12-1-2021 9:30 AM

Edge Intelligence Enabled Distributed and Collaborative Authentication in UAV Swarms

Huanchi Wang, *The University of Western Ontario*

Supervisor: Wang, Xianbin, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Electrical and Computer Engineering

Abstract

Unmanned Aerial Vehicles (UAVs) have been widely deployed in various fields with many benefits such as cost reduction, safety improvement and service coverage enhancement. Unlike the other mobile ad hoc networks, the UAV swarm, which is a flying ad hoc network, may operate in a hostile environment or experience rapid network topology change which brings high vulnerability by using cloud-based centralized security provisioning techniques. Hence, securing the UAV networks with the on-site authentication resources becomes a vital aspect to accomplish the mission. The on-site authentication resources, such as the cross-layer attributes, can be utilized to form a unique characteristic of each UAV. Alternatively, decentralized authentication techniques have also been considered where multiple collaborative nodes are utilized to fuse a final authentication decision. Although the decentralized authentication techniques usually have a better security performance, they may increase the computational overhead and decrease the efficiency. Hence, limiting the computational overhead becomes a critical challenge when designing more sophisticated authentication schemes for UAV swarms.

In this thesis, a linear discriminant analysis-based centralized authentication mechanism is first proposed to enhance the security performance with limited computational overhead by eliminating the non-informative attributes. Then, to compensate for the single-point failure of the centralized authentication schemes, a collaborative authentication mechanism is proposed to enhance the performance by utilizing the soft edge authentication decisions. Ultimately, we define a novel concept of Security-of-Service (SoS) which is further utilized to minimize the complexity of the collaborative authentication. Instead of utilizing all authentication resources to reach a maximized security performance which creates a higher overhead, the SoS aims to only promise the exact authentication requirement by utilizing a minimum amount of authentication resources. The simulation results demonstrate that our proposed scheme is robust across the changing environment and can fulfill the SoS with limited authentication resources.

Keywords: Cross-layer Security, Decentralized Authentication, Intelligent Authentication, Physical-layer Security, Unmanned Aerial Vehicles (UAVs)

Summary of Lay Audience

With reduced cost and growing capability, UAVs have become very popular for supporting many different applications. Rather than the single UAV enabled applications, emerging applications utilizing multiple UAVs, also known as a UAV swarm, have attracted increasing interest due to the better efficiency and reliability in different fields such as logistics as well as search and rescue. However, the potential security risks and attacks by malicious parties in such sensitive networks could lead to catastrophic consequences or cause avalanche-like damages in a critical mission. Therefore, securing the UAV network and protecting the sensitive data from various attacks become a vital aspect of the UAV network design.

Physical-layer and cross-layer authentication utilizing the situation-related characteristics of the wireless link, hardware and environment between the devices can provide a promising security enhancement in the UAV swarm. By adopting these unique characteristics, the difficulty for the attackers to impersonate a legitimate device can be significantly increased. However, the traditional centralized authentication schemes make the final authentication decision based on only the central node which may cause a single-point failure due to the imperfect attributes estimations. To solve this challenge, the decentralized authentication techniques which collect authentication decisions from multiple devices can be considered to enhance the overall authentication reliability and robustness. Nevertheless, the extra computational cost caused by using more devices may significantly downgrade the network efficiency.

In this thesis, we propose an intelligent collaborative authentication mechanism in which a minimum number of authentication devices are chosen to fuse the final authentication decision. A fluid authