= \arg\max\{\wp[t]s_1\Pr(\mathcal{F}[t-1] \in (2v_1 - 1 + \epsilon, 2g(v_1) \\ &\quad -1 + \epsilon]) + \wp[t]s_2\Pr(\mathcal{F}[t-1] \in (2g(v_1) - 1 + \epsilon, 1])\}.\end{aligned} \tag{4.48}$$

Therefore, the solution of problem (4.46) does indeed exist because the righthand side of (4.48) is a continuous function in terms of v_1 based on the closed-form expression of individual satisfaction of (4.43). $\square$

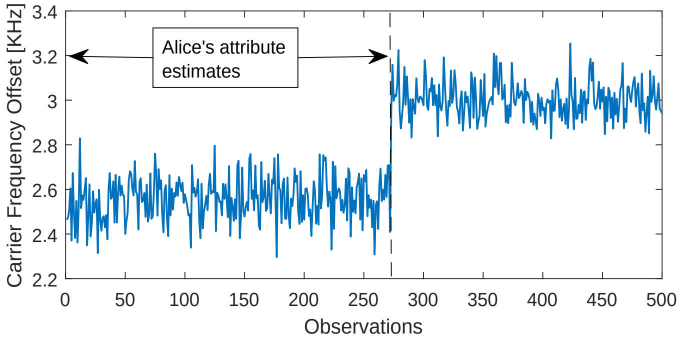
Remark 4.4. Corollaries 4.2 and 4.3 give the closed-form expressions of the individual risk and individual satisfaction in the soft authentication phase (i.e., $t = 1$) and in the following phases (namely $t = 2, 3, 4, ...$), respectively. It is observed from Corollary 4.2 that the required soft security is achieved by setting multiple authorization levels, thus the risk of a misdetection can be carefully controlled by configuring this device for a low authorization level.

Remark 4.5. As it can be observed from above Theorems and Corollaries that the individual risk and individual satisfaction depend on the thresholds $\nu_1, \nu_2, ..., \nu_{N-1}$. Most of the conventional physical layer authentication techniques determine the threshold of the authentication system based on the Neyman-Pearson criterion [2, 25, 37], which minimizes the misdetection rate subject to a maximum tolerable constraint on the false alarm rate. However, these schemes constitute binary authentication solutions, which are unsuitable for achieving the soft authentication and progressive authorization. More importantly, for a communication system, the thresholds can be flexibly determined to meet the requirement of security.

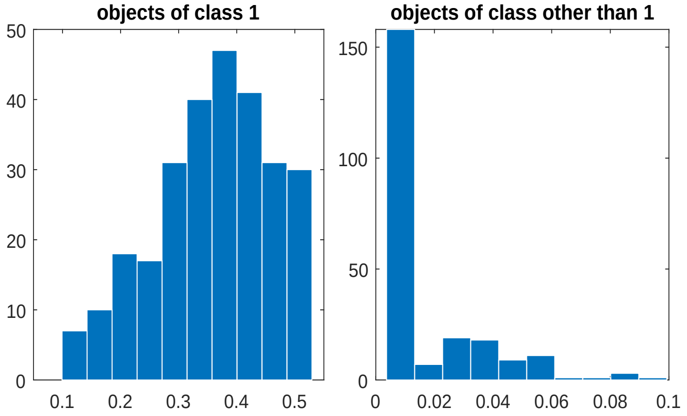
4.4 Simulation Results

In order to evaluate the performance of the proposed soft authentication and progressive authorization scheme, simulation results are provided in this section by utilizing both carrier frequency offset (CFO) and received signal strength indicator (RSSI). Firstly, the training process and results characterizing the proposed online conformal predictor are presented. Then the performance of the proposed soft authentication solution is characterized by studying the trade-off between individual satisfaction level vs. individual risk level during the soft authentication stage. A scenario is studied for characterizing the security performance and robustness of the proposed progressive authorization solution, where a misdetection event occurs during the soft authentication stage or the Spoofer imitates Alice after the soft authentication. Compared to the static binary authentication scheme and the kernel learning-based authentication scheme of [2], the superiority of the proposed scheme is highlighted.

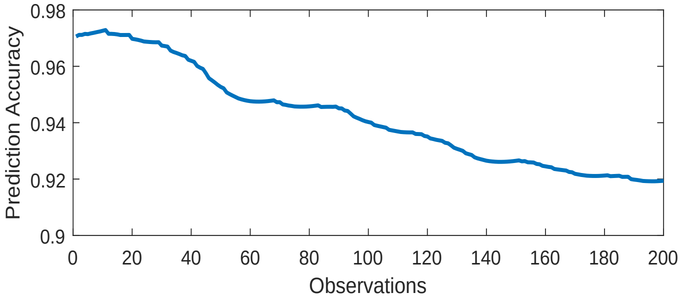
In order to achieve soft authentication and progressive authorization, both the CFO [37] and RSSI [117] are utilized for the validation of the proposed scheme. The observations of the CFO seen in Figure 4.2 (a) and those of the RSSI seen in Figure 4.3 (a) used for training and testing are collected from the implementation-oriented contributions of [37] and [117], respectively. In a little more detail, the authors of [37] built a software-defined radio platform based on the Universal Software Radio Peripheral to capture the real CFO data. The system implemented



(a) CFO observations of Alice for training, and CFO observations of both Alice and the Spoofer for testing in the proposed scheme.



(b) p-value for case $y = 1$, i.e., the CFO estimate is from Alice.



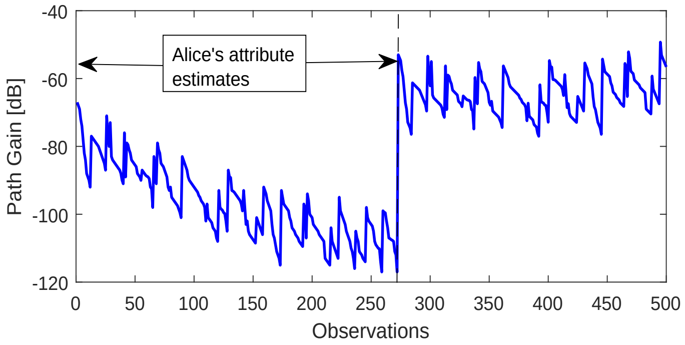
(c) Accuracy of the proposed online conformal predictor by utilizing CFO observations.

Figure 4.2: Performance of the proposed online conformal predictor relying on CFO.

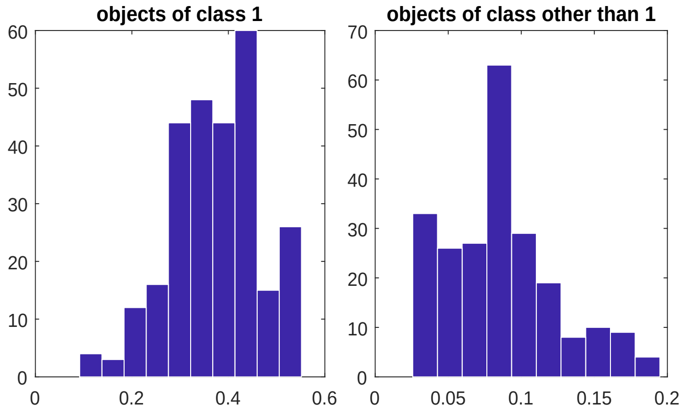
comprises two transmitters (i.e., Alice and the Spoofer) and one receiver (Bob) operating at a carrier frequency of 2.47 GHz. Furthermore, the authors of [117] collected data throughout three different measurement campaigns, seven days combined and spread across two summer seasons. The measurements were carried out in an approximate range of 0-100 m at points which were approximately 10 m apart from each other at 9 different parts of the orchard described in [117] along five directions, namely along, across, 30°, 45°, and 60° with respect to the tree rows. As shown in Figure 4.1 and the system model, the Spoofer can be viewed as the second transmitter, who is located in a third location (i.e., more than a wave-length away from Alice) and tries to imitate Alice for gleaning illegal advantages from Bob. Hence, the CFO and RSSI estimates of the Spoofer are also collected for testing in the simulation.

Given the initial training set $\{z_1, z_2, ..., z_L\}$, $L = 40$, and the significance level of $\epsilon = 0.1$, the proposed online conformal predictor is trained and tested by utilizing the collected observations of the CFO. Note that only Alice's CFO observations are used for training, i.e., the first 40 samples in Figure 4.2 (a), and the CFO observations of both Alice and the Spoofer are utilized for testing the prediction accuracy of the proposed scheme based on the online conformal predictor. The distribution of the smoothened p-values recorded for $y = 1$ (i.e., the CFO observations are from Alice) is given in Figure 4.2 (b), which is used to form the predicted set of (4.15). To be more specific, the x-axis represents the p-values, while the y-axis is the number of CFO observations. When the p-value is below the significance level ϵ, the class (either 0 or 1) will be removed from the predicted set Y_t^ϵ. Then a confidence level of 0.9 is obtained concerning the predicted set. More importantly, Figure 4.2 (c) characterizes the prediction accuracy of the proposed online conformal predictor relying on new CFO observations, i.e., $\wp_t$. It can be observed from Figure 4.2 (c) that the prediction accuracy values concerning new CFO observations are all higher than 0.9. The reason for this trend is that the proposed conformal predictor keeps the error rate below the significance level ϵ.

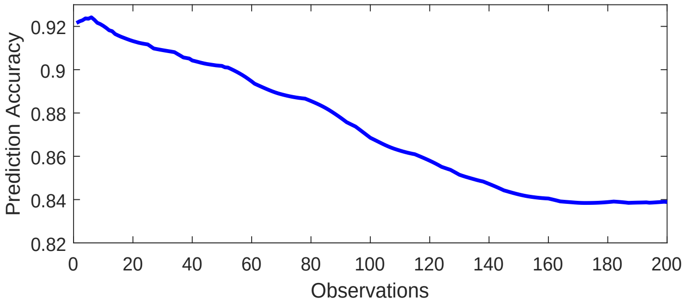
Similarly, only Alice's RSSI observations are used for training, i.e., the first 40 samples in Figure 4.3 (a), and the RSSI observations of both Alice and the Spoofer are utilized for testing in the online conformal predictor. Figure 4.3 (b) and (c) characterize the online conformal prediction results relying on the RSSI observations by setting the significance level of $\epsilon = 0.2$, where (b) presents the p-values for the class of $y = 1$, and (c) demonstrates the prediction



(a) RSSI observations of Alice for training, and RSSI observations of both Alice and the Spoofer for testing in the proposed scheme.



(b) p-value for case $y = 1$, i.e., the RSSI estimate is from Alice.



(c) Accuracy of the proposed online conformal predictor by utilizing RSSI observations.

Figure 4.3: Performance of the proposed online conformal predictor relying on RSSI.

accuracy of the proposed scheme concerning new RSSI observations. It is observed from Figure 4.3 (c) that the prediction accuracy concerning new observations is higher than 0.8.

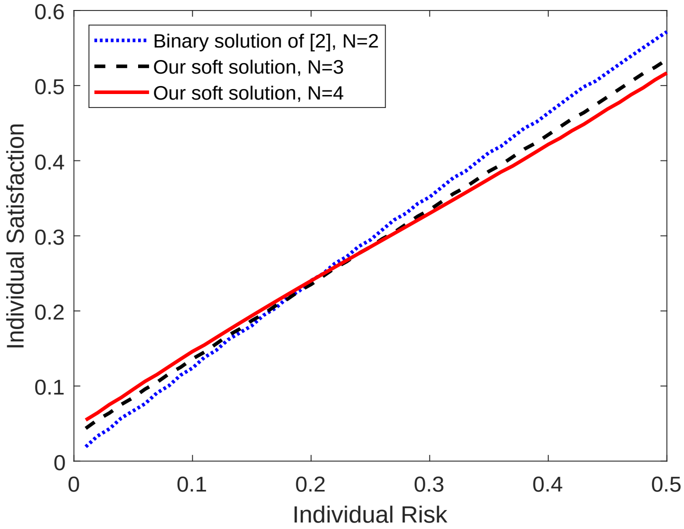


Figure 4.4: Individual satisfaction vs. threshold of individual risk for the numbers of authorization levels $N = 2$, $N = 3$, and $N = 4$ based on the results of Figure 4.2.

Figure 4.4 characterizes the individual satisfaction vs. the individual risk with respect to the number of authorization levels of $N = 2$, $N = 3$, and $N = 4$ by utilizing CFO of Figure 4.2. It can be observed from Figure 4.4 that upon increasing the individual risk threshold, namely δ, the individual satisfaction values increase in all cases. The reason for this trend is that there is a trade-off between the individual risk and individual satisfaction as demonstrated by the analytical results of subsection 4.3. Furthermore, when the threshold of the individual risk is lower than 0.2, the individual satisfaction value of the scenario associated with $N = 4$ is the highest, while that of $N = 2$ is the lowest. It is because using multiple authorization levels in the proposed scheme helps to access services/resources quickly when the threshold of individual risk is low, i.e., the security requirement is high.

Then the scenario when a misdetection event occurs during the soft authentication stage or when the Spoofer attacks Alice after the soft authentication stage is studied. In Figure 4.5, the performance of the proposed progressive authorization scheme is characterized by utilizing the CFO (see Figure 4.2) with respect to the forgetting factors of $\rho = 0.8$, $\rho = 0.6$ and $\rho = 0.4$ compared to that of the static binary authentication scheme. In this figure, the number of authorization levels is set to $N = 3$ in the proposed scheme, while the classification of the services/resources is given by Φ_0, Φ_1, and Φ_2. It can be observed from Figure 4.5 that the individual risk values of the proposed scheme decrease in all cases upon increasing the number of observations (i.e., the estimates of CFO) of the transmitter. The reason for this trend is that if Bob observes that the CFO is in nonconformity with the training samples of Alice, the trustworthiness of this transmitter will be decreased. Thereafter the authorization level will be reduced to Φ_0 within a short time. However, in the static binary authentication scheme, the individual risk value will not be decreased, leading to substantial losses in this scenario. This demonstrates that the static binary authentication scheme fails to deal with the scenario, when a misdetection occurs during the soft authentication phase or the Spoofer attacks the authorized device after the soft authentication stage. It also demonstrates the superiority of the proposed scheme after soft authentication by providing additional protection. Additionally, it can be observed from Figure 4.5 that the individual risk of the proposed scheme associated with the forgetting factor of $\rho = 0.8$ is higher than that of $\rho = 0.6$ and $\rho = 0.4$. The risk level associated with $\rho = 0.4$ is the lowest in these three cases. This is because the historical observations of Alice's CFO have more substantial effects on the adaptive trust adjustment system in the case $\rho = 0.8$, so that the trust level $\mathcal{F}$ is reduced slower than that of the forgetting factors of $\rho = 0.6$ and $\rho = 0.4$.

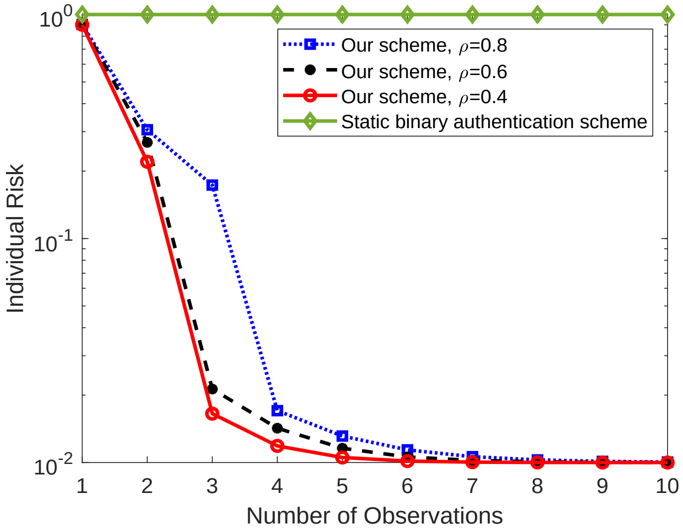


Figure 4.5: Performance of the proposed progressive authorization solution for different forgetting factors benchmarked against the static binary authentication scheme.

In Figure 4.6, the security performance of the proposed scheme for $N = 3$, $N = 4$ and

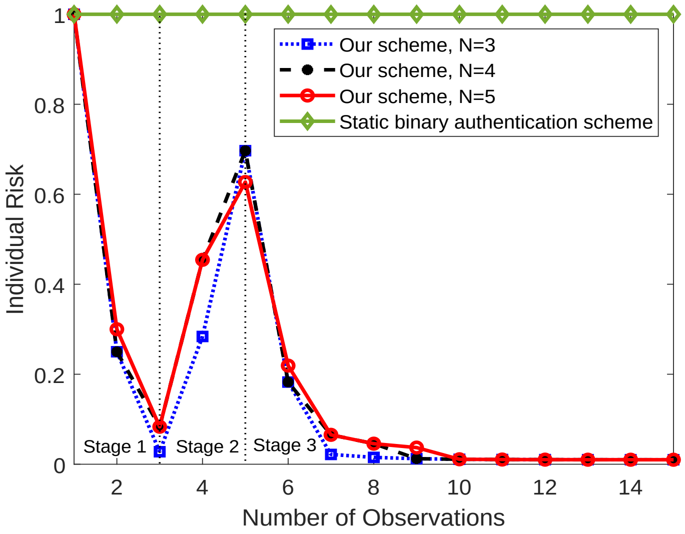


Figure 4.6: Security performance and robustness of the proposed progressive authorization solution parameterized by different numbers of authorization levels.

$N = 5$ authorization levels is characterized to show the effects of N on the proposed scheme in the scenario that a misdetection event occurs in the soft authentication stage or the Spoofer attacks the authorized device after the soft authentication stage. Some transient observations (from 3 to 5 observations) are added to show the robustness of the proposed scheme, which represent the prediction errors in the proposed online conformal predictor, and are mainly caused by the imperfect estimates and variations of the CFO, noisy observations, as well as owing to the dynamic behaviors of the Spoofer. It can be observed from Figure 4.6 that the individual risk value of the proposed scheme recorded for $N = 3$ decreases quicker than in the other cases in Stage 1. The reason is that when the CFO estimates are identified by Bob to be from the Spoofer, the authorization of the transmitter in the $N = 3$ scenario will be reduced to the lowest level more quickly. By contrast, the case of $N = 5$ needs more time (observations) to achieve a low individual risk. Furthermore, the performance of the proposed scheme recorded for $N = 3$ suffers from the lowest robustness, although the individual risk level of this scenario decreases more quickly than in the other cases in Stage 1. To be specific, the risk level of $N = 3$ decays fastest in Stage 1 (before 3 observations), while it increases fastest in Stage 2 (from 3 to 5 observations). In Stage 3, it decreases fastest in all cases. This indicates that the proposed scheme having a lower number of authorization levels is less robust, but it achieves a reduced individual risk more quickly in the scenario that a misdetection event occurs in the soft authentication stage or the Spoofer attacks Alice after the soft authentication stage.

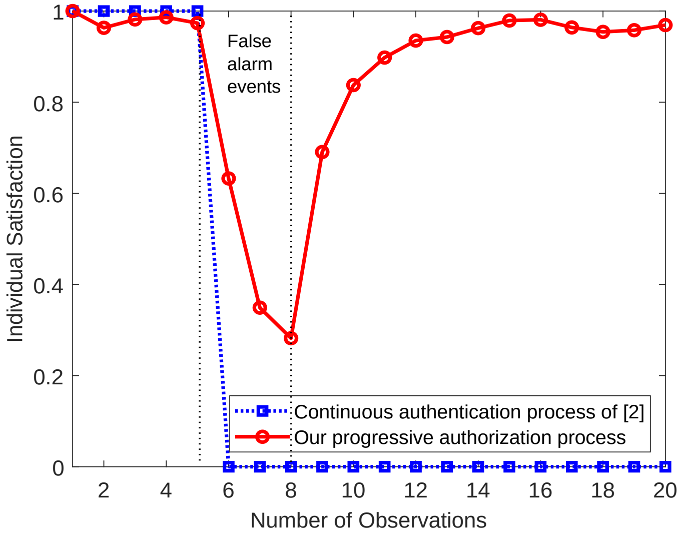


Figure 4.7: Individual satisfaction comparison results of the proposed scheme and the scheme of [2] in the scenario that false alarms happen during the authentication process.

Figure 4.7 characterizes the individual satisfaction comparison results of the proposed progressive authorization process and the kernel learning-based physical layer authentication process of [2]. In this figure, a scenario that false alarm events occur during the authentication process is studied because of the imperfect estimates and variations of the CFO, as seen from 6 to 8 observations. It is observed from Figure 4.7 that the individual satisfaction level of the proposed scheme is a bit lower than that of the physical layer authentication process of [2] for less than 6 CFO observations. This is because of the specific nature of the trust management approach used in the proposed scheme, where the individual satisfaction level depends on the trust level between Alice and Bob. However, once a false alarm event occurs during the authentication process, the individual satisfaction value of the authentication process of [2] tends to 0, because the communication session between Alice and Bob is terminated by Bob. By contrast, the proposed progressive authorization scheme exhibits its robustness in term of tolerating a few false alarms. In conclusion, both Figure 4.4 and Figure 4.7 demonstrate that the proposed soft authentication and progressive authorization scheme performs better than the kernel learning-based authentication scheme of [2] when the threshold of individual risk is low or when false alarm events occur during the authentication process, hence resulting in a faster access and higher robustness.

4.5 Chapter Summary

In this chapter, a soft authentication and progressive authorization scheme based on the trust management was proposed to achieve security enhancement by evaluating the physical layer attribute estimates. A trust model was firstly designed for evaluating the trustworthiness of the relationship between transmitter and receiver, and for supporting a multiple-level authorization. Then a conformal predictor was developed for classifying the estimates of the physical layer attribute selected, which are used for characterizing the trustworthiness of the transmitter. An adaptive algorithm based on online machine learning was developed to update the trust management in real time. The simulation results characterized the benefits of the proposed scheme, demonstrating its superiority over the static binary authentication scheme and the exiting physical layer authentication scheme benchmarker.

In next chapter, the security, trust, and privacy will be comprehensively designed for the blockchain-enabled IoT systems. To be more specific, a distributed access control scheme will be proposed by jointly considering security and privacy-preservation to secure the access of devices and to protect the private information stored in the blockchain. The trust management will be designed to achieve multiple-level authorization and accountable security services for all nodes in the consortium blockchain-enabled IoT systems.

Chapter 5

Accountable Distributed Access Control with Privacy Preservation

While being able to avoid the risk of single point failure, decentralized security provisioning (e.g., access control and authentication) is facing new challenges of increased system complexity, lacking a sense of responsibility, and privacy preservation. To circumvent these impediments, a distributed access control scheme using consortium blockchain is proposed for the Internet of Things (IoT) systems. In achieving overall system efficiency and privacy preservation, the proposed framework has three key components, i.e., a distributed recommendation mechanism, an anonymous credential generation strategy, and a reputation update scheme for accountability. In the proposed recommendation mechanism, multiple authorized nodes are utilized as referrers to efficiently confer their trust on a new public entity. The authentication can be conducted by the referrers in a distributed behavior to issue the required credential for the new entity to join in the system, and an anonymous credential generation strategy is developed for the new entity to further protect its privacy from linking attacks. A reputation update strategy is proposed based on the new entity's behaviors after its joining in the system, and a false recommendation will reduce the referrers' reputation values. The accountability of the referrers can be achieved by lessening its significance in the new authentications and by adaptively adjusting its authorization based on the proposed dynamic multiple-level authorization strategy. The results show that the proposed scheme significantly improves security performance and provides privacy preservation for IoT systems.

5.1 Introduction

IoT systems have attracted a multitude of interests from research and industrial communities due to their ongoing convergence with vertical industry applications [4, 151]. The growing complexity of IoT systems as well as dramatically increased use of intelligent machines and devices within industry processes bring many security vulnerabilities in IoT systems, such as data injection, spoofing, privacy leakage, and so on [14, 194]. Access control techniques protect against unauthorized use of network resources, and also ensure that only the authorized persons or devices can access the network resources, services, data, and information flows. However, most state-of-the-art IoT systems are heavily centralized relying on third parties, which are facing a lot of challenges, such as security, privacy, and trust risks when the third parties are compromised, as well as the lacks of data accountability and traceability, especially in the decentralized industry applications [14]. Hence, distributed access control with security enhancement, privacy protection, and reputation management for defending against both outside and inside attacks is extremely helpful in securing the IoT systems.

Blockchain is a growing list of blocks that record transaction data based on distributed consensus mechanisms [152]. Given its advantages including decentralized nature, traceability, coordinability, and robustness to data tampering, the integration of blockchain technology and IoT infrastructures has been widely studied in [152, 153, 154, 8, 155, 156, 157, 158]. It not only decentralizes the management and operation of IoT systems, but also brings many potential benefits, such as higher adaptability of heterogeneous IoT, higher fault tolerance. Different from the private blockchain [152] and public blockchain [155, 156], a consortium blockchain is controlled by several authorized nodes from multiple organizations, as exemplified by Hyperledger [154, 8], Quorum [153], and Corda [153]. Compared with a public blockchain, the consortium blockchain is more scalable and acceptable among IoT applications due to its much higher system interaction efficiency [153]. Such integration systems can be applied in different areas, for example, smart building and smart industry, and can also achieve the collaborations among different networks as exemplified by information sharing among these networks relying on different gateways or clusters.

5.1.1 Security Weaknesses and Motivations

In a consortium blockchain-enabled IoT system, several authorized nodes will decide who can be part of the system, who can transact, mine, and deploy smart contracts, as well as whether read or write permissions would be public or limited to selected authorized nodes. They have common goals but do not fully trust each other. More importantly, such integration systems are facing some critical security threats from both outside and inside of the system, which limits its deployment in distributed IoT applications. To be specific, the adversaries may imitate or forge the identities of legitimate users to bypass the authentication, then try to obtain illegal benefits from the system. Moreover, the insider attacks are more challenging because they are caused by the misbehaved authorized nodes, e.g., false data injection attacks [159] and denial of service attacks [160]. The private information of authorized nodes may also be leaked to the attackers by linking the IoT data stored in blocks to their real identities. Hence, all the nodes should be authenticated and authorized before they access and transact in the consortium blockchain-enabled IoT system [154].

The access control methods have been studied in [50, 51, 52, 53, 54, 147, 148, 149]. However, most of the existing access control methods are centralized and rely on the trusted third parties or managers, binary in nature and static in time, where nodes either pass the security check or fail by a one-time verification. Once the trusted third parties or static protocols are cracked, the IoT data stored in blocks will be revealed to adversaries. Hence, a dynamic multiple-level authorization is necessary to provide the soft and accountable security service for protecting the consortium blockchain-enabled IoT system, which aims at ensuring that malicious behaviors are able to be identified and punished [161]. More importantly, in the existing consortium blockchain-enable IoT systems, a trusted membership service provider is required to maintain the identities for all nodes, and the credential authorities take responsibility to issue credentials for authentication and authorization, such as [154, 162, 163]. Such a centralized mechanism goes against the partially distributed property of the consortium blockchain.

In a nutshell, the concept of distributed access control with privacy preservation and accountable security service is exceedingly helpful in the consortium blockchain-enabled IoT system. However, such a scheme is facing the following challenges for the IoT systems, i.e.,

P1. How to achieve a reliable and secure access control, so that the integration system can be protected from outside attacks?

P2. How to achieve the privacy preservation for IoT entity as well as IoT data for each authorized node in the system?

P3. How to respond to the incorrect recommendations and authentications to provide accountable security service?

5.1.2 Technical Contributions

In this chapter, a novel distributed access control scheme is proposed based on the consortium blockchain for IoT systems. First, a recommendation mechanism is developed, where several authorized nodes act as referrers to provide recommendations for a public node and to a issue credential to it for further authentication and authorization, which provides a solution for **P1**. To address **P2**, an anonymous credential generation strategy is proposed, so that the private information of each new authorized node stored in the blockchain will not be directly linked to its real identity. Finally, a reputation update strategy is proposed to achieve accountable security service through decreasing the referrers' reputation values if they provide wrong recommendations, as well as lowering their authorization levels based on the proposed dynamic multiple-level authorization strategy, thus **P3** is solved.

The contributions of this chapter are summarized as follows:

- A recommendation mechanism is proposed for distributed access control relying on multiple referrers to protect the IoT data from outside attacks. The trade-off between false alarm and misdetection of the proposed scheme can be improved by using more referrers based on the proposed scheme;

- The privacy of each authorized node is further protected from the linking attacks by generating anonymous credentials. Through both the recommendation mechanism and anonymous credential generation strategy, the private information of authorized nodes in the integration system can be protected from both the outside and inside nodes;

- The developed reputation update strategy provides a method for evaluating the behaviors of authorized nodes and for dynamic multiple-level authorization. Moreover, the accountable security services can be achieved by the proposed scheme through decreasing the reputation values of referrers if they provide wrong recommendations.

Table 5.1: Notations of Chapter 5

Notations	Definitions
N	Number of authorized nodes who control the blockchain.
K	Number of authorization levels.
Ψ_0	The case that the transmitter is an adversary.
Ψ_1	The case that the transmitter is a legitimate node.
$\nu_1, ..., \nu_{K-1}$	Thresholds of the multi-level authorization.
M	Number of referrers.
R_n	Reputation value of n-th authorized node.
S	Average recommendation score.
S_m	Recommendation score of m-th referrer.
P_{FA}	False alarm rate.
P_{MD}	Misdetection rate.

The rest of this chapter is organized as follows. In Section 5.2, the system model used and the key requirements of this chapter are presented. In Section 5.3, the distributed access control scheme is proposed, and the performance analysis is presented. The simulations and numerical results are shown in Section 5.4. Finally, Section 5.5 concludes this chapter.

Notations: In this chapter, scalars are denoted by italic letters, while vectors are respectively denoted by bold-face letters. Table 5.1 shows the notations of this chapter.

5.2 System Model

The framework of a consortium blockchain-enabled IoT system is shown in Figure 5.1. Each block in the blockchain contains the hash of the previous block (previous hash), transaction data, an arbitrary nonce, a timestamp, and hash of the current block (current hash). In this integration system, all communications go through the blockchain, and N authorized entities are acting as end-points in the blockchain network. Each authorized node is designed to hold one copy of the blockchain and is capable of voting on each transaction prior to appending it to the blockchain. There are also some public nodes in this IoT system, who want to join in the consortium blockchain system for the data access. This work considers the system having no centralized service provider, credential authority, and manager, corresponding to the properties of consortium blockchain but increases the grade of challenge imposed on the legitimate users as well. The Practical Byzantine Fault Tolerance (PBFT) algorithm [154] is applied in this integration system.

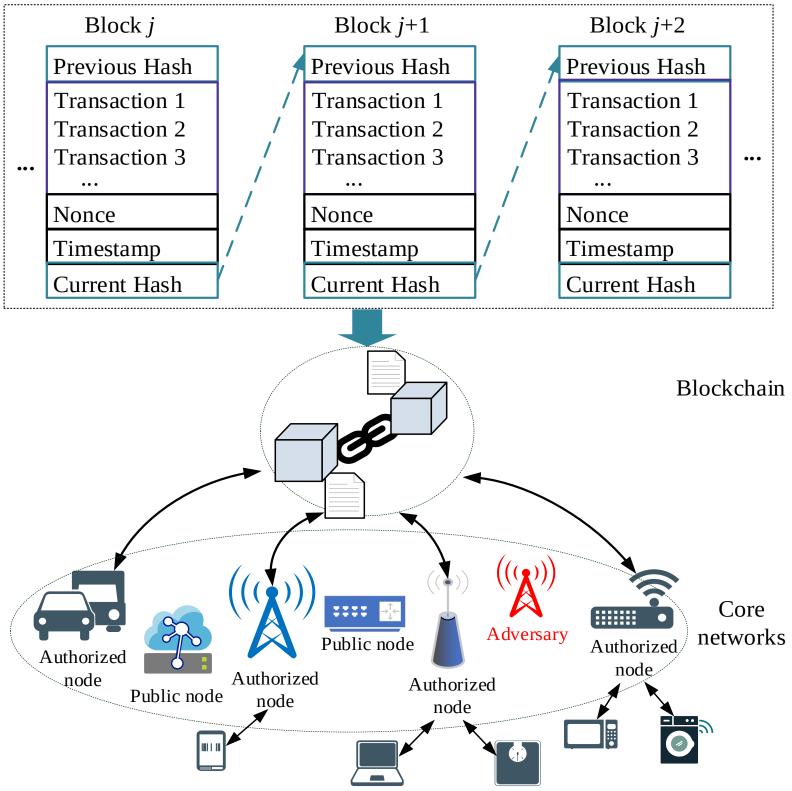


Figure 5.1: Framework of a consortium blockchain-enabled IoT system.

In this integration system, the adversary aims at accessing and obtaining illegal benefits from the system. Although the N authorized nodes have a common goal, they do not fully trust each other, and some of them may attack/cheat for illegal benefits. Furthermore, the public nodes and authorized nodes may try to observe private information of other authorized nodes from the IoT data stored in blocks. To improve the security performance and protect privacy, this chapter focuses on proposing a new distributed access control scheme for the consortium blockchain-enabled IoT system to meet the following requirements:

– *Authentication:* Public nodes should be authenticated before their access to the integration system with the help of authorized nodes in a distributed way, so that the system will be protected from the outside attackers.

– *Authorization:* Every node in the integration system should be authorized what it can do, as exemplified by transacting and deployment of smart contracts. Moreover, the dynamic multiple-level authorization is required to provide soft and progressive security service for protecting system.

– *Privacy Preservation:* The IoT data and the privacy of authorized nodes stored in blocks should be protected from both public nodes and other authorized nodes. In other words, the public nodes cannot gain any knowledge of the transactions in the system, and transactions stored in blocks are anonymous;

– *Accountability:* Authorized nodes in the IoT system should be accountable for their behaviors, especially for the adversarial behaviors. It means that malicious behaviors are able to be identified and punished in the integration system.

5.3 Proposed Distributed Access Control Scheme

In this section, a recommendation mechanism is firstly developed that several authorized nodes should act as referrers to authenticate a public node before its access to the consortium blockchain-enabled IoT system, so that **P1** will be addressed. These referrers will then issue the initial credential together to the new authenticated node based on an anonymous credential generation strategy, so that the IoT data stored in blocks will not be linked to the real identities of devices, thus **P2** will be solved. Then, a reputation update strategy is developed for adaptively updating the reputation values of authorized nodes based on their interactions with other nodes and recommendations, so that the dynamic multiple-level authorization is achieved according to their reputation values. This strategy provides a solution for **P3**, since an incorrect recommendation will lead to punishments on the referrers by decreasing their reputation values.

5.3.1 Recommendation for Distributed Access Control

As shown in Figure 5.2, if a public node, i.e., Alice or Adversary, wants to access/join in the consortium blockchain-enabled IoT system, M referrers in the set of N authorized nodes are incentivized to provide their recommendations for this node. The recommendation score of

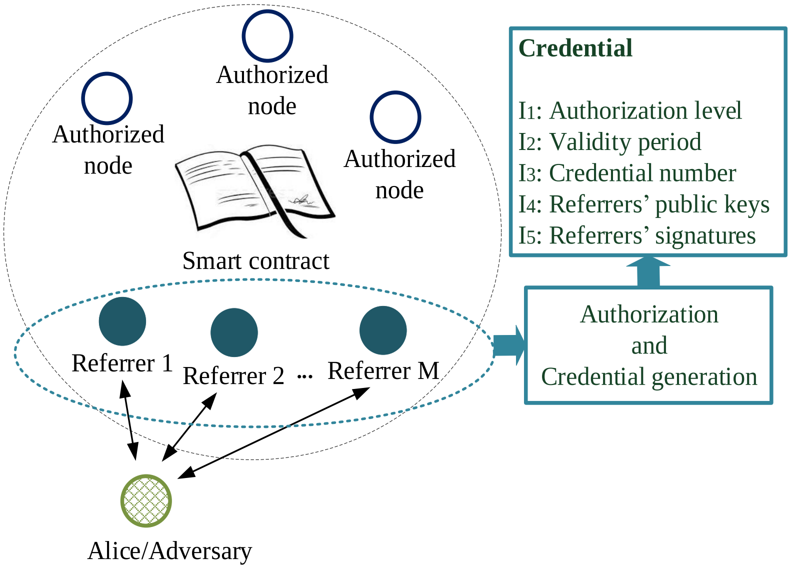


Figure 5.2: The proposed recommendation mechanism for distributed access control.

m-th referrer on new public node is denoted as S_m, which depends on the familiarity degree of referrer m on this public node and satisfies $S_m \in [-1, 1]$. If the value of S_m is high, the referrer m is familiar with this public node and its recommendation is Alice, while $S_m = 0$ represents that referrer m has no knowledge of this public node. Moreover, if the value of S_m is low and less than 0, it means that the referrer m is familiar with this public node and its recommendation is Adversary. Then the average recommendation score of referrers on this public node is formulated as

$$S = \frac{\sum_{m=1}^{M} S_m R_m}{M}, \tag{5.1}$$

where $R_m \in [0, 1]$ is the reputation value of referrer m representing the global perception of its trustworthiness in the system. The recommendations of the referrers and reputation values of all authorized nodes are stored in the blockchain as transactions. It is observed from (5.1) that a referrer having higher reputation value has higher significance on the recommendation for the public nodes.

K authorization levels are set by dividing the services/resources of the integration system into K sets, denoted as $\Phi_0, \Phi_1, ..., \Phi_{K-1}$, in the system according to their importance. Φ_0 represents the service set with lowest authorization level, which means the node is not allowed to access any services/resources of the system, while Φ_{K-1} is denoted as the service set with highest authorization level, with which the nodes can access all services/resources in the system. Therefore, $\emptyset = \Phi_0 \subset \Phi_1 \subset \cdots \subset \Phi_{K-1}$ satisfies, where $\emptyset$ represents null set. Then, the distributed access control is formulated as

$$\begin{cases} \Phi_0: & S \in (-\infty, \nu_1] \\ \Phi_1: & S \in (\nu_1, \nu_2] \\ & \vdots \\ \Phi_{K-1}: & S \in (\nu_{K-1}, \infty) \end{cases}, \tag{5.2}$$

where $\nu_1 < \nu_2 < \cdots < \nu_{K-1}$,

$$\begin{cases} S \in (-\infty, \nu_1] & \Psi_0 \\ S \in (\nu_1, \infty) & \Psi_1 \end{cases}, \tag{5.3}$$

and

$$S = G(\cdot)\mid_{t_0}. \tag{5.4}$$

Ψ_1 indicates that the public node is a legitimate node, while Ψ_0 represents that it is an adversary. t_0 represents the initial authentication time instant.

According to the proposed recommendation mechanism of (5.1) and (5.2), the false alarm rate and misdetection rate of the distributed access control can be calculated, respectively, as

$$P_{\text{FA}} = \Pr(S \leq \nu_1 | \Psi_1) = \Pr(\sum_{m=1}^{M} S_m R_m \leq M\nu_1 | \Psi_1) \tag{5.5}$$

and

$$P_{\text{MD}} = \Pr(S > \nu_1 | \Psi_0) = \Pr(\sum_{m=1}^{M} S_m R_m > M\nu_1 | \Psi_0). \tag{5.6}$$

The recommendation score S_m is assumed to be Gaussian variable in $[-1, 1]$, where its probability distribution functions (PDF) of Ψ_1 and Ψ_0 are formulated, respectively, as

$$f_{\Psi_1}(x) = \frac{1}{\sqrt{2\pi}\sigma_1} \exp(-\frac{(x-\mu_1)^2}{2\sigma_1^2}) \tag{5.7}$$

and

$$f_{\Psi_0}(x) = \frac{1}{\sqrt{2\pi}\sigma_0} \exp(-\frac{(x-\mu_0)^2}{2\sigma_0^2}), \tag{5.8}$$

where $\mu_0 < 0 < \mu_1$ holds. Hence, the average recommendation score S is also a Gaussian variable. Then, the false alarm rate and misdetection rate of (5.5) and (5.6) can be derived, respectively, as

$$P_{\text{FA}} = \int_{-M}^{M\nu_1} \frac{1}{\sqrt{2\pi \sum_{m=1}^{M} R_m^2}\sigma_1} \exp(-\frac{(x-\mu_1 \sum_{m=1}^{M} R_m)^2}{2\sigma_1^2 \sum_{m=1}^{M} R_m^2})dx \tag{5.9}$$

and

$$P_{\text{MD}} = \int_{M\nu_1}^{M} \frac{1}{\sqrt{2\pi \sum_{m=1}^{M} R_m^2}\sigma_0} \exp(-\frac{(x-\mu_0 \sum_{m=1}^{M} R_m)^2}{2\sigma_0^2 \sum_{m=1}^{M} R_m^2})dx. \tag{5.10}$$

Then, the security performance of the proposed scheme depends on both the number of referrers M and threshold ν_1. According to (5.9) and (5.10), there is a trade-off between false alarm and misdetection relying on the threshold ν_1. Therefore, the optimization problem of the access control is designed as

$$\min_{M,\nu_1} P_{MD} \tag{5.11}$$
$$\text{s.t. } P_{FA} \leq \delta,\ M \leq M_{\max},\ \text{and } \nu_1 > 0,$$

where δ represents the threshold of false alarm rate, and $M_{\max}$ is the threshold of referrer number, which is set to control the time latency and communication overhead of the proposed scheme. This optimization problem can be evaluated based on the Neyman-Pearson criterion [23]. It is concluded that P_{MD} achieves the minimum value while P_{FA} meets equality constraint δ. Thresholds $\nu_2, \cdots, \nu_{K-1}$ are determined by the users depending on the historical knowledge of

Algorithm 4 Distributed access control

```
1. Initialization:
   ${1, 2, ..., N}$: set of authorized nodes
   ${R_1, R_2, ..., R_N}$: set of reputation values of the authorized nodes
2. Referrer selection and threshold design:
2.1 sort authorized nodes relying on their reputation values in descending order as
    $\tau_1, \tau_2, ..., \tau_N$;
2.2 for $M = 1, 2, ..., M_{\max}$
2.3     select referrers $\tau_1, \tau_2, ..., \tau_M$;
2.4     obtain optimal threshold $\nu_1^*$ by setting $P_{FA} = \delta$;
2.5     obtain misdetection rate $P_{MD}$ via (5.10) based on $M$ and $\nu_1^*$;
2.6 end for
2.7 obtain the optimal number of referrers $M^*$, which achieves the minimum $P_{MD}(M, \nu_1^*)$ in
    set ${1, 2, ..., M_{\max}}$
2.8 referrers $\tau_1, \tau_2, ..., \tau_{M^*}$ provide recommendations for the public node;
2.9 authorize this public node with $\Phi_i$ via (5.2) based on the average recommendation score
    of (5.1).
```

the consortium blockchain-enabled IoT system and the specific application. In order to solve this optimization problem, a distributed access control algorithm is proposed as Algorithm 4.

5.3.2 Anonymous Credential Generation

In the distributed access control, the selected M^* referrers will issue a credential together to this public node if it is authorized with one of $\Phi_1, ..., \Phi_{K-1}$. A credential is also shown in Figure 5.2, which contains authorization level, validity period, credential number, referrers' public keys, and referrers' signatures. The validity period is denoted as Γ, which is determined and agreed by more than 50% authorized nodes in the system initialization phase. Any authorized nodes can verify the credential by checking the referrers' signatures.

To achieve privacy preservation, the anonymous credentials are issued by the referrers to Alice for further authentication and authorization. Figure 5.3 characterizes the process of anonymous credential generation. Firstly, Alice generates L credentials, and blinds them by mixing a randomly blinding factor [164], so that the referrers cannot recognize its original credentials based on the blind versions. Then, Alice sends the blinded credentials to request signatures from its referrers. To verify the blinded credentials, the referrers challenge Alice to show randomly assigned $L - 1$ credentials. After Alice opens the specific $L - 1$ credentials,

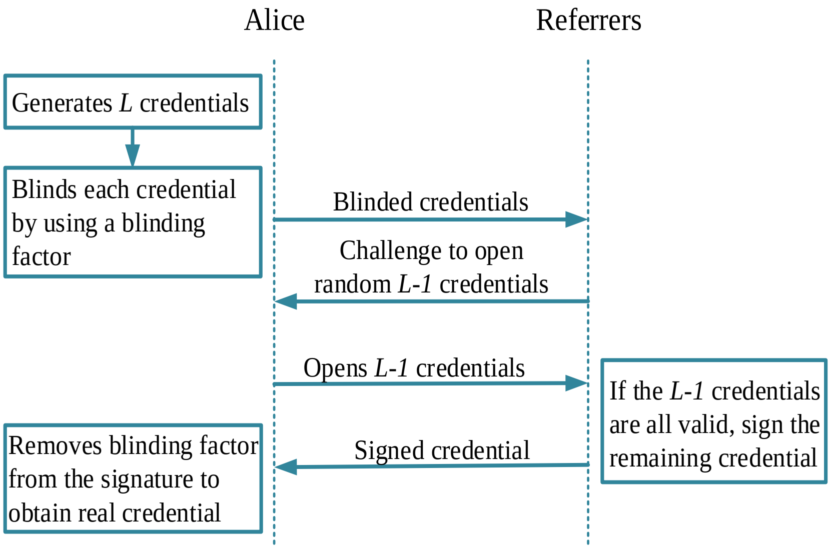

Alice
Referrers
Generates *L* credentials
Blinds each credential by using a blinding factor
Blinded credentials
Challenge to open random *L-1* credentials
Opens *L-1* credentials
If the *L-1* credentials are all valid, sign the remaining credential
Signed credential
Removes blinding factor from the signature to obtain real credential

Figure 5.3: Anonymous credential generation procedure.

the referrers verify them and sign the remaining ones if those $L-1$ credentials are all valid. Here, a credential is valid if I1-I3 in Figure 5.2 are all valid. Finally, after Alice receives the new signed credentials, it removes the blinding factor from the signatures to obtain the real credentials [164]. It can be observed from the process of anonymous credential generation that the real identity of Alice in the consortium blockchain-enabled IoT system will not be linked to its public key by its referrers. Furthermore, a higher L defends against the cheating attacks of signed credentials by Alice, but leads to higher computation, communication overhead, and time latency.

5.3.3 Accountability based on Adaptive Reputation Update and Dynamic Multiple-Level Authorization

The reputation values of N authorized nodes at time t are denoted as $R_1[t], R_2[t], ..., R_N[t]$ and are recorded in the blocks. Note that once a public node joined in the system, the set of authorized nodes will be renewed by adding this node. To stimulate them to provide recommendations for the new public nodes, the referrers' reputation values will be increased as

$$R_m[t+1] = R_m[t] + \theta_0, \tag{5.12}$$

where θ_0 represents the reward for the recommendations.

If the authorized node n attacks the system, such as false data injection attacks [159], denial of service attacks [160], and spoofing other authorized nodes to obtain illegal benefits, the attacked node(s) will broadcast its behaviors to the other authorized nodes, once more than 50% authorized nodes verified them as adversarial, then the reputation value of authorized node n will be decreased as

$$R_n[t+1] = R_n[t] - \vartheta_n[t],\ n \in \{1, 2, ..., N\}, \tag{5.13}$$

where $\vartheta_n[t] \in [0, 1]$ represents the attack level, which is defined corresponding to the specific IoT application. $\vartheta_n[t] = 1$ indicates the case that this node attacked the IoT system with highest level at time t, while $\vartheta_n[t] = 0$ means this node was well-behaved at time t. The average recommendation score of its referrers on this node in the distributed access control of (5.1) is the initial reputation value of authorized node n.

More importantly, if authorized node n attacked the IoT system at time t, the reputation values of its referrers will be decreased as

$$R_{nm}[t+1] = R_{nm}[t] - \theta,\ m = 1, 2, ..., M, \tag{5.14}$$

where R_{nm} represents the m-th referrer of authorized node n and θ is the punishment of recommending a misbehaved node to the system. The punishment on decreasing their reputation values is set to be higher than the reward for the recommendations θ_0. It can be observed from (5.14) that an incorrect recommendation will lead to the decrease of their own reputation values, resulting in an *accountable recommendation mechanism.*

The dynamic multiple-level authorization is processed as

$$\Phi_k : \quad R_n[t] \in (\nu_k, \nu_{k+1}],\ n = 1, 2, ..., N. \tag{5.15}$$

Once the reputation value of authorized node n is lower than ν_1, it will be denied to access the system.

As shown in Figure 5.2, a smart contract is used for the effective, efficient, and secure creation of the proposed scheme, which operates as autonomous actors, and can be trusted to drive forward any on-chain logic that can be expressed as a function of on-chain data inputs [165]. The corresponding functions for adding nodes should be contained in the smart contract, while their opposite functions should also be designed for removing the nodes. To achieve the reputation update for dynamic multiple-level authorization in the system, the adversarial behaviors of a node will be recorded in the blocks, so that the reputation update for both this node and its referrers can be achieved via (5.12), (5.13), and (5.14), respectively. The reputation update function can be executed by the authorized nodes to update the reputation value of a misbehaved node in the smart contract. More importantly, the dynamic multiple-level authorization of (5.2) is also implemented in the smart contract, so that the authorization levels of all authorized nodes can be adaptively updated through publishing the transactions containing adversarial behaviors of the authorized nodes to trigger the function.

5.3.4 Analysis

In the proposed scheme, if an authorized node tries to deanonymize Alice, the anonymity set size is $N-1$, which is defined as the set of nodes that are indistinguishable from Alice with the set including Alice itself [166]. Then the entropy of the anonymity set, denoted as H_q, which expresses the attacker's knowledge of the anonymity set [167], is formulated as

$$H_q = -\sum_{n=1}^{N-1} q_n \log_2 q_n, \tag{5.16}$$

where q_i represents the probability of Alice being the target of this attacker. If all authorized nodes except the attacker have the same probabilities to be the target, H_q achieves its maximum value, denoted as $H_{\max}$, which is given by

$$H_{\max} = \log_2(N-1). \tag{5.17}$$

The accountability is guaranteed in the proposed scheme, and a misbehaved authorized node in the consortium blockchain-enabled IoT system is traceable and punished. To be specific, the adversarial behaviors of authorized nodes and all the recommendations are stored as the transactions in blocks. These records indicate the trustworthiness of authorized nodes, and guarantee the accuracy of reputation values of authorized nodes, so that the multiple-level authorization can be achieved to protect system and to control the risk level of being attacked. More importantly, the referrers should be responsible for their recommendations based on the proposed scheme.

5.4 Simulation Results

In this section, simulation and numerical studies are provided to evaluate the performance of the proposed scheme. Firstly, a blockchain is built, which is controlled by 20 authorized nodes (ANs). The size of block is set to 10. A smart contract is created containing functions for adding and removing nodes, as well as for reputation update. The recommendations of the selected referrers, as well as reputation values and malicious behaviors of all ANs are recorded in the blocks as transactions. Each transaction contains time, transaction identity (ID), blockchain ID, node ID, and public key of exponent. After a transaction is generated, it is signed by the exponent using its private key.

Attack model in the simulation: The 9-th AN (denoted as AN9) is set to be a misbehaved node who cheats the other ANs in the recommendation process and voting process. Moreover, 10-th AN (denoted as AN10) is set to be a misbehaved node who attacks the other ANs in the system and causes denial of service attacks, false data injection attacks, or spoofing attacks by imitating the other ANs to collect private information and obtain illegal benefits in the system. Furthermore, an adversary, who is a public node, tries to join in the integration system controlled by ANs to obtain the illegal benefits. Specifically, Type I attacks represent the cheating attacks and wrong recommendations, while the denial of service attacks, false data injection attacks, and spoofing attacks are denoted as Type II attacks. The punishments for Type I and Type II attacks are set to be 0.1 and 0.2, respectively.

Figure 5.4 characterizes the trade-off between misdetection and false alarm of the proposed recommendation mechanism with respect to different numbers of referrers, i.e., $M = 2$, $M = 3$, and $M = 4$. One can be observed from Figure 5.4 that the misdetection rates of all cases decrease with the increase of threshold of false alarm rate. More importantly, by utilizing more

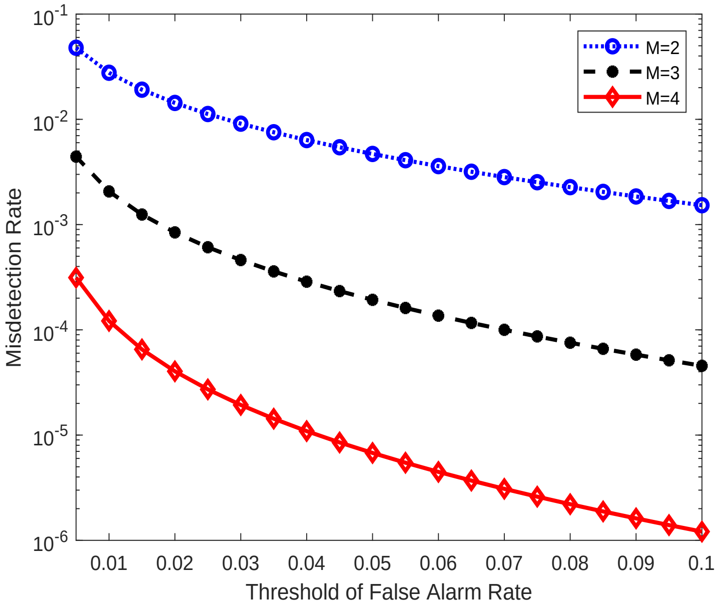


Figure 5.4: Misdetection rate vs. false alarm rate with different numbers of referrers.

referrers in the proposed recommendation mechanism, the misdetection rate of the proposed scheme is lower with a specific threshold of false alarm rate, leading to the improvement of trade-off between misdetection and false alarm.

Figure 5.5 characterizes the effects of referrer number, i.e., M, on the false alarm rate of the proposed scheme with respect to different thresholds, namely for $\nu_1 = 0.2$, $\nu_1 = 0.3$, $\nu_1 = 0.4$, and $\nu_1 = 0.5$, in the distributed access control. It can be observed from Figure 5.5 that as the number of referrers increasing, the false alarm rates of all cases decrease significantly. The reason is that the use of more referrers provides more recommendation information and achieves robust authentication in the proposed scheme. Furthermore, the false alarm rate of the proposed scheme with $\nu_1 = 0.2$ is the lowest, while that of $\nu_1 = 0.5$ is the highest. The reason for this trend is that a higher threshold ν_1 leads to higher probability of failure of Alice to join in the consortium blockchain-enabled IoT system.

Figure 5.6 characterizes the misdetection rate versus the number of referrers, i.e., M, to show the authentication performance of the proposed mechanism with respect to $\nu_1 = 0.2$, $\nu_1 = 0.3$, $\nu_1 = 0.4$, and $\nu_1 = 0.5$ in the distributed access control. It can be observed that the increase of referrer number results in the decrease of misdetection rate. The reason is that it is more difficult for an adversary to conclude or cheat the referrers when more referrers are

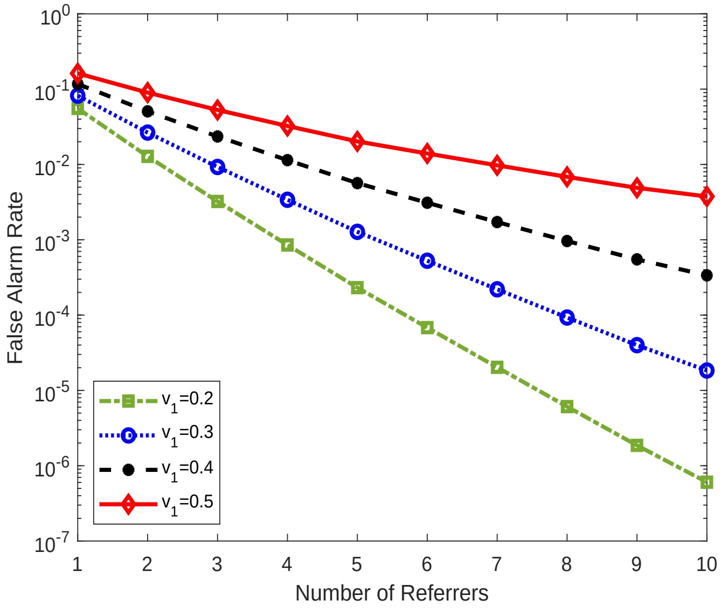


Figure 5.5: False alarm rate vs. number of referrers with respect to different thresholds in the distributed access control.

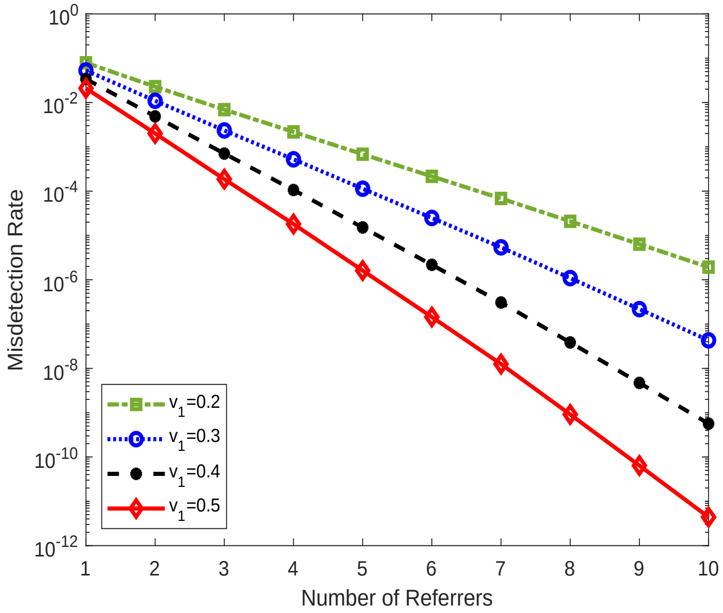


Figure 5.6: Misdetection rate vs. number of referrers with respect to different thresholds in the distributed access control.

required in the proposed scheme. Furthermore, the higher ν_1 leads to lower misdetection rate, which demonstrates the trade-off between the false alarm rate and misdetection rate (see both Figure 5.5 and Figure 5.6).

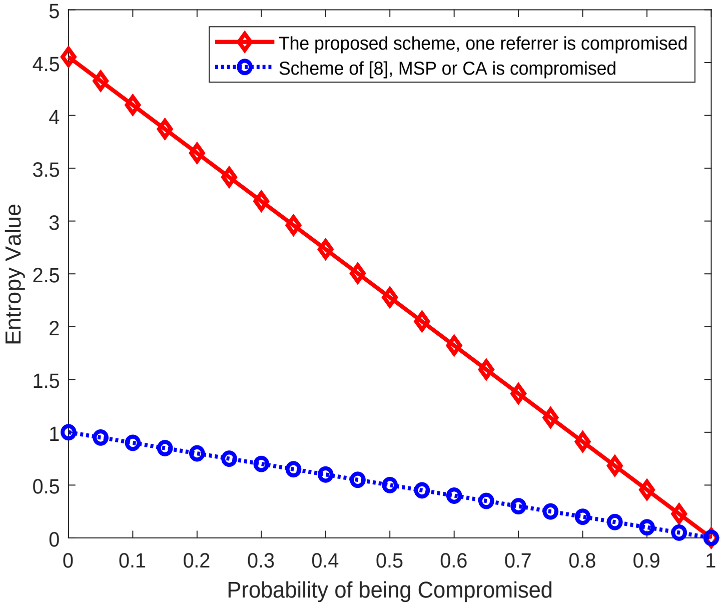


Figure 5.7: Comparison results of privacy preservation between the scheme of [8] and the proposed scheme in the case that the trusted third party or one of Alice's referrers is compromised with a probability.

Figure 5.7 characterizes the comparison results between the scheme of [8] and the proposed scheme, where authentication and authorization in [8] are based on a membership service provider (MSP) and a credential authority (CA), while that of the proposed scheme utilizes multiple referrers. The trusted third party in the scheme of [8] and one of the Alice's referrers in the proposed scheme are compromised with a probability. It is observed from Figure 5.7 that as the increase of probability of trusted third party or one of Alice's referrers being compromised, the entropy values (5.16) of all cases are decreasing. The reason for this trend is that both the scheme of [8] and the proposed scheme suffer from a lower entropy of anonymity set if the third trusted third party or one of Alice's referrers is compromised with a higher probability. One can also observe from Figure 5.7 that the entropy value of the proposed scheme is higher than that of [8] because the scheme in [8] is centralized and controlled by the trusted third party, and the privacy of all authorized nodes in the system will be leaked once the trusted third party is being compromised.

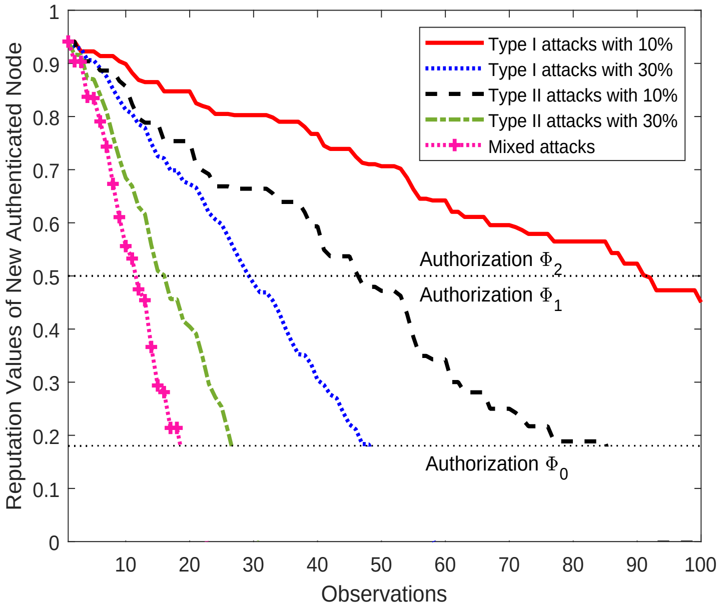


Figure 5.8: Reputation update of the misdetected adversary with respect to different attacking behaviors in the proposed scheme.

Assuming that the Adversary passed the initial authentication and joined the consortium blockchain-enabled IoT system, the reputation value update results of this new authenticated node can be obtained in Figure 5.8 with respect to different attacking behaviors in the case $K = 3$. The observations represent the behaviors of the node observed by the other ANs and recorded as transactions in the blocks. The hybrid attacks of Type I and Type II attacks are denoted as mixed attacks. In Figure 5.8, the attacking behaviors are set to be "on-off" in the system with a probability, e.g., 10% and 30%. The threshold v_1 of (5.2) can be obtained from Algorithm 4 as 0.18, and another threshold is set to be $v_2 = 0.5$ by users. One can observe from Figure 5.8 that the reputation values of misdetected adversary decrease faster if it performs Type II attacks or with a higher attacking probability. The reason for this trend is that the Type II attacks and higher attacking probability cause more damages to the system, thus the punishment will be higher in decreasing the reputation value of this node. According to the multiple-level authorization of (5.2), when the reputation value of this misdetected adversary is lower than 0.5, it will be authorized by Φ_1 with less services/resources to reduce the damages caused by this node as well as to protect the other ANs. Moreover, it will be denied to access the system if its reputation value is lower than 0.18.

The reputation values of the misdetected Adversary and its referrers in the system are given

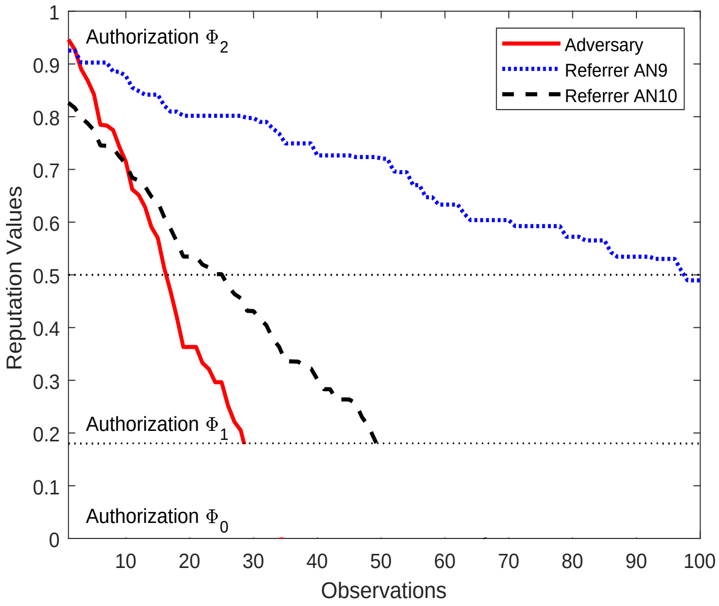


Figure 5.9: Reputation update of the misdetected adversary and its referrers in the proposed scheme.

in Figure 5.9. The observations represent the behaviors of the node and its referrers observed by the other ANs and recorded as transactions in the blockchain. AN9, and AN10 are chosen as the referrers of the misdetected Adversary in the case $M = 2$. In this figure, the misdetected Adversary performs Type II attacks with 30% attacking probability. It can be observed from Figure 5.9 that the reputation values of the misdetected Adversary, AN9, and AN10 are decreasing with the increase of observations. Moreover, the reputation value of AN10 is lower than that of AN9, since it also attacks the system during the distributed access control. In a nutshell, Figure 5.9 characterizes the proposed scheme with the accountable security service based on the developed reputation update strategy.

5.5 Chapter Summary

A distributed access control scheme is proposed for the consortium blockchain-enabled IoT system in this chapter. The developed recommendation mechanism utilizes multiple referrers, who are the authorized nodes in the integration system, to authenticate public nodes in a distributed way. To protect the private information, an anonymous credential update strategy is developed, so that the real identity of each authorized node can be concealed. Then a reputation update strategy was proposed for the referrers to take responsibility for their recommendations and for achieving multiple-level authorization. The simulation and numerical results demonstrated that by increasing the number of referrers, the trade-off between the misdetection rate and false alarm rate of the proposed scheme is increased. Furthermore, the accountability can be achieved based on the proposed scheme.

In next chapter, the communication performance and security enhancement will be comprehensively considered for securing resource-constrained communications. A lightweight continuous authentication scheme will be proposed to identify devices via their pre-arranged pseudo-random access sequences. A device will be authenticated as legitimate if its access sequences are matched with the pre-agreed unique order between the transceiver pair, without incurring long latency and high overhead.

Chapter 6

Lightweight Continuous Authentication via Intelligent Access

Conventional authentication techniques based on cryptography and computational hardness are facing growing challenges for deployment in resource-constrained Internet-of-Things (IoT) devices. To meet the stringent and diverse security requirements of IoT applications, the dramatically increased security overhead and latency from the inherent computational processing make these conventional static security techniques undesirable for emerging machine communications. In this chapter, a novel lightweight continuous authentication scheme is proposed for identifying multiple resource-constrained IoT devices via their pre-arranged pseudo-random access time sequences. A transmitter will be authenticated as legitimate only if its access time sequential order is matched with a pre-agreed unique pseudo-random binary sequence (PRBS) between itself and the base station. The seed for generating the PRBS between each transceiver pair is acquired by exploiting the channel reciprocity and applying the support vector machine (SVM) algorithm, which is time-varying and difficult for a third party to predict. Hence, the proposed scheme provides seamless protection for legitimate communications by refreshing the seeds adaptively without incurring long latency, complex computation, and high communication overhead. Simulation results show that the proposed scheme achieves high entropy and seed bit randomness, and low bit mismatch rate, as well as is robust in the noisy environment. Finally, the superiority of the proposed scheme over the existing schemes is demonstrated in quantization performance, authentication performance, and computation cost.

6.1 Introduction

The fifth generation (5G)-and-beyond networks connect billions of things that include sensors, actuators, services, and other Internet-connected objects, enabling the future smart life and connected industries by Internet-of-Things (IoT) applications, as exemplified by smart cities, intelligent transportation, smart building, just to name a few [4, 168]. However, resource-constrained IoT devices in 5G-and-beyond networks are extremely vulnerable to spoofing attacks, leading to unauthorized access to network resources/services and privacy leakage. The root causes for security weaknesses in wireless IoT communications mainly include the open broadcast nature of radio signal propagation, intermittent machine communications, heterogeneous complex network architecture, as well as the abundance of miniaturized and resource-constrained IoT devices used [2, 95]. More importantly, wireless sensors are widely used in 5G-and-beyond networks for monitoring and recording the physical conditions of the environment, while being equipped with limited computation, storage, and power resources. Hence, lightweight authentication is extremely critical for guarding against the spoofing attacks in 5G-and-beyond networks.

Although the conventional cryptographic techniques [169, 170] have been widely studied, their excessive latency and computation overhead are extremely undesirable for resource-constrained IoT devices. For example, the group key agreement protocols require thousands of interactions to exchange keys for establishing group keys among 5-client groups [26]. The authors of [27] developed a lightweight mutual authentication protocol based on the public key encryption for smart city applications, which strikes a balance between the efficiency and communication cost without sacrificing the security. A scalable framework for lightweight authentication and hierarchical routing in data networking IoT is proposed in [28]. However, these schemes also require many rounds for the key generation, refresh, and delivery, resulting in long time latency and high communication overhead. The authors of [29] proposed a two-factor lightweight privacy-preserving authentication scheme to enhance the security of vehicular ad-hoc network communications relying on the decentralized certificate authority and the biological passwords, which is also unsuitable for the authentication between multiple IoT devices and the base station. Furthermore, the key transmission process in the security management procedures of the cryptographic techniques could lead to potential key leakage [14].

Physical layer authentication techniques of [37, 171, 172] may provide lightweight authentication by exploiting the inherent physical attributes and channel reciprocity of wireless communication links. Compared with the conventional cryptographic based authentication techniques, security overhead and reduced energy consumption in IoT devices can be achieved with physical layer authentication by eliminating the explicit key exchange and its related computation process. The authors of [173] proposed a lightweight mutual authentication protocol based on physical unclonable functions, which may be regarded as unique physical features of a device. Unfortunately, the physical features of a device suffer from imperfect and time-varying estimates, causing their estimates to differ between the transmitter and receiver. Hence, the physical layer key generation techniques of [174, 175, 176, 177, 178, 179] require a key agreement process to guarantee the key correctness between transceiver, but the information of the generated keys may be intercepted during this process. Moreover, the physical layer key generation techniques suffer from very low key generation rates.

Most of the existing authentication schemes are static in time, e.g., [37, 171, 172], thus resulting in abundant loopholes for the adversaries owing to the time-varying wireless environment and heterogeneous complex architecture of 5G-and-beyond networks. Furthermore, the authentication after initial identification cannot be achieved using these one-time schemes. To overcome these challenges, a continuous physical layer authentication scheme is proposed in [2] based on the kernel machine learning approach as an intelligent process by utilizing multiple communication link-related and device-related attributes. Its performance still suffers from the imperfect estimates and variations of physical layer attributes, leading to inevitable misdetections and false alarms in the continuous authentication process.

Hence, a new lightweight continuous authentication scheme is proposed by identifying the pre-arranged pseudo-random access time sequence of each transmitter (i.e., IoT device), which provides high uncertainties for the adversaries as well as seamless protections for legitimate communications. To be more specific, a pseudo-random binary sequence (PRBS) is pre-agreed between a pair of IoT device and base station for authentication, which is difficult for the adversaries to predict and does not require additional hardware for implementation. The access time sequence of an IoT device, which is different from this pre-agreed PRBS, will be identified to be coming from a spoofer by the base station. Different from the time-division multiplexing (TDM) methods [180], the time domain is divided into recurrent time slots of fixed length and arrange them intelligently for authentication purposes.

In order to achieve lightweight continuous authentication, the channel reciprocity [14] is explored to acquire the seeds for generating PRBSs, where a transceiver pair can observe the same channel simultaneously. To be more specific, the physical layer features are utilized for generating dynamic seeds, which benefit from their time-varying characteristic and are difficult for the adversaries to predict. In contrast to the physical layer key generation techniques of [174, 175, 176, 177, 178, 179], the seed acquisition technique does not require a high seed generation rate, since the seeds are used for generating PRBSs rather than for practical applications directly, as exemplified by encryption and decryption. Moreover, only three phases are required for seed acquisition, namely for channel probing, quantization and verification, where the quantization phase is the main phase of the developed seed acquisition technique for transferring the extracted channel measurements into bits.

Although the received signal strength (RSS)-based quantization method [175] is easy to implement, its entropy is low and does not work well for wireless communication systems that consist of static nodes. Moreover, the frequency phase-based quantization method [179] applies multiple thresholds to quantize each estimated frequency-phase, but wrong decisions can be made if the estimated frequency phases are close to the region boundaries, leading to a high mismatch rate of quantization between the transceiver pair. Hence, the fundamental principle of machine learning-based anomaly detection techniques [181, 182] is studied in this chapter to improve the quantization performance. Different from the anomaly detection techniques, which focus on maximizing the detection accuracy, the objective of quantization in this chapter is to divide the channel measurements into bits by designing a region boundary intelligently to achieve high entropy and seed bit randomness as well as low bit mismatch rate on transceiver sides, so that a high quantization accuracy and uncertainty can be achieved.

In this chapter, a lightweight continuous authentication scheme is proposed by identifying the pre-arranged access time sequence of each IoT device corresponding to the PRBS pre-generated by an identical unique seed on both transceiver sides. To obtain the seed, a new support vector machine (SVM)-based seed acquisition technique is developed by utilizing physical layer features for generating specific PRBSs between the base station and multiple IoT devices, which consists of three phases, namely channel probing, quantization, and verification. The SVM is applied to derive an optimal nonlinear boundary for quantizing the measurements of physical layer attributes used into bits to improve entropy and seed bit randomness while decreasing the bit mismatch rate of the obtained seed. The seeds for PRBS generation are updated dynamically by estimating the time-varying physical layer features, thus resulting in natural adaptive protections for the legitimate communication parties and high uncertainty for the adversaries.

Specifically, the contributions of this chapter are summarized as follows:

- A novel authentication scheme is proposed to identify the access time sequence of each IoT device corresponding to its pre-agreed unpredictable PRBS. This scheme is lightweight and provides continuous authentication between a base station and multiple IoT devices. Explicitly, this scheme provides a new device authentication method, which is radically different from the existing authentication schemes via the identification of keys or communication-related features;

- A seed acquisition technique is developed by utilizing physical layer features to obtain identical seeds for PRBS generation and update between a base station and IoT device pair without exchanging the obtained seed, so that the PRBS leakage could be avoided. To transform the measurements of the physical layer features into seeds, the SVM is explored to derive an optimal nonlinear boundary to improve the quantization accuracy;

- Simulation results are presented to demonstrate the superior performance of the proposed scheme in quantization performance, time complexity, authentication performance, and computation cost, compared with some exiting schemes. Furthermore, the results show that the proposed scheme is robust in the noisy communication environment and false alarm events can be avoided.

The rest of this chapter is organized as follows. In Section 6.2, the system model used in this chapter is presented. The lightweight continuous authentication scheme is proposed based on the intelligently arranged pseudo-random access in Section 6.3. The performance analysis is also presented in Section 6.3. Simulation results are given in Section 6.4. Finally, Section 6.5 concludes this chapter.

Table 6.1: Notations of Chapter 6

Notations	Definitions
N	Number of physical layer attributes used.
$\boldsymbol{H}_B$	Attribute estimates at the base station.
L	Number of IoT devices.
$\boldsymbol{H}_l$	Attribute estimates at the l-th IoT device.
B^{II}	Bit mismatch rate of quantization phase.
γ_0	Ratio of 0 bits in the obtained seed.
$\boldsymbol{c}$	Center of quantization boundary.
R	Radius of quantization boundary.
J	Number of samples for training at the base station.

Notations: In this chapter, scalars are denoted by italic letters, while vectors are respectively denoted by bold-face letters. Table 6.1 shows the notations of this chapter.

6.2 System Model and Dynamically Arranged Pseudo-Random Access

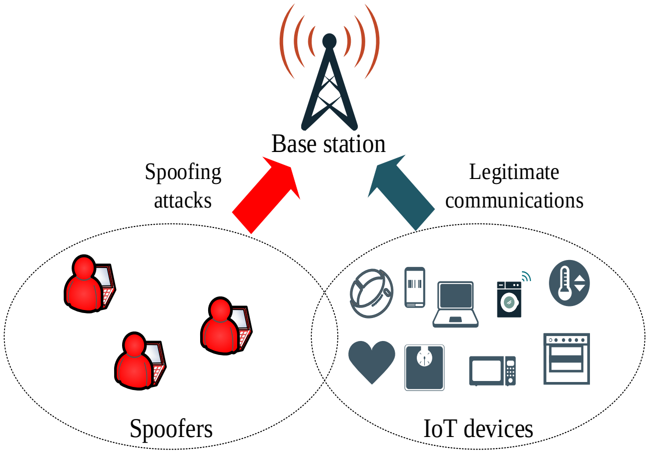


Figure 6.1: System model in the 5G-and-beyond network. The communications between multiple IoT devices and a base station suffer from the spoofing attacks caused by the adversaries.

As shown in Figure 6.1, wireless communications between legitimate IoT devices and a base station suffer from spoofing attacks. The spoofers aim at imitating the legitimate IoT devices, then try to access the system for gleaning illegal advantages or injecting false data to the cloud/Internet, leading to unauthorized access, privacy leakage, wrong decisions, and so on. The base station needs to unambiguously and continuously identify the spoofers from the legitimate devices. It is assumed that the spoofers are located more than a wavelength away from the legitimate IoT devices, and that the clocks of IoT devices and base station are synchronized. More importantly, owing to the characteristics of IoT devices, namely the limited computation, storage, and power resources, the concept of lightweight authentication is extremely critical in the 5G-and-beyond networks.

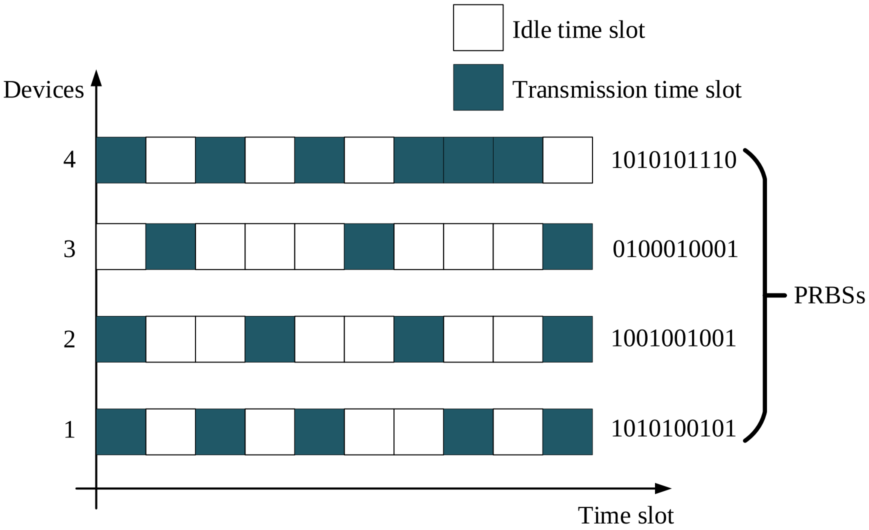


Figure 6.2: The developed authentication method between IoT devices 1-4 (transmitters) and a base station (receiver) through the identification of the pre-arranged pseudo-random access time sequences of IoT devices according to the pre-agreed PRBSs.

Figure 6.2 characterizes the novel authentication scheme based on the arranged pseudo-random access in the time-domain, which aims at supporting the authentication between a base station and multiple IoT devices, e.g., devices 1-4. To be more specific, the time domain is divided into recurrent time slots of fixed length. Each IoT device sends its messages to the base station in the time slots corresponding to its identical pseudo-random binary sequence (PRBS) pre-agreed between this IoT device and the base station, thus an incorrect access in the time-domain will be detected from a spoofer. The PRBSs are very difficult for the adversaries to predict, if their seeds are concealed from the spoofers. More importantly, a seed can be used to generate a number of PRBS bits, thus providing a lengthy secure identification of each IoT device at the base station. In contrast to the conventional key-based cryptographic and physical layer security techniques, authentication via pseudo-random access does not require complicated computation, extra hardware, and excessive latencies. Hence, a *lightweight continuous authentication* between a base station and multiple IoT devices can be achieved.

To achieve the lightweight continuous authentication, the seeds for generating PRBSs are required to satisfy the following policies: 1) a transceiver pair should obtain the same seed, so that an identical PRBS could be generated for authentication at the base station; 2) seeds should be concealed from any other devices, thus the generated PRBSs will be difficult for the spoofers to predict; and 3) seeds should be refreshed dynamically to achieve a continuous authentication having high uncertainty for the spoofers. To meet these requirements, the physical layer features are utilized to develop a new seed acquisition technique for PRBS generation, e.g., channel state information (CSI) [4], carrier frequency offset (CFO) [37], and received signal strength indicator (RSSI) [39], just to name a few. The main reason is that the physical layer features provide a high degree of uncertainty for adversaries as well as strong correlated information between a transceiver pair. In other words, it is very difficult for spoofers to predict the physical layer features of a transceiver if they are at different locations, while each pair of transceiver can obtain the same channel estimates at the same time because of the channel reciprocity property [174, 175, 176, 177, 178, 179]. More importantly, the time-varying features of communication links provide a natural refresh method for renewing seeds.

However, perfect channel reciprocity is generally impractical mainly due to the mobility of devices, the different responses of the radio frequency front ends and the non-symmetric interference characteristics observed at the two devices of a communication link, the quantization and measurement errors, as well as the time lag between the bidirectional channel measurements [174, 175]. This imperfect channel reciprocity directly influences the accuracy of seed acquisition, thus leading to a possible disagreement of the generated PRBSs on both sides. The channel estimates at the base station and IoT devices are denoted, respectively, as

$$\boldsymbol{H}_B[t_1] = (H_{B1}[t_1], H_{B2}[t_1], ..., H_{BN}[t_1])^{\mathrm{T}}, \tag{6.1}$$

and

$$\boldsymbol{H}_l[t_2] = (H_{l1}[t_2], H_{l2}[t_2], ..., H_{lN}[t_2])^{\mathrm{T}},\ l = 1, 2, ..., L, \tag{6.2}$$

where N is the number of physical layer features used, L denotes the number of IoT devices, and T represents the transposition of a vector. t_1 and t_2 are estimation time instants at the base station and IoT device, respectively, which represent the time lag of channel estimation on different sides.

The objective is to obtain an identical unique seed between the base station and each IoT device based on $\boldsymbol{H}_B[t_1]$ and $\boldsymbol{H}_l[t_2]$, which satisfies the policies listed above, and will directly affect the performance of the proposed scheme. To facilitate the discussion of the developed seed acquisition technique, some important evaluation metrics are presented next to assess the performance of the proposed scheme.

Entropy: which refers to the uncertainty associated with a random variable [175], and is used to evaluate the security strength of the proposed scheme. It is defined as

$$E = \sum_{k=1}^{K} E_k, \tag{6.3}$$

where

$$E_k = -p_{k0} \log p_{k0} - (1 - p_{k0}) \log(1 - p_{k0}), \tag{6.4}$$

K is the binary bit number of the acquired seed and p_{k0} denotes the posterior probability of its k-th bit when the bit is 0 from the spoofers' knowledge.

Bit mismatch rate: which represents the difference between the seeds obtained by the base station and each IoT device relying on physical layer attribute estimation [175], and is defined as

$$B = \frac{|S_B - S_l|}{K}, \tag{6.5}$$

where S_B and S_l represent the seeds obtained at the base station and IoT device l, respectively.

Seed bit randomness: which is used to evaluate the security performance of the seed acquisition technique, since a less random seed will result in a smaller search space by brute force attacks thus compromising the security [174].

This chapter focuses on developing a new seed acquisition technique to increase the entropy and seed bit randomness, as well as to decrease the bit mismatch rate to achieve the lightweight continuous authentication via pseudo-random access in the time-domain (see Figure 6.2).

6.3 Intelligently Arranged Access for Lightweight Continuous Authentication

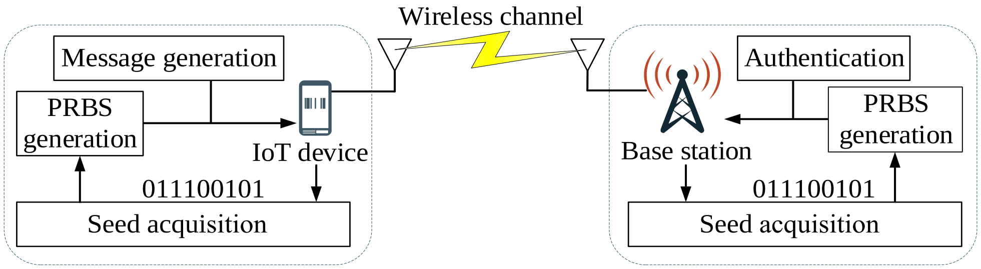


Figure 6.3: Framework of the proposed lightweight continuous authentication scheme through identifying the pre-arranged pseudo-random access time sequences of IoT devices.

As shown in Figure 6.3, the proposed scheme contains three components at both the base station and IoT device sides. IoT device l should probe the channel between itself and the base station to obtain a channel estimate, namely for $\boldsymbol{H}_l[t_2]$, which is used for acquiring a seed. Then, IoT device l sends its messages in the time sequence corresponding to the PRBS generated by this seed. The base station should also obtain the same seed relying on the channel estimate, i.e., $\boldsymbol{H}_B[t_1]$, for generating an identical PRBS to authenticate IoT device l. In this section, a new seed acquisition technique based on the support vector machine (SVM) algorithm is firstly proposed to obtain identical seeds between the base station and IoT device l by utilizing multiple features of the communication links. Note that the machine learning algorithm is implemented at the base station, which is used to derive an optimal non-linear boundary to quantize the channel measurements into bits (i.e., seeds). Then, the PRBS generation and update schemes as well as the performance analysis are presented.

6.3.1 Seed Acquisition Technique

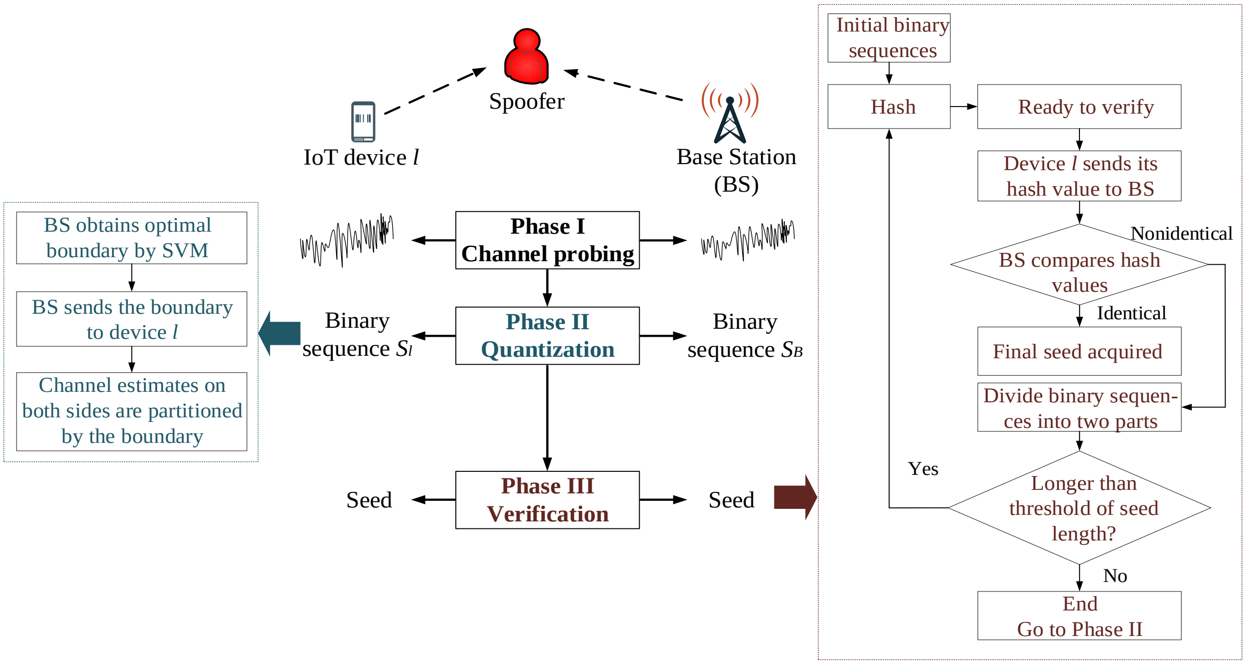


Figure 6.4: Process of the developed new seed acquisition technique for PRBS generation containing three phases: Channel probing, Quantization, and Verification.

The developed seed acquisition technique at the base station and each IoT device operates in three phases shown as Figure 6.4 as follows:

Phase I. Channel probing: This is used to collect channel measurements by the base station and IoT devices [183, 184]. In this phase, the base station and IoT device l exchange channel probing signals with each other. Then, highly correlated measurements of the physical layer attributes used are collected by the base station and IoT device l because of the channel reciprocity property, namely for $\boldsymbol{H}_B[t_1]$ and $\boldsymbol{H}_l[t_2]$, respectively.

In the channel probing process, a higher probing rate enjoys a high seed generation rate but compromises the randomness of the generated seed sequence because of correlation between the sampled data, while a lower probing rate results in a lower seed generation rate [179]. Different from the physical layer key generation techniques [174, 175, 179], the developed seed acquisition technique does not require a high seed generation rate. The reason is that the seeds are used for generating PRBSs rather than for applications directly, such as encryption and decryption.

Phase II. Quantization: This phase is used to quantize the extracted channel measurements into bits [175, 179]. It is the main phase of the developed seed acquisition technique, since it provides the initial binary sequences for seed acquisition and significantly affects the authentication performance. Note that wrong decisions can be made in the quantization phase if the channel measurements are close to the region boundaries. The imperfect channel reciprocity and the noise are the main factors that impact the quantization accuracy [179]. More importantly, the measurements of physical layer attributes are usually not uniformly distributed. For example, according to [37], the estimated CFO can be well approximated by a Gaussian random variable. Hence, most of the measurements of physical layer attributes used could be intensively distributed. In this case, the quantization accuracy will be low if the region boundary crosses those intensive measurements.

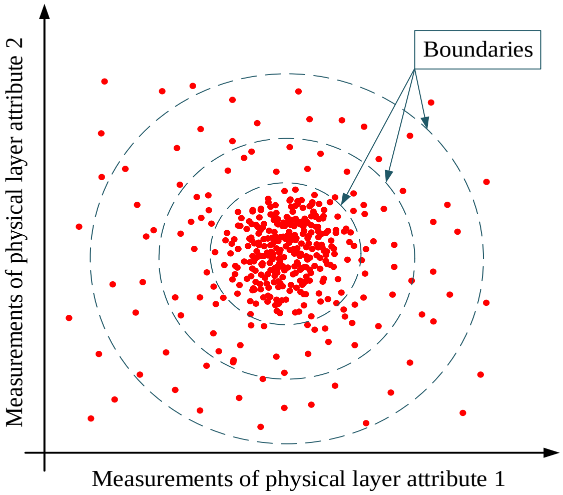

Boundaries
Measurements of physical layer attribute 2
Measurements of physical layer attribute 1

Figure 6.5: The schematic diagram of the developed SVM-based quantization method with multiple boundaries. The red dots are the measurements of physical layer attributes used.

The extracted channel measurements are quantized into bits by designing an optimal region boundary based on the support vector machine (SVM) algorithm [185, 186, 187, 188]. A two-dimensional example of the developed quantization method with different boundaries is shown in Figure 6.5, where only two physical layer attributes are used in this example. As it is shown in Figure 6.5, those sparsely distributed data are partitioned by each boundary from the intensively distributed data, thereby the quantization accuracy will be increased because there are fewer data close to the boundary. Those intensive data in the boundary are quantized to 1, and the others are quantized to 0. It can also be observed from Figure 6.5 that a larger boundary will lead to a smaller number of 0 bits in the generated seed, leading to low entropy, although achieving a better quantization accuracy. On the other hand, a smaller boundary will result in a higher bit mismatch rate of the seed, since there are more data close to the boundary. Hence, there is a trade-off between the quantization performance and security performance in this phase, and the boundary, which is a super-circle, should be well-designed to achieve a better trade-off.

The objective of quantization is to minimize the bit mismatch rate while guaranteeing the minimum number of 0 bits required by deciding the radius and center of the boundary. Hence, the quantization optimization problem in the proposed scheme can be formulated as

$$\begin{gathered}(R, \boldsymbol{c}) = \arg\min B^{\mathrm{II}}, \\ \text{s.t. } \gamma_0 \geq \theta,\end{gathered} \tag{6.6}$$

where B^{II} represents the bit mismatch rate between the base station and IoT device l in phase II, while R and $\boldsymbol{c} = (c_1, c_2, ..., c_N)^{\mathrm{T}}$ denote the radius and center of the boundary, respectively. The parameter γ_0 is the ratio of 0 bits in the obtained seed, which is formulated as

$$\gamma_0 = \frac{K_0}{K}, \tag{6.7}$$

where K_0 represents the number of 0 bits, and θ in (6.6) is the threshold of the ratio of 0 bits in the obtained seed.

In order to solve the optimization problem of (6.6), the SVM technique is applied to determine the radius and center of the optimal boundary. Assuming that J samples of the utilized physical layer features of IoT device l are used for training at the base station, i.e., $\boldsymbol{H}_{lj}, j = 1, 2, ..., J$, the optimization problem of (6.6) is turned into the classification problem

$$\begin{gathered}\min_{(R, \boldsymbol{c}, \boldsymbol{\xi})} \{R^2 + C \sum_{j=1}^{J} \xi_j\} \\ \text{s.t. } \parallel \boldsymbol{H}_{lj} - \boldsymbol{c} \parallel^2 \leq R^2 + \xi_j,\ \xi_j \geq 0,\ j = 1, 2, ..., J,\end{gathered} \tag{6.8}$$

where $\xi_j, j = 1, 2, ..., J$, are known as slack variables [189] and commonly used in optimization to define relaxed versions of some constraints, $\boldsymbol{\xi} = (\xi_1, \xi_2, ..., \xi_J)^{\mathrm{T}}$. In this optimization problem, a slack variable ξ_j measures the distance by which vector $\boldsymbol{H}_{lj}$ violates the desired inequality, i.e., $\| \boldsymbol{H}_{lj} - \boldsymbol{c} \|^2 \geq R^2$. Parameter C determines the trade-off between margin-maximization and the minimization of the slack penalty $\sum_{j=1}^{J} \xi_j$. Note that C can be determined to satisfy $\gamma_0 \geq \theta$ in (6.6) according to specific training data obtained, i.e., $\boldsymbol{H}_{lj}, j = 1, 2, ..., J$. In other words, if the slack penalty C is set to be smaller, the slack variables ξ_j will be higher, then more channel measurements will be quantized to be 0s in the developed seed acquisition technique. However, the amount of physical layer feature estimates of legitimate IoT devices available is usually limited to set aside a validation sample since that would leave an insufficient amount of training data in practice. Therefore, the cross-validation method [189] is applied to exploit the labeled data for determining C in the implementation of the proposed scheme, which satisfies

$$\vartheta_0 \leq C \leq \vartheta. \tag{6.9}$$

ϑ_0 and ϑ are two parameters designed to satisfy the condition $\gamma_0 \geq \theta$ in (6.6), since a smaller C results in higher γ_0 while ϑ_0 represents the minimum C that leads to $\gamma_0 = 0.5$.

The optimization problem of (6.8) is a convex optimization problem, since the constraints are affine and convex, and the objective function is convex. Hence, the Lagrangian function is derived with Lagrange variables $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_J)^{\mathrm{T}}$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, ..., \beta_J)^{\mathrm{T}}$ as

$$\mathcal{L}(R, \boldsymbol{c}, \boldsymbol{\xi}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = R^2 + C \sum_{j=1}^{J} \xi_j - \sum_{j=1}^{J} \beta_j \xi_j - \sum_{j=1}^{J} \alpha_j (R^2 + \xi_j - \| \boldsymbol{H}_{lj} - \boldsymbol{c} \|^2). \tag{6.10}$$

Defining the Lagrange dual function $\mathcal{F}$ as the minimum value of the Lagrangian function over $(R, \boldsymbol{c}, \boldsymbol{\xi})$, it has

$$\begin{aligned} \mathcal{F}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \inf_{(R, \boldsymbol{c}, \boldsymbol{\xi})} \mathcal{L}(R, \boldsymbol{c}, \boldsymbol{\xi}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \inf_{(R, \boldsymbol{c}, \boldsymbol{\xi})} \{ R^2 + C \sum_{j=1}^{J} \xi_j \\ - \sum_{j=1}^{J} \alpha_j (R^2 + \xi_j - \| \boldsymbol{H}_{lj} - \boldsymbol{c} \|^2) - \sum_{j=1}^{J} \beta_j \xi_j \}. \end{aligned} \tag{6.11}$$

Since the dual function is the pointwise infimum of a family of affine functions of $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, it is also concave. Then, the Lagrange dual problem associated with the problem of (6.8) is given as

$$\max_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \mathcal{F}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \max_{(\boldsymbol{\alpha},\boldsymbol{\beta})} \inf_{(R,\boldsymbol{c},\boldsymbol{\xi})} \mathcal{L}(R,\boldsymbol{c},\boldsymbol{\xi},\boldsymbol{\alpha},\boldsymbol{\beta}). \tag{6.12}$$

According to the Karush-Kuhn-Tucker (KKT)'s theorem of [189], the KKT conditions apply at the optimum and can be obtained by setting the gradient of the Lagrangian function of (6.10) with respect to the primal variables R, $\boldsymbol{c}$, and ξ_j to zero. Hence, the flowing equations can be obtained

$$\begin{gathered}\sum_{j=1}^{J} \alpha_j = 1, \ \sum_{j=1}^{J} \alpha_j \boldsymbol{H}_{lj} = \boldsymbol{c}, \ \alpha_j + \beta_j = C, \\ \alpha_j = 0 \vee R^2 + \xi_j = \| \boldsymbol{H}_{lj} - \boldsymbol{c} \|^2, \ \beta_j = 0 \vee \xi_j = 0. \end{gathered} \tag{6.13}$$

Then, the Lagrange dual problem of (6.12) can be rewrote as

$$\begin{gathered}\max_{\boldsymbol{\alpha}} \sum_{j=1}^{J} \alpha_j \| \boldsymbol{H}_{lj} - \boldsymbol{c} \|^2 = \max_{\boldsymbol{\alpha}} \{ \sum_{j=1}^{J} \alpha_j \boldsymbol{H}_{lj}^{\mathrm{T}} \boldsymbol{H}_{lj} - \sum_{i,j=1}^{J} \alpha_i \alpha_j \boldsymbol{H}_{li}^{\mathrm{T}} \boldsymbol{H}_{lj} \}, \\ \text{s.t. } 0 \leq \alpha_j \leq C, \ j = 1, 2, ..., J, \end{gathered} \tag{6.14}$$

where C satisfies (6.9). This is a quadratic programming problem, which can be solved by some well-studied algorithms, as exemplified by the interior point, active set, augmented Lagrangian, conjugate gradient, gradient projection, extensions of the simplex algorithm [190].

Theorem 6.1: In the quantization phase, the optimal boundary for dividing the estimates of attributes used in the proposed scheme is a hypersphere with center and radius given, respectively, by

$$\boldsymbol{c}^* = \sum_{j=1}^{J} \alpha_j^* \boldsymbol{H}_{lj}, \tag{6.15}$$

and

$$R^{*2} = \| \widehat{\boldsymbol{H}}_{li} - \boldsymbol{c}^* \|^2 \tag{6.16}$$

where $\boldsymbol{\alpha}^* = (\alpha_1^*, \alpha_2^*, ..., \alpha_J^*)^{\mathrm{T}}$ is the solution of the quadratic programming problem of (6.14). $\widehat{\boldsymbol{H}}_{li}$ is the support vector, whose Lagrange variable satisfies $0 < \alpha_i^* < C$.

Proof: According to the KKT conditions of (6.13), the center of the optimal boundary can be obtained directly as (6.15) by deriving the solution of the quadratic programming problem of (6.14). Moreover, some results of the developed SVM-based quantization method can be obtained as follows

$$\begin{cases} \xi_i = 0 \ \& \ \| \boldsymbol{H}_{li} + \boldsymbol{c} \|^2 \leq R^2, & \text{if } \alpha_i = 0 \\ \xi_i = 0 \ \& \ \| \boldsymbol{H}_{li} + \boldsymbol{c} \|^2 = R^2, & \text{if } 0 < \alpha_i < C \\ \xi_i \geq 0 \ \& \ \| \boldsymbol{H}_{li} + \boldsymbol{c} \|^2 \geq R^2, & \text{if } \alpha_i = C \\ \xi_i = 0 \ \& \ \alpha_i = 0, & \text{if } \| \boldsymbol{H}_{li} + \boldsymbol{c} \|^2 < R^2 \\ \xi_i > 0 \ \& \ \alpha_i = C, & \text{if } \| \boldsymbol{H}_{li} + \boldsymbol{c} \|^2 > R^2 \end{cases} . \tag{6.17}$$

Hence, if $0 < \alpha_i^* < C$, $\| \boldsymbol{H}_{li} + \boldsymbol{c}^* \|^2 = R^2$ satisfies. To obtain the radius of the optimal boundary, the support vector $\widehat{\boldsymbol{H}}_{li}$ is utilized. Then, the radius of the optimal boundary in the developed SVM-based quantization method is formulated as (6.16). □

Remark 6.1: The designed boundaries in the existing quantization methods, e.g., the RSS-based quantization method [175] and frequency phase-based quantization method [179], are static in time. Moreover, only one-dimensionality is considered in these quantization methods, i.e., RSS and frequency phase. These all lead to low quantization performance of the proposed scheme relying on multiple attributes in the time-varying environment. This is mainly because these quantization methods lack analysis of the physical layer attributes used and adaptation in the noisy dynamic environment. The developed SVM-based quantization method is intelligent in designing the optimal boundaries based on the measurements of physical layer attributes, which circumvents the intensively distributed data, thus resulting in high quantization accuracy and seed randomness.

As shown in Figure 6.4, after obtaining the optimal radius and center of the boundary, the base station sends the trained super-circle to the IoT device l, so that highly similar binary sequences will be acquired on both the base station and IoT device sides. Note that the spoofers cannot predict the seed generated by the base station and IoT device l, even though they intercept and compromise the boundary information. It is because they do not observe the same channel between the base station and IoT device l if they are at different locations. More importantly, the super-circle can be trained in the beginning of network establishment, and updated frequently at the base station. Hence, the developed seed acquisition technique is lightweight at the IoT devices, as well as achieves high entropy and seed bit randomness while minimizing the bit mismatch rate of binary sequences S_B and S_l.

Phase III. Verification: In order to make sure that the seeds generated at both the base station and IoT device l sides are identical, the verification is designed in the last phase of the seed acquisition technique. The block diagram of verification is given in Figure 6.4 (on the right side). Firstly, both the base station and IoT device l use the same hash function to generate hash values for binary sequences S_B and S_l obtained in Phase II, and exchange their hash values to verify the agreement of the binary sequences S_B and S_l. An agreement is reached if their hash values are identical. Otherwise, they divide each binary sequence into two binary sequences with the same length, and verify both of them until an identical binary sequence appears. This identical binary sequence is specified as the final seed of the base station and IoT device l for generating PRBS.

Remark 6.2: It can be observed from the verification process that the seed exchange is not required, so that authentication information (i.e., PRBS) leakage could be avoided. This is mainly because the SVM is applied to achieve high quantization accuracy for acquiring the highly similar binary sequences S_B and S_l. More importantly, the identical seed is acquired between the base station and each IoT device although the physical layer features suffer from the imperfect estimation and variations in the complex time-varying environment. In other words, the proposed scheme is robust in the noisy wireless communication environment.

6.3.2 PRBS Generation and Update

After obtaining a seed between the base station and IoT device l, the PRBS can be generated using the linear feedback shift registers [191]. A PRBS sequence is generated by a monic polynomial of degree μ with typical values of μ equal to 7, 9, 11, 15, 20, 23, and 31. $2^{\mu} - 1$ is the maximum number of bits. Note that the PRBS generator design has been well-studied, and is not a main focus in this chapter.

One can be observed from the process of seed acquisition in Figure 6.4 that the key physical layer feature is the time-varying nature of the channel, so that the seeds for PRBS generation between the base station and each IoT device can be renewed naturally by repeating the developed seed acquisition process. Due to the unique property of physical layer features used for seed acquisition, the pseudo-random access designed for authentication, and the PRBS update, it is extremely difficult for spoofers to imitate the legitimate IoT devices. Moreover, the time period can be decided for renewing the seed between the base station and each IoT device based on the sequence generating monic polynomial used.

Remark 6.3: Collisions may occur when multiple IoT devices transmit the packets to the base station at the same time, since their PRBSs are pre-generated by seeds utilizing the channel estimation. This provides high uncertainty for spoofers but makes it difficult to control the collisions as well. The orthogonal frequency-division multiplexing (OFDM) scheme can be applied to reduce the collisions, but resulting in the waste of spectrum resources in the 5G-and-beyond network. In order to overcome this difficulty, the code-domain or power-domain non-orthogonal multiple access (NOMA) can be applied to reduce the collisions as well as to improve the quality of services (QoS). The principle is that the multiple domains (i.e., time domain, frequency domain, power domain, and code domain) can be well designed to coordinate the accesses of IoT devices, so that both high communication performance and efficient security management can be achieved.

Remark 6.4: The proposed authentication scheme is suitable for those IoT applications that devices are not distributed with a high density or different authentication schemes are co-existing for smart services.

6.3.3 Performance Analysis

As shown in Figure 6.4, the quantization phase significantly affects the performance of seed acquisition, i.e., entropy, bit mismatch rate, and seed bit randomness. Performance analysis of the proposed scheme on these evaluation metrics is presented as follows:

Entropy

Due to the physical layer features used in the proposed scheme for obtaining the seed between the base station and each IoT device, it is extremely difficult for the spoofers, who are in different locations, to observe and predict the same channel measurements. Furthermore, the proposed SVM-based quantization method provides further entropy improvement. To be specific, on the one hand, the channel measurements are quantized to bits, instead of using them directly. On the other hand, the binary sequences obtained in the quantization phase will be further processed in the verification phase without releasing any seed information between the base station and each IoT device in the developed seed acquisition technique. Hence, the unique property of physical layer features, SVM-based quantization, and verification of the proposed scheme provide multi-dimensional and multi-layered protections for the legitimate communications between the base station and IoT devices, resulting in high entropy.

Bit mismatch rate & Seed bit randomness

Theorem 1 provides the optimal solution for the optimization problem of (6.6), which minimizes the bit mismatch rate under the constraint $\gamma_0 \geq \theta$. Since a higher γ_0 will result in higher randomness of seed bits, the optimization problem of (6.6) describes a trade-off between the bit mismatch rate and seed bit randomness. In the proposed scheme, given the requirement of seed bit randomness θ, the lowest bit mismatch rate in Phase II of the developed seed acquisition technique can be obtained.

Lightweight authentication

The proposed scheme authenticates the IoT devices through their pseudo-random access in the time-domain. Compared with the conventional key-based cryptographic techniques [169, 170], the proposed scheme does not require a number of rounds for the system setup, key generation, distribution, refreshment, and revocation. Different from the physical layer security techniques [37, 171, 172], the proposed scheme provides robust continuous authentication even in noisy complex communication without continuous parameter updating. Note that the developed SVM-based quantization method can be implemented at the base station before the authentication. Hence, the proposed scheme is a lightweight solution and provides continuous protections for the communications between the base station and each IoT device in the 5G-and-beyond network.

6.4 Simulation Results

In this section, the simulation of the proposed lightweight continuous authentication scheme is firstly presented to show its feasibility. To be specific, the optimal quantization boundary $(R^{*2}, \boldsymbol{c}^*)$ given in Theorem 1 is derived relying on the estimates of given physical layer attributes, namely carrier frequency offset (CFO), channel impulse response (CIR), and received signal strength indicator (RSSI). After the verification phase, the seeds of multiple pairs of transceivers are acquired. The continuous authentication between each pair of transceiver is achieved based on the identical PRBS generated by their unique seed. Then, the comparison results between the proposed scheme and state-of-the-art schemes are given to demonstrate the superior performance of the proposed solution in quantization performance, authentication performance, and computation cost. Specifically, it is compared with the RSS-based quantization scheme of [175], physical layer key generation schemes of [174, 175, 176, 177, 178], static authentication scheme, continuous kernel machine learning-based physical layer authentication scheme of [2], and physical layer authentication scheme of [39].

6.4.1 Implementation of The Proposed Scheme

Table 6.2: Simulation parameters of Chapter 6

Parameters	Value
Range	1 km × 1 km
Center frequency f_c	5 GHz
Sampling rate	20 MHz
Antenna number of IoT devices	4
Antenna number of the base station	8
Time lag between the bidirectional channel measurements	10 ms

The proposed lightweight continuous authentication scheme is simulated by utilizing multiple physical layer attributes, i.e., CFO [37], CIR [2], and RSSI [39], in an urban scenario. The simulation parameters for the implementation are shown in Table 6.2 and the system topology of the simulation is shown in Figure 6.6. Specifically, 10 IoT devices are distributed in the range of 1 km × 1 km, and the multipath channel model used in the simulation is formulated

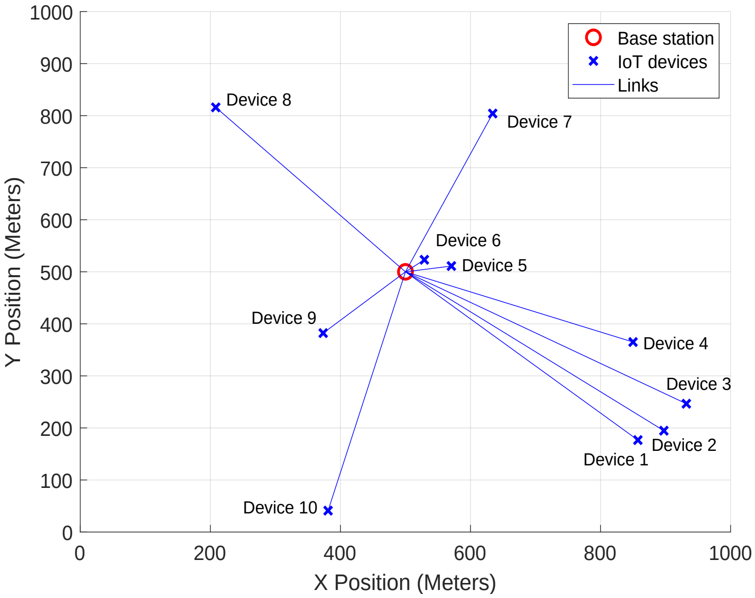


Figure 6.6: Simulation scenario of the proposed scheme.

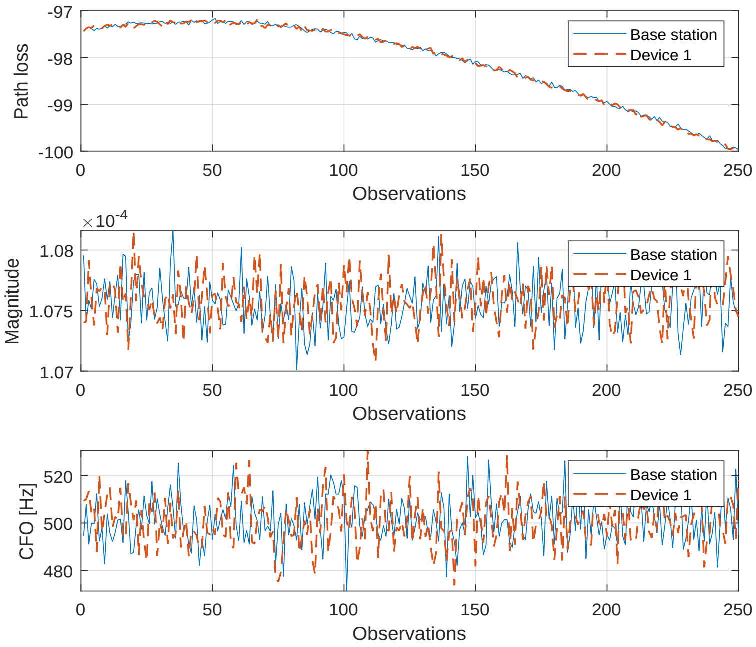


Figure 6.7: Observations of physical layer attributes used at base station and Device 1.

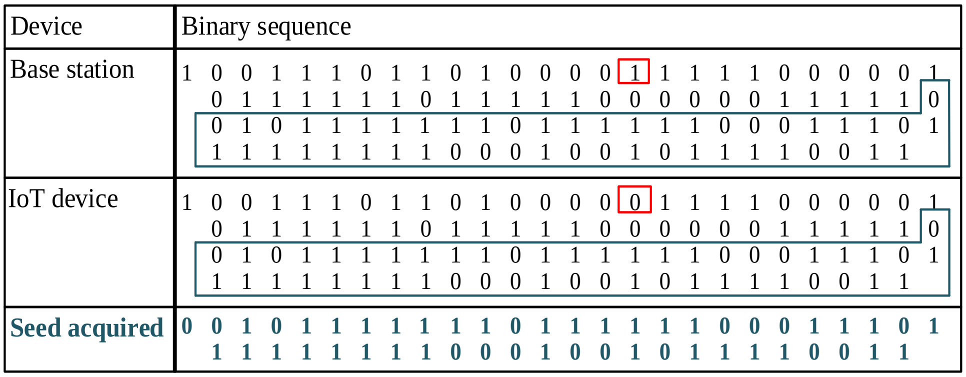
as

$$h_{IR}(\tau; t) = \sum_{i=1}^{I} A_i(t)\delta(\tau - i\Delta\tau), \tag{6.18}$$

where I is the number of multipath propagation paths, $i\Delta\tau$ and A_i represent the delay and complex amplitude of the i-th multipath component, respectively. According to [118], the path loss model is given as

$$PL = 22.7\log_{10}(d[m]) + 41 + 20\log_{10}(\frac{f_c[GHz]}{5}), \tag{6.19}$$

where $d[m]$ is the distance between each pair of transceiver in meters.



Device	Binary sequence

Base station	1 0 0 1 1 1 0 1 1 0 1 0 0 0 0 1 1 1 1 1 0 0 0 0 0 1
	0 1 1 1 1 1 1 0 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 0
	0 1 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1
	1 1 1 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 0 0 1 1

IoT device	1 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1
	0 1 1 1 1 1 1 0 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 0
	0 1 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1
	1 1 1 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 0 0 1 1

Seed acquired	**0 0 1 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1** **1 1 1 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 0 0 1 1**

Figure 6.8: Initial binary sequences obtained (100 bits) at the base station and Device 1 in Phase II of the developed seed acquisition technique, as well as the unique seed acquired (50 bits) in the proposed scheme.

The observations at the base station and Device 1 are given in Figure 6.7. The initial 100 observations of these attributes are used to derive the optimal boundary given in Theorem 1, namely for $(R^{*2}, \boldsymbol{c}^{*})$, where the estimates of three-dimensional training samples are divided into two sets, i.e., inside the sphere and outside the sphere. To be specific, those estimates inside the sphere are set to 1, while the remaining estimates are set to 0. Then, the initial binary sequences in Phase II of the developed seed acquisition technique (please see Figure 6.4) can be obtained. The initial binary sequences of the base station and first IoT device are shown in Figure 6.8. In the quantization Phase, 63 bits of '1' are obtained at the base station, while 62 bits are generated at the IoT device because of the imperfect estimates and different estimation times at the base station and IoT device. Through the verification phase of the developed seed acquisition technique, a 50 bits seed is acquired in the implementation as shown in Figure 6.8. Finally, a PRBS with 500 bits is generated by this seed for the authentication between the base station and this IoT device. To be more specific, only when the access time sequence of this IoT device is identical to the pre-agreed PRBS, it will be identified as a legitimate device. Otherwise, it will be authenticated as a spoofer.

6.4.2 Comparison Results

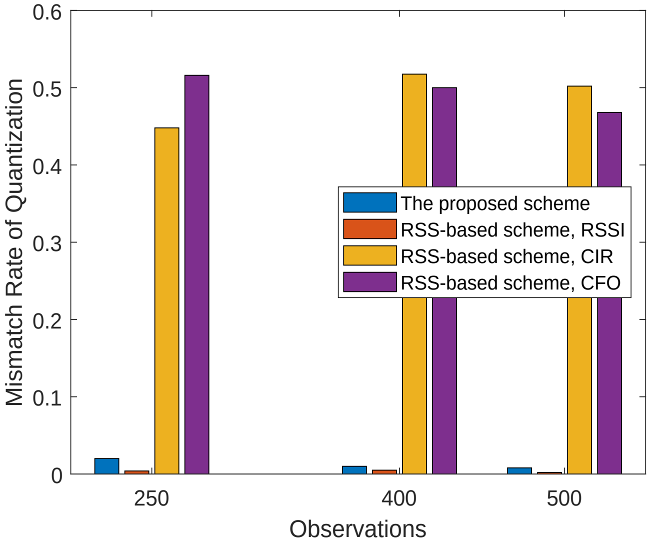


Figure 6.9: Comparison results between RSS-based quantization method of [175] and the proposed SVM-based quantization method.

The comparison results between the RSS-based quantization method of [175] and the proposed SVM-based quantization method are depicted in Figure 6.9 assuming that 250, 400, and 500 observations of physical layer features are used. The proposed SVM-based quantization method utilizes RSSI, CIR, and CFO, while the RSS-based quantization method only uses one physical layer attribute. As it is shown in Figure 6.9, the mismatch rate of the RSS-based quantization method of [175] utilizing RSSI is slightly lower than that of the proposed quantization method, while the mismatch rates of other cases (i.e., utilizing CIR or CFO) are much higher that of the proposed SVM-based quantization method. The reason is that the proposed SVM-based quantization method derives an optimal boundary, while the RSS-based quantization method only applies a fixed threshold for quantization. Moreover, since the RSSI changes faster than the other physical layer attributes (see Figure 6.7), the fixed threshold in the RSS-based quantization method can achieve a smaller mismatch rate. However, this highly depends on both the physical environment and physical layer attribute used, and this method suffers from very low seed bit randomness. Hence, the generated seed could be easily compromised by spoofers.

Authentication schemes	Physical layer key generation scheme	Our scheme
Characteristic	Static and one time	Continuous
Key/seed generation rate requirement	High	Low
Key/seed transmission (privacy leakage)	√	×
Channel probing	√	√
Quantization	√	√
Information reconciliation/ verification	√	√
Privacy amplification	√	×
PRBS generation	×	√
Time Complexity for $\mathcal{N}$ times of authentication	$O(\mathcal{N})$	$O(1)$

Figure 6.10: Comparison results between the proposed scheme and the physical layer key generation schemes of [174, 175, 176, 177, 178].

Figure 6.10 characterizes the comparison results between the physical layer key generation schemes of [174, 175, 176, 177, 178] and the proposed scheme. It can be observed from Figure 6.10 that the schemes of [174, 175, 176, 177, 178] are static in time and one-time authentication, while the proposed scheme achieves continuous identification of multiple IoT devices in the time-domain. To achieve security enhancement, the high key generation rate is required in the schemes of [174, 175, 176, 177, 178], but it is not required in the proposed scheme. Furthermore, the seed transmission is not required in the proposed scheme, thus resulting in privacy protection of the obtained seed. On the contrary, the physical layer key generation schemes need the key transmission during the process, which leads to the potential key leakage. More importantly, the time complexity for $\mathcal{N}$ times of authentication in the proposed scheme is much lower than that of the schemes of [174, 175, 176, 177, 178], where $\mathcal{N}$ represents the number of authentication times between the transceiver pair. In a nutshell, the proposed scheme achieves higher security performance and continuous protection for legitimate devices as well as lower time complexity.

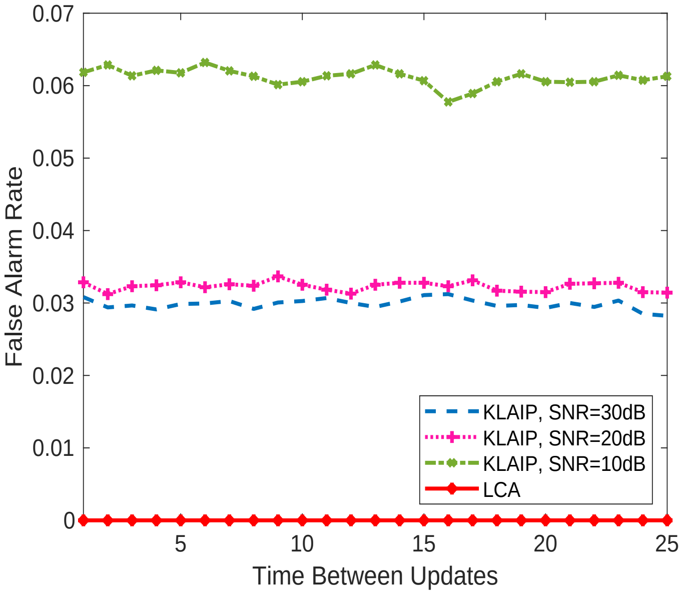


Figure 6.11: False alarm comparison results between the Kernel Learning-based Authentication as an Intelligent Process (KLAIP) scheme of [2] and the proposed Lightweight Continuous Authentication (LCA) scheme.

The false alarm comparison results between the proposed scheme and the scheme of [2] with respect to SNR=30dB, 20dB, and 10dB are characterized in Figure 6.11. Due to the verification phase designed in the developed seed acquisition technique, an identical seed is acquired at both the base station and IoT device sides for PRBS generation. To be specific, the PRBS generated in the proposed scheme for authentication between an IoT device and base station pair is unique and identical. Therefore, the false alarm events can be avoided in the proposed lightweight continuous authentication scheme. However, the false alarm events are inevitable in the scheme of [2] due to the imperfect and time-varying estimates of the physical layer attributes encountered, although the kernel machine learning approach is explored for tracking the attributes to achieve continuous authentication. Lower SNR could lead to a higher false alarm rate in the scheme of [2], since its performance relies on the observations of physical layer attributes used.

Figure 6.12 characterizes the misdetection rate of the proposed scheme with respect to S-

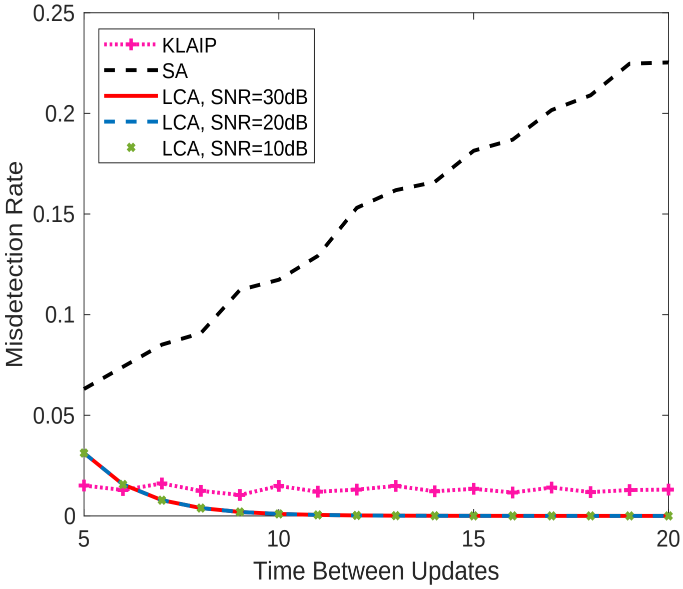


Figure 6.12: Misdetection comparison results of the Kernel Learning-based Authentication as an Intelligent Process (KLAIP) scheme of [2], Static Authentication (SA) scheme, and the proposed Lightweight Continuous Authentication (LCA) scheme.

NR=30dB, 20dB, and 10dB. With the increase of access time slots, the misdetection rate of the proposed LCA scheme significantly decreases because it is more difficult for the spoofer to predict more access time slots of the legitimate IoT devices. More importantly, it can be observed from Figure 6.12 that the misdetection rates of the proposed scheme remain unchanged with the decrease of SNR. The reason for this trend is that the authentication of the proposed scheme depends on the identification of the access time sequences of the IoT devices and the verification phase designed. Hence, the proposed scheme is robust in the noisy wireless communication environment. Figure 6.12 also demonstrates that the continuous authentication schemes, including the KLAIP scheme of [2] and the proposed LCA scheme, perform better than the static authentication scheme because they adapt to the time-varying communication environment. More importantly, the proposed scheme performs best after a few time slots, typically less than 6, and does not require a complex system parameter update scheme, resulting in a lightweight solution.

Figure 6.13 characterizes the computation overhead comparison between the proposed Lightweight Continuous Authentication (LCA) scheme and the schemes of [39], i.e., Incremental Aggregated Gradient (IAG), Frank-Wolfe (FW), and distributed Frank-Wolfe (dFW). The

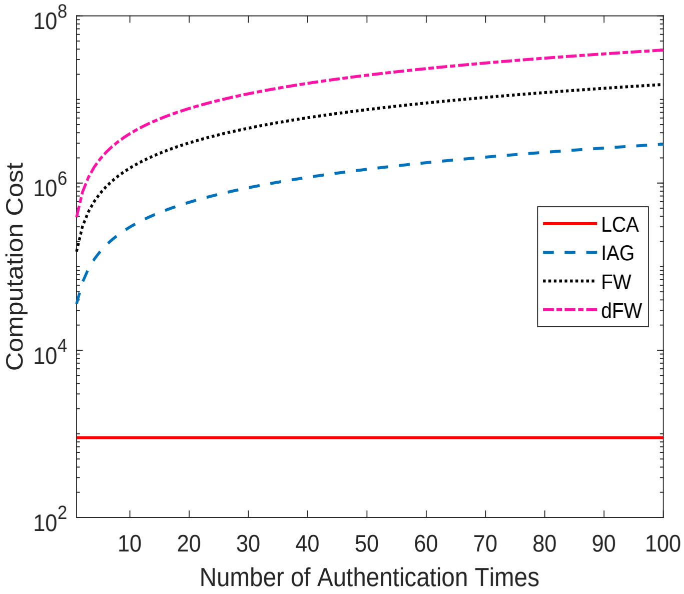


Figure 6.13: Computation cost comparison between the proposed Lightweight Continuous Authentication (LCA) scheme and the schemes of [39], namely IAG, FW, and dFW.

total computation overhead of the schemes of [39] is according to the Lemma 4 of [39]. Explicitly, the schemes of [39] are static and one-time authentication solutions requiring the help of landmarks for collecting RSSI of signals, while the proposed LCA scheme is continuous. The computation overhead of the proposed LCA scheme stays stable as $O(\max(J,N)\min(J,N)^2)$ [192, 193] with the increase of authentication times, which is 900 in this case. Note that the computation is required to obtain the optimal boundary for quantization in the proposed LCA scheme. The designed optimal boundary can be used for generating multiple PRBSs for authentication, where each PRBS containing 500 bits representing 500 authentication times. The schemes of [39] require the iterations to reach optimal solutions, thus leading to much higher computation overhead compared with the proposed scheme with the increase of authentication times. By calculating 15 iterations in IAG, FW, and dFW, their computation overhead values are 35758, 151140, and 389940 runs for only one authentication, respectively. With the increase of authentication, the computation overhead values of the schemes of [39] increase linearly.

6.5 Chapter Summary

In this chapter, a lightweight continuous authentication scheme was proposed by identifying the pre-arranged pseudo-random access time sequences of the IoT devices in 5G-and-beyond networks. First, a new seed acquisition technique was developed for generating identical PRBSs between each pair of the base station and IoT device by utilizing channel reciprocity. Second, a SVM-based method was explored to derive an optimal boundary for quantizing the estimates of physical layer attributes into bits, so that the bit mismatch rate can be reduced, while the seed bit randomness is guaranteed. Then, if the access time sequence of an IoT device is identical to its pre-agreed PRBS, it will be authenticated as a legitimate device by the base station. Finally, the proposed scheme was verified by comparing it with state-of-the-art schemes to demonstrate its superior performance in quantization, authentication, and computation cost.

Through identifying the access sequences of IoT devices in the time domain, the authentication between multiple devices and the base station could be significantly simplified. Similarly, different access methods, e.g., in the frequency domain, the power domain, and the code domain, can be developed for authentication in the future works. Moreover, by intelligently design the authentication method in multiple domains, the security performance and communication performance will be improved.

Chapter 7

Conclusion and Future Work

This chapter presents the conclusion of this thesis. Some future works are also presented in this chapter.

7.1 Conclusion

In this thesis, two multi-dimensional adaptive physical-layer authentication schemes were firstly proposed based on AI techniques as an intelligent process to learn and utilize the time-varying and imperfectly estimated communication link attributes, i.e., the kernel learning-based scheme and fuzzy learning-based scheme. In the former scheme, a kernel-based fusion model was designed to deal with the multiple attributes without knowledge of their statistical properties. The authentication was developed as a linear convex model, which greatly reduces authentication complexity. In the latter scheme, fuzzy functions were explored to characterize the multiple physical-layer attributes with imperfectness and uncertainties as parametric models. A hybrid learning-based adaptive algorithm was proposed to near-instantaneously update the authentication parameters. These two schemes both act as an intelligent process to tackle the variations of the utilized attributes and hence to improve the reliability and robustness of the authentication.

An adaptive trust management based soft authentication and progressive authorization scheme was proposed by intelligently exploiting the time-varying communication link-related attributes. Through evaluating the selected attributes, the trust relationships between transceivers were established. To dynamically update the trust level of the transmitter, an online conformal prediction-based adaptive trust adjustment algorithm was proposed relying on the real-time validation of attributes estimated at the receiver, resulting in soft security and progressive authorization.

A privacy-preserved distributed access control scheme based on accountable recommendation was proposed for blockchain-enabled IoT systems. In the recommendation mechanism, multiple authorized devices were utilized as referrers to authenticate a public device and issue the required credential for joining the system. Then, the anonymous credential generation strategy was developed to further achieve privacy protection, and the reputation update mechanism was proposed to evaluate the behaviors of the authorized devices.

Finally, to meet the stringent and diverse security requirements of 5G-and-beyond systems, a lightweight continuous authentication scheme was proposed for identifying multiple resource-constrained IoT devices via their pre-arranged pseudo-random access time sequences. A transmitter will be authenticated as legitimate if and only if its access time-sequential order is matched with a pre-agreed unique pseudo-random binary sequence (PRBS) between itself and the base station. The seeds for generating PRBS between each transceiver pair were determined by exploiting the channel reciprocity and by applying Support Vector Machine (SVM) algorithm. Through the proposed scheme, seamless protection for legitimate communications can be achieved without incurring long latency, complex computation, and high communication overhead.

7.2 Future Work

With the rapidly increasing number of intelligent devices used in 5G-and-beyond networks, there are also many other perspectives and areas in which AI can play a remarkable role and improve the quality of human lives. A range of future research ideas on AI for intelligent security and smart services in future wireless communications can be summarized as follows.

The AI techniques may be utilized for other security applications, such as anomaly/ fault/ intrusion detection, access control, and authorization. This is mainly due to their ability to provide continuous protection for legitimate communications in 5G-and-beyond networks. Furthermore, with the ongoing convergence between wireless devices and human beings, machine learning provides a new insight for studying human-device interaction, and the interplay between devices and information security, as well as the database security and data mining, operation systems security, Internet and cyber-security, incident handling, hacking, biometric techniques, smart cards, infrastructure protection, and risk management. Through identifying and learning the dynamic adversarial systems, automatic security management may be achieved by machine learning techniques.

With the fast development of distributed communication systems (e.g., blockchain), machine learning may facilitate distributed security management. To be specific, it may be explored for inferring the mobile users' decision making and device's dynamic states under unknown network conditions for better security performance, for example, adversarial behaviors study for predicting the possible attacks of adversaries in peer-to-peer networks. The family of machine learning algorithms may be also applied for better decision making, such as resource allocation, distributed computing, analytical thinking, customer orientation, strategy, and planning. These are expected to be extremely important for 5G-and-beyond wireless networks to achieve intelligent and autonomous services for human beings.

The design of more effective machine learning and distributed machine learning algorithms is also beneficial for wireless communication applications and security provisioning. Statistical learning methods ranging from a simple calculation of averages to the construction of complex models may be utilized, such as Bayesian learning and maximum-likelihood learning. Some AI techniques may be also explored for reducing the dimensionality of authentication and authorization systems, such as principal component analysis.

Considering that the insider attacks caused by adversaries who have passed the authentication may cause cascaded damages to large-scale IoT systems, the game theory may be also utilized for defending against insider attacks through modelling the behaviors of attackers. Some typical game models for studying interactions between legitimate devices and adversaries include the potential game, Stackelberg game, and evolutionary game, just to name a few. The incentive mechanism and punishment mechanism can be designed for achieving security enhancement and cooperations among untrusted entities in smart applications.

For resource allocation problems, the game theory, auction theory, and reinforcement learning can be explored to achieve better decision making. The interactions among devices can be modeled based on game theory, so that cooperations can be consummated by searching its equilibrium based on learning algorithms. Auction theory, such as ascending-bid auctions and descending-bid auctions, may be utilized for modeling the resource competitions among multiple entities in 5G-and-beyond networks, so that the reliable "market" may be built for wireless communication applications.

Bibliography

[1] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun. Mag.*, vol. 24, no. 2, pp. 98-105, 2018.

[2] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp: 2260-2273, 2019.

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682-3722, 2019.

[4] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G-and-beyond wireless networks," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 55-61, 2019.

[5] S. Zhang, S. Liu, V. Sharma, and P. K. Varshney, "Optimal sensor collaboration for parameter tracking using energy harvesting sensors," *IEEE Trans. Signal Process.*, vol. 66, no. 12, pp. 3339-3353, 2018.

[6] J. Zhou, Z. Liu, J. Li, and G. Zhang, "The effects of collaboration with different partners: A contingency model," *IEEE Trans. Eng. Manag.*, DOI: 10.1109/TEM.2020.2983067, 2020.

[7] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453-3495, 2018.

[8] Hyperledger whitepaper. Accessed July 20, 2020, [Online]: https://www.slideshare.net/milkers/hyperledger-whitepaper-77604132.

[9] K. Govindan and P. Mohapatra, “Trust computations and trust dynamics in mobile Adhoc networks: a survey,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279-295, 2012.

[10] D. Eckhoff and I. Wagner, “Privacy in the smart cityApplications, technologies, challenges, and solutions,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489-516, 2018.

[11] I. Farris, T. Taleb, Y. Khettab, and J. Song, “A survey on emerging SDN and NFV security mechanisms for IoT systems,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812-837, 2019.

[12] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196-248, 2019.

[13] H. Fang, X. Wang, and L. Hanzo, “Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes,” *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2607-2620, 2020.

[14] H. Fang, A. Qi, and X. Wang, “Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement?” *IEEE Network*, Accepted, to be appeared, 2020.

[15] Y. Qu, S. Yu, L. Gao, W. Zhou, and S. Peng, “A hybrid privacy protection scheme in cyber-physical social networks,” *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 3, pp. 773-784, 2018.

[16] W. Jiang, J. Wu, F. Li, G. Wang, and H. Zheng, “Trust evaluation in online social networks using generalized network flow,” *IEEE Trans. Computer*, vol. 65, no. 3, pp. 952-963, 2016.

[17] G. Theodorakopoulos and J. S. Baras, “On trust models and trust evaluation metrics for ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 318-328, 2006.

[18] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, “A survey on security aspects for 3GPP 5G networks,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170-195, 2020.

[19] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602-622, 2016.

[20] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236-262, 2016.

[21] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks,* vol. 21, no. 6, pp. 1835-1846, 2015.

[22] M. Iwamoto, K. Ohta, and J. Shikata, "Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654-685, 2018.

[23] Y. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1082-1091, 2017.

[24] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, "Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463-8476, 2016.

[25] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152-158, 2016.

[26] T. R. Halford, T. A. Courtade, K. M. Chugg, X. Li, and G. Thatte, "Energy-efficient group key agreement for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5552-5564, 2015.

[27] N. Li , D. Liu, and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Trans. Sustainable Computing*, vol. 2, no. 4, pp. 359-370, 2017.

[28] T. Mick, R. Tourani, and S. Misra, “LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 755-764, 2018.

[29] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, “2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896-911, 2016.

[30] X. Duan and X. Wang, “Authentication handover and privacy protection in 5G HetNets using software-defined networking,” *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28-35, 2015.

[31] X. Wu, Z. Yang, C. Ling, and X. Xia, “Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611-6625, 2016.

[32] P. L. Yu, J. S. Baras, and B. M. Sadler, “Physical-layer authentication,” *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38-51, 2008.

[33] P. L. Yu and B. M. Sadler, “MIMO authentication via deliberate fingerprinting at the physical layer,” *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 606-615, Sep. 2011.

[34] N. Xie and C. Chen, “Slope authentication at the physical layer,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1579-1594, 2018.

[35] J. Liu and X. Wang, “Physical layer authentication enhancement using two-dimensional channel quantization,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171-4182, 2016.

[36] G. Caparra, M. Centenaro, N. Laurenti, S. Tomasin, and L. Vangelista, “Energy-based anchor node selection for IoT physical layer authentication,” *in Proc. IEEE International Conference on Communications (ICC),* 2016.

[37] W. Hou, X. Wang, J. Chouinard, and A. Refaey, “Physical layer authentication for mobile systems with time-varying carrier frequency offsets,” *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658-1667, 2014.

[38] W. Wang, Y. Chen, and Q. Zhang, “Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1218-1225, 2016.

[39] L. Xiao, X. Wan, and Z. Han, “PHY-layer authentication with multiple landmarks with reduced overhead,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676-1687, 2018.

[40] A. A. D’Amico, L. Marchetti, M. Morelli, and M. Moretti, “Frequency estimation in OFDM direct-conversion receivers using a repeated preamble,” *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1246-1258, 2016.

[41] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, “On the error region for channel estimation-based physical layer authentication over Rayleigh fading,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 941-952, 2015.

[42] P. Baracca, N. Laurenti, and S. Tomasin, “Physical layer authentication over MIMO fading wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564-2573, 2012.

[43] K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks,” *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56-62, 2010.

[44] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, “Wireless physical-layer identification: modeling and validation,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091-2109, 2016.

[45] V. Kumar, J. Park, and K. Bian, “PHY-layer authentication using duobinary signaling for spectrum enforcement,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1027-1038, 2016.

[46] F. Zhu, B. Xiao, J. Liu, and L. Chen, “Efficient physical-layer unknown tag identification in large-scale RFID systems,” *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 283-295, 2016.

[47] H. Fang, L. Xu, Y. Zou, X. Wang, and K.-K. R. Choo, “Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication,” *IEEE Trans. Veh. Technol.,* vol.67, no.11, pp. 10788-10799, 2018.

[48] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. C. Mason, “Continuous physical layer authentication using a novel adaptive OFDM system,” *in Proc. IEEE International Conference on Communications (ICC)*, 2011.

[49] X. Wu and Z. Yang, “Physical-Layer Authentication for Multi-Carrier Transmission,” *IEEE Commun. Lett.*, vol. 19, no. 1, 2015, pp. 74-77.

[50] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, “LIVE: Lightweight integrity verification and content access control for named data networking,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 308-320, 2015.

[51] M. A. Rahman and E. S. Al-Shaer, “Automated synthesis of distributed network access controls: A formal framework with refinement,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 2, pp. 416-430, 2017.

[52] M. Khan, P. Ginzboorg, K. Jrvinen, and V. Niemi, “Defeating the downgrade attack on identity privacy in 5G,” in *Proc. Int. Conf. Res. Security Standardisation*, 2018, pp. 95-119.

[53] A. Castiglione et al., “Hierarchical and shared access control” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 850-865, 2016.

[54] M. Ion, J. Zhang, and E. M. Schooler, “Toward content-centric privacy in ICN: Attribute-based encryption and routing,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 513-514, 2013.

[55] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, “5G privacy: Scenarios and solutions,” in *Proc. IEEE 5G World Forum (5GWF)*, 2018, pp. 197-203.

[56] W. D. de Mattos and P. R. L. Gondim, “M-health solutions using 5G networks and M2M communications,” *IT Prof.*, vol. 18, no. 3, pp. 24-29, 2016.

[57] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight authentication and key agreement for smart metering in smart energy networks,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349-4359, 2019.

[58] J. Soria-Comas, J. Domingo-Ferrer, D. Snchez, and D. Megas, “Individual differential privacy: A utility-preserving formulation of differential privacy guarantees,” *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1418-1429, 2017.

[59] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, “Location and trajectory privacy preservation in 5G-enabled vehicle social network services,” *J. Netw. Comput. Appl.*, vol. 110, pp. 108-118, 2018.

[60] B. Gedik and Ling Liu, “Protecting location privacy with personalized k-anonymity: Architecture and algorithms,” *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1-18, 2008.

[61] R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, and J.-P. Seifert, “LTE and IMSI catcher myths,” in *Proc. BlackHat Europe*, 2015, pp. 1-5.

[62] C.-H. Tai, P.-J. Tseng, P. S. Yu, and M.-S. Chen, “Identity protection in sequential releases of dynamic networks,” *IEEE Trans. Knowledge and Data Eng.*, vol. 26, no. 3, pp. 635-651, 2014.

[63] K. S. Cook, Trust in Society, vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York.

[64] M. Blaze, J. Feigenbaum, and J. Lacy, “Decentralized trust management,” in *Proc. IEEE Symposium on Security and Privacy*, 1996, pp. 164-173.

[65] J.-H. Cho, A. Swami, and I.-R. Chen, “A survey on trust management for mobile ad hoc networks,” *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562-583, 2011.

[66] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671-2701, 2019.

[67] J. S. Baras and T. Jiang, “Managing trust in self-organized mobile ad hoc networks,” in *Proc. 12th Annual Network and Distributed System Security Symposium Workshop*, 2005, San Diego, CA.

[68] H. Li and M. Singhal, “Trust management in distributed systems,” *Computers*, vol. 40, no.2, pp. 45-53, 2007.

[69] E. Aivaloglou, S. Gritxalis, and C. Skianis, “Trust establishment in ad hoc and sensor networks,” in *Proc. 1st Int’l Workshop on Critical Information Infrastructure Security, Lecture Notes in Computer Science*, vol. 4347, pp. 179-192, 2006, Samos, Greece.

[70] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Trans. Netw. Service Management*, vol. 9, no. 2, pp. 169-183, 2012.

[71] I.-R. Chen , J. Guo, D.-C. Wang, J. J. P. Tsai, H. Al-Hamadi , and I. You, “Trust-based service management for mobile cloud IoT systems,” *IEEE Trans. Netw. Service Management*, vol. 16, no. 1, pp. 246-263, 2019.

[72] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, “A novel approach to trust management in unattended wireless sensor networks,” *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1409-1423, 2014.

[73] G. Han, J. Jiang, L. Shu, and M. Guizani, “An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network,” *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447-2459, 2015.

[74] S. Russell and P. Norvig, “Artificial intelligence: A modern approach,” Pearson Education, Inc., Upper Saddle River, New Jersey, 2010.

[75] N. Wang, T. Jiang, S. Lv, and L. Xiao, “Physical-layer authentication based on extreme learning machine,” *IEEE Commun. Letters*, vol. 21, no. 7, pp. 1557-1560, 2017.

[76] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, “Machine learning methods for attack detection in the smart grid,” *IEEE Trans. Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773-1786, 2015.

[77] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?” *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41-49, 2018.

[78] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037-10047, 2016.

[79] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

[80] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relay based physical layer security improvement: a single-leader multiple-follower Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197-209, 2018.

[81] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171-4182, 2016.

[82] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948-5956, 2009.

[83] W. Liu, J. C. Principe, and S. Haykin, "Kernel adaptive filtering: a comprehensive introduction," John Wiley and Sons, pp. 16-98, 2010.

[84] K. Li and J. C. Principe, "Tranfer learning in adaptive filters: the nearest instance centroid-estimation kernel least-mean-square algorithm," *IEEE Trans. Signal Process.*, vol. 65, no. 24, pp. 6520-6535, 2017.

[85] R. Boloix-Tortosa, J. J. Murillo-Fuentes, I. Santos, and F. Perez-Cruz, "Widely linear complex-valued kernel methods for regression," *IEEE Trans. Signal Process.*, vol. 65, no. 19, pp. 5240-5248, 2017.

[86] B. Chen, L. Xing, B. Xu, H. Zhao, N. Zheng, and J. C. Principe, "Kernel risk-sensitive loss: Definition, properties, and application to robust adaptive filtering," *IEEE Trans. Signal Process.*, vol. 65, no. 11, pp. 2888-2901, 2017.

[87] J. Liu, P. C. Cosman, and B. D. Rao, "Robust linear regression via l_0 regularization," *IEEE Trans. Signal Process.*, vol. 66, no. 3, pp. 698-713, 2018.

[88] G. D. Finlayson, M. Mackiewicz, and A. Hurlbert, "Color correction using root-polynomial regression," *IEEE Trans. Image Process.*, vol. 24, no. 5, pp. 1460-1470, 2015.

[89] X. Tan, C. Sun, and T. D. Pham, "Edge-aware filtering with local polynomial approximation and rectangle-based weighting," *IEEE Trans. Cybern.,* vol. 46, no. 12, pp. 2693-2705, 2016.

[90] L. Yang, L. Zhao, G. Bi, and L. Zhang, "SAR ground moving target imaging algorithm based on parametric and dynamic sparse Bayesian learning," *IEEE Trans. Geosci. Remote Sens.,* vol. 54, no. 4, pp. 2254-2267, 2016.

[91] Y. Li, W. Dong, X. Xie, G. Shi, J. Wu, and X. Li, "Image super-resolution with parametric sparse model learning," *IEEE Trans. Image Process.,* vol. 27, no. 9, pp. 4638-4650, 2018.

[92] X. Shen and Y. Gu, "Nonconvex sparse logistic regression with weakly convex regularization," *IEEE Trans. Signal Process.*, vol. 66, no. 12, pp. 3199-3211, 2018.

[93] S. Wang, Z. Bao, J. S. Culpepper, T. Sellis, and G. Cong, "Reverse k nearest neighbor search over trajectories," *IEEE Trans. Knowledge and Data Eng.*, vol. 30, no. 4, pp. 757-771, 2018.

[94] Y.-C. Cheng and Pi-Chung Wang, "Packet classification using dynamically generated decision trees," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 582-586, 2015.

[95] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: a compact and robust approach," *IEEE Trans. Wireless Commun.*, doi: 10.1109/TWC.2020.2993175, 2020.

[96] T. K. Sarkar, M. Salazar-Palma, and E. L. Mokole, "Application of the principle of analytic continuation to interpolate/extrapolate system responses resulting in reduced computations: Part B: nonparametric methods," *IEEE J. Multiscale Multiphys. Comput. Techn.*, vol. 1, pp. 60-72, 2016.

[97] F. Doshi-Velez, D. Pfau, F. Wood, and N. Roy, “Bayesian nonparametric methods for partially-observable reinforcement learning,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, no. 2, pp. 394-407, 2015.

[98] H. Zhan, Z. Q. Zhu, and M. Odavic, “Nonparametric sensorless drive method for open-winding PMSM based on zero-sequence back EMF with circulating current suppression,” *IEEE Trans. Power Electron.*, vol. 32, no. 5, pp. 3808-3817, 2017.

[99] H. Xu, W. Wang, and Y. Qian, “Fusing complete monotonic decision trees,” *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 10, pp. 2223-2235, 2017.

[100] Z. Jiang, S. Shekhar, X. Zhou, J. Knight, and J. Corcoran, “Focal-test-based spatial decision tree learning,” *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 6, pp. 1547-1559, 2015.

[101] T. K. Sarkar, M. Salazar-Palma, and E. L. Mokole, “Application of the principle of analytic continuation to interpolate/extrapolate system responses resulting in reduced computations: Part A: Parametric methods,” *IEEE J. Multiscale Multiphys. Comput. Techn.*, vol.1, pp. 48-59, 2016.

[102] A. Kadu, T. Van Leeuwen, and W. A. Mulder, “Salt reconstruction in full-waveform inversion with a parametric level-set method,” *IEEE Trans. Comput. Imag.*, vol. 3, no. 2, pp. 305-315, 2017.

[103] M. Brell, C. Rogass, K. Segl, B. Bookhagen, and L. Guanter, “Improving sensor fusion: a parametric method for the geometric coalignment of airborne hyperspectral and lidar data,” *IEEE Trans. Geosci. Remote Sens.*, vol. 54, no. 6, pp. 3460-3474, 2016.

[104] S. Liu, J. Zhang, Y. Xiang, and W. Zhou, “Fuzzy-based information decomposition for incomplete and imbalanced data learning,” *IEEE Trans. Fuzzy Syst.*, vol. 25, no. 6, pp. 1476-1490, 2017.

[105] Y. Tian, M. Sun, Z. Deng, J. Luo, and Y. Li, “A new fuzzy set and nonkernel SVM approach for mislabeled binary classification with applications,” *IEEE Trans. Fuzzy Syst.*, vol. 25, no. 6, pp. 1536-1545, 2017.

[106] C. Gu, W. Yang, Y. Song, and F. Li, “Distribution network pricing for uncertain load growth using fuzzy set theory,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1932-1940, 2016.

[107] H. Sun, H. Zhao, K. Huang, M. Qiu, S. Zhen, and Y.-H. Chen, “A fuzzy approach for optimal robust control design of an automotive electronic throttle system,” *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 2, pp. 694-704, 2018.

[108] W. Nicolas, “Fuzzy classification of online customers,” Springer, pp. 7-26, 2015.

[109] W. Wang, Y. Liang, E. P. Xing, and L. Shen, “Nonparametric decentralized detection and sparse sensor selection via weighted kernel,” *IEEE Trans. Signal Process.*, vol. 64, no. 2, pp. 306-321, 2016.

[110] B. Scholkopf and A. Smola, “Learning with kernels,” Cambridge, MA, USA: MIT Press, 2002.

[111] W. Hrdle, “Applied nonparametric regression,” Cambridge, UK: Cambridge University Press, 1992.

[112] S. Haykin, “Adaptive filter theory, 4th edition,” Upper Saddle River, NJ: Prentice Hall, 2002.

[113] J. Jantzen, “Foundations of fuzzy control: a practical approach,” University of the Aegean at Chios, Wiley, pp. 53-84, 2013.

[114] X. Duan and X. Wang, “Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer,” in *Proc. of IEEE International Conference on Communications (ICC)*, 2016.

[115] J. R. Jang, C. T. Sun, and E. Mizutani, “Neuro-fuzzy and soft computing a computational approach to learning and machine intelligence,” Prentice Hall Upper Saddle River, NJ 07458, pp. 104-117, 1997.

[116] Y. Shi and M. A. Jensen, “Improved radiometric identification of wireless devices using MIMO transmission,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346-1354, 2011.

[117] P. Abouzar, D. G. Michelson, and M. Hamdi, “RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6638-6650, 2016.

[118] Kyosti, Pekka, Juha Meinila, et al. WINNER II Channel Models. D1.1.2 V1.2. IST-4-027756 WINNER II, 2007.

[119] K. S. Narendra and K. Parthasarathy, “Identification and control of dynamical systems using neural networks,” *IEEE Trans. Neural Netw.,* vol. 1, no. 1, pp. 4-27, 1990.

[120] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, “Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463-8476, 2016.

[121] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, “Passive attacks against searchable encryption,” *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 789-802, 2019.

[122] H. Fang, L. Xu, and X. Wang, “Coordinated multiple-relays based physical-layer security improvement: a single-leader multiple-followers Stackelberg game scheme,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197-209, 2018.

[123] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, “Physical layer security in heterogeneous cellular networks,” *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204-1219, 2016.

[124] D. Wang, B. Bai, W. Chen, and Z. Han, “Secure green communication via untrusted two-way relaying: a physical layer approach,” *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861-1874, 2016.

[125] Y. L. Sun, W. Yu, Z. Han, and K. J. Ray Liu, “Information theoretic framework of trust modeling and evaluation for Ad Hoc networks,” *IEEE J. Sel. Areas Commn.*, vol. 24, no. 2, pp. 305-316, 2006.

[126] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, “Trust-distortion resistant trust management frameworks on mobile Ad Hoc networks: a survey,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287-1309, 2016.

[127] X. Fan, L. Liu, M. Li, and Z. Su, “GroupTrust: dependable trust management,” *IEEE Trans. Parallel Distrib.*, vol. 28, no. 4, pp. 1076-1090, 2017.

[128] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, “Trust-based communication for the industrial internet of things,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16-22, 2018.

[129] P. Zhang, Y. Kong, and M. Zhou, “A domain partition-based trust model for unreliable clouds,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167-2178, 2018.

[130] H. Fang, L. Xu, and X. Huang, “Self-adaptive trust management based on game theory in fuzzy large-scale networks,” *Soft Computing*, vol. 21, no. 4, pp. 907-921, 2017.

[131] M. Zhao, J. Y. Ryu, J. Lee, T. Q. S. Quek, and S. Feng, “Exploiting trust degree for multiple-antenna user cooperation,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 4908-4923, 2017.

[132] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, “Secure routing based on social similarity in opportunistic networks,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594-605, 2016.

[133] T. C. Silva and L. Zhao, “Machine learning in complex networks,” Springer Cham Heidelberg New York Dordrecht London, pp. 71-82, 2016.

[134] H. Yang, Q. Yao, A. Yu, Y. Lee, and J. Zhang, “Resource assignment based on dynamic fuzzy clustering in elastic optical networks with multi-core fibers,” *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3457-3469, 2019.

[135] M. Gharbieh, A. Bader, H. ElSawy, H.-C. Yang, M.-S. Alouini, and A. Adinoyi, “Self-organized scheduling request for uplink 5G networks: A D2D clustering approach,” *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1197-1209, 2019.

[136] O. Ibidunmoye, A.-R. Rezaie, and E. Elmroth, “Adaptive anomaly detection in performance metric streams,” *IEEE Trans. Netw. Service Manag.*, vol. 15, no. 1, pp. 217-231, 2018.

[137] R. Laxhammar and G. Falkman, “Online learning and sequential anomaly detection in trajectories,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1158-1173, 2014.

[138] M. Dashevskiy and Z. Luo, “Network traffic demand prediction with confidence,” in *Proc. 2008 IEEE Global Telecommunications Conference (GLOBECOM)*, 2008.

[139] A. Lambrou, H. Papadopoulos, and A. Gammerman, “Reliable confidence measures for medical diagnosis with evolutionary algorithms,” *IEEE Trans. Inf. Technol. Biomed.*, vol. 15, no. 1, pp. 93-99, 2011.

[140] X. Lu, F. Yin, C. Liu, and M. Huang, “Online spatiotemporal extreme learning machine for complex time-varying distributed parameter systems,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1753-1762, 2017.

[141] S. Scardapane, D. Comminiello, M. Scarpiniti, and A. Uncini, “Online sequential extreme learning machine with kernels,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 9, pp. 2214-2220, 2015.

[142] V. Vovk, A. Gammerman, and G. Shafer, “Algorithmic learning in a random world,” New York, NS, USA: Springer-Verlag, Inc., 2005.

[143] G. Rhafer and V. Vovk, “A tutorial on conformal prediction,” *J. Mach. Learn. Res.*, vol. 9, pp. 371-421, 2008.

[144] J. Zhang, Z. Wang, X. Zheng, L. Guan, and C. Y. Chung, “Locally weighted ridge regression for power system online sensitivity identification considering data collinearity,” *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1624-1634, 2018.

[145] S. S. Mullick, S. Datta, and S. Das, “Adaptive learning-based k-nearest neighbor classifiers with resilience to class imbalance,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 11, pp. 5713-5725, 2018.

[146] E. Isufi, A. Loukas, A. Simonetto, and G. Leus, “Autoregressive moving average graph filtering,” *IEEE Trans. Signal Process.*, vol. 65, no. 2, pp. 274-288, 2017.

[147] R. Tourani, S. Misra, T. Mick, and G. Panwar, “Security, privacy, and access control in information-centric networking: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566-600, 2018.

[148] T. Chen, K. Lei, and K. Xu, “An encryption and probability based access control model for named data networking,” in *Proc. IEEE Int. Perform. Comput. Commun. Conf. (IPCCC)*, Austin, TX, USA, 2014, pp. 1-8.

[149] S. Singh, “A trust based approach for secure access control in information centric network,” *Int. J. Inf. Netw. Security*, vol. 1, no. 2, pp. 97-104, 2012.

[150] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, “A survey of trust and reputation management systems in wireless communications,” *Proc. IEEE*, vol. 98, no. 10, pp. 1755-1772, 2010.

[151] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182-8201, 2019.

[152] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you wanted to know about the blockchain: its promise, components, processes, and problems,” *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6-14, 2018.

[153] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690-3700, 2018.

[154] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” *arXiv preprint arXiv:1808.10228v1*, 2018.

[155] M. C. K. Khalilov and A. Levi, “A survey on anonymity and privacy in Bitcoin-like digital cash system,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543-2585, 2018.

[156] V. Buterin, “Ethereum white paper: a next generation smart contract and decentralized application platform,” Accessed Nov. 20, 2019, [Online]: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[157] M. Alaslani, F. Nawab, and B. Shihada, “Blockchain in IoT systems: End-to-end delay evaluation,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8332-8344, 2019.

[158] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, “Privacy-preserving support vector machine training over Blockchain-based encrypted IoT data in smart cities,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702-7712, 2019.

[159] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630-1638, 2017.

[160] M. Chlela, D. Mascarella, G. Jos, and M. Kassouf, “Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks,” *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702-4711, 2018.

[161] A. Boualouache, S-M. Senouci, and S. Moussaoui, “A survey on pseudonym changing strategies for vehicular Ad-Hoc networks,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770-790, 2018.

[162] O. Novo, “Scalable access management in IoT using Blockchain: A performance evaluation,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4694-4701, 2019.

[163] O. Novo, “Blockchain meets IoT: An architecture for scalable access management in IoT,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184-1195, 2018.

[164] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “Privacy-preserving advance power reservation,” *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 18-23, 2012.

[165] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An edge-IoT framework and prototype based on Blockchain and smart contracts," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4719-4732, 2019.

[166] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE J. Sel. Areas Commn.*, vol. 25, no. 8, pp. 1569-1589, 2007.

[167] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mob. Comput. Commun.*, vol. 5, no. 1, pp. 3-55, 2001.

[168] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2341-2381, 2017.

[169] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3567-3569, 2018.

[170] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of Drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64-69, 2018.

[171] J. Choi, "A coding approach with key-channel randomization for physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 175-185, 2019.

[172] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X.-Y. Li, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88-100, 2017.

[173] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327-1340, 2017.

[174] K. Zeng, "Physical layer key generation in wireless networks: challenge and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33-39, 2015.

[175] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835-1846, 2015.

[176] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842-1852, 2013.

[177] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779-1790, 2013.

[178] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1796-1806, 2016.

[179] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578-2588, 2016.

[180] R. Bonjour, S. Welschen, and J. Leuthold, "Time-to-space division multiplexing for Tb/s mobile cells," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4806-4818, 2018.

[181] J. Yu, Z. Chen, Y. Zhu, Y. Chen, L. Kong, and M. Li, "Fine-grained abnormal driving behaviors detection and identification with smartphones," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2198-2212, 2017.

[182] K. Gokcesu and S. S. Kozat, "Online anomaly detection with minimax optimal density estimation in nonstationary environments," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1213-1227, 2018.

[183] Z. Xiao, S. Shan, and L. Cheng, "Identification of cascade dynamic nonlinear systems: A bargaining-game-theory-based approach," *IEEE Trans. Signal Process.*, vol. 66, no. 17, pp. 4657-4669, 2018.

[184] Z. Xiao and X. Wang, “Nonlinear polynomial graph filter for signal processing with irregular structures,” *IEEE Trans. Signal Process.*, vol. 66, no. 23, pp. 6241-6251, 2018.

[185] X. Wu, W. Zuo, L. Lin, W. Jia, and D. Zhang, “F-SVM: Combination of feature transformation and SVM learning via convex relaxation,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 11, pp. 5185-5199, 2018.

[186] L. Lan, Z. Wang, S. Zhe, W. Cheng, J. Wang, and K. Zhang, “Scaling up kernel SVM on limited resources: A low-rank linearization approach,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 2, pp. 369-378, 2019.

[187] Y. Guo, X. Jia, and D. Paull, “Effective sequential classifier training for SVM-based multitemporal remote sensing image classification,” *IEEE Trans. Image Process.*, vol. 27, no. 6, pp. 3036-3048, 2019.

[188] M. Kafai and K. Eshghi, “CROification: Accurate kernel classification with the efficiency of sparse linear SVM,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 1, pp. 34-48, 2019.

[189] M. Mohri, A. Rostamizadeh, and A. Talwalkar, *Foundations of Machine Learning*. The MIT Press Cambridge, Massachusetts London, England, 2012.

[190] D. Zdenek, *Optimal Quadratic Programming Algorithms: With Applications to Variational Inequalities*. Boston, MA: Springer-Verlag US, 2009.

[191] P. H. Bardell, W. H. McAnney, and J. Savir, *Built-in Test for VLSI: Pseudorandom Techniques*. John Wiley and Sons, New York, 1987.

[192] O. Chapelle, “Training a support vector machine in the primal,” *Neural Computation*, vol. 19, no. 5, pp. 1155-1178, 2007.

[193] A. Bordes, S. Ertekin, J. Weston, and L. Bottou, “Fast kernel classifiers with online and active learning,” *Journal of Machine Learning Research*, vol. 6, no. 5, pp. 1579-1619, 2005.

[194] Z. Xiao, H. Fang, and X. Wang, “Nonlinear polynomial graph filter for anomalous IoT sensor detection and localization,” *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4839-4848, 2020.

Curriculum Vitae

Name:	He Fang
	Western University London, ON 2017 - 2020 Ph.D.
Post-Secondary Education and Degrees:	Fujian Normal University Fujian, China 2012 - 2017 Ph.D
Honours and Awards:	Ontario Graduate Scholarships, May 2020-April 2021. Ontario Graduate Scholarships, May 2019-April 2020. 2019 PSAC GTA Research Contribution Scholarship. 2019 Graduate Student Research Award Recipients. 2019 Graduate Student Award for Excellence in Research Recipients. Outstanding Engineer Award, Communication/Broadcast Chapter, IEEE London Section, 2019.
Related Work	Teaching Assistant of ‘Project Design’ Jan. 2020 - April 2020 Teaching Assistant of ‘Communication Theory’ Sep. 2018 - Dec. 2018 & Sep. 2019 - Dec. 2019 Teaching Assistant of ‘Digital Communication System’ Jan. 2019 - April 2019 Teaching Assistant of ‘Programming Fundamentals for Engineers’ Sep. 2017 - April 2018
Experience:	Vice-Chair of Communication/Broadcast Chapter, IEEE London Section, 2019. IEEE Globecom 2020 CQRM TPC member. Reviewer for IEEE Journals, e.g., IEEE Trans, Wireless Commun., IEEE Trans. Commun., IEEE Trans. Inf. Forensics Security, IEEE Internet of Things Journal.

Publications: (Selected articles from last three years)

Articles in Peer-Reviewed Journals:

[1] ***He Fang***, Xianbin Wang, and Li Xu, “Fuzzy learning for multi-dimensional adaptive physical layer authentication: a compact and robust approach,” ***IEEE Transactions on Wireless Communications***, vol. 19, no. 8, (2020): 5420-5432. (IF: 6.779)

[2] ***He Fang***, Xianbin Wang, and Lajos Hanzo, “Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes,” ***IEEE Transactions on Communications***, vol. 68, no. 4, (2020): 2607 - 2620. (IF: 5.646)

[3] ***He Fang***, Angie Qi, and Xianbin Wang, “Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement?” ***IEEE Network***, vol. 34, no. 3, (2020): 24-29. (IF: 8.808)

[4] ***He Fang***, Xianbin Wang, and Lajos Hanzo, “Learning-aided physical layer authentication as an intelligent process,” ***IEEE Transactions on Communications***, vol. 67, no. 3, (2019): 2260-2273. (IF: 5.646)

[5] ***He Fang***, Xianbin Wang, and Stefano Tomasin, “Machine learning for intelligent authentication in 5G-and-beyond wireless networks,” ***IEEE Wireless Communications***, vol. 26, no. 5, (2019): 55-61. (IF: 11.391)

[6] ***He Fang***, Li Xu, and Xianbin Wang, “Coordinated multiple relays based physical layer security improvement: a single leader-multiple followers Stackelberg game scheme,” ***IEEE Transactions on Information Forensics and Security***, vol. 13, no. 1, (2018): 197-209. (IF: 6.013)

[7] ***He Fang***, Li Xu, Yulong Zou, Xianbin Wang, and Kim-Kwang Raymond Choo, “Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication,” ***IEEE Transactions on Vehicular Technology***, vol.67, no.11, (2018): 10788-10799. (IF: 5.379)

[8] Zhenlong Xiao, ***He Fang****, and Xianbin Wang, “Nonlinear polynomial graph filter for anomalous IoT sensor detection and localization,” ***IEEE Internet of Things Journal***, vol. 7, no. 6, (2020): 4839-4848. (IF: 9.936)

[9] Chenbin Zhao, Li Xu, Jiguo Li, Feng Wang, and ***He Fang***, “Fuzzy identity-based dynamic

auditing of big data on cloud storage," ***IEEE Access***, vol. 7, (2019): 160459-160471. (IF: 3.745)

[10] Rushan Lin, Li Xu, and ***He Fang***, "Efficient physical layer key generation technique in wireless communications," ***EURASIP Journal on Wireless Communications and Networking***, (2020): 13. (IF: 1.408)

[11] Jiyang Bai, ***He Fang***, Junghoon Suh, Osama Aboul-Magd, Edward Au, and Xianbin Wang, "An adaptive grouping scheme in ultra-dense IEEE 802.11ax network using buffer state report based two-stage mechanism," ***China Communications***, vol. 16, no. 9, (2019): 31-44. (IF: 2.024)

Articles Under Review:

[12] ***He Fang***, Xianbin Wang, Nan Zhao, and Naofal Al-Dhahir, "Lightweight continuous authentication via intelligently arranged pseudo-random access in 5G-and-beyond," ***IEEE Transactions on Communications***, (2020): under review. (IF: 5.646)

[13] ***He Fang***, Xianbin Wang, Kan Zheng, and Li Xu, "Privacy-preserved distributed access control based on accountable recommendation for blockchain-enabled IoT systems," ***IEEE Transactions on Industrial Informatics***, (2020): under review. (IF: 9.112)

[14] Zhenlong Xiao, ***He Fang***, and Xianbin Wang, "Distributed nonlinear polynomial graph filter and its output graph spectrum-part I: Filter analysis and design," ***IEEE Transactions on Signal Processing***, (2020): under review. (IF: 5.028)

[15] Zhenlong Xiao, ***He Fang***, and Xianbin Wang, "Distributed nonlinear polynomial graph filter and its output graph spectrum-part II: Properties and applications," ***IEEE Transactions on Signal Processing***, (2020): under review. (IF: 5.028)

[16] Zhenlong Xiao, ***He Fang****, and Xianbin Wang, "Anomalous IoT sensor data detection: An efficient approach enabled by nonlinear frequency-domain graph analysis," ***IEEE Internet of Things Journal***, (2020): under review. (IF: 9.936)

[17] Chenbin Zhao, Li Xu, Jiguo Li, ***He Fang***, and Yinghui Zhang, "Towards:Secure and privacy-preserving cloud data sharing: Online/offline multi-authority CP-ABE with hidden policy," ***IEEE Transactions on Services Computing***, (2020): under review. (IF: 5.823)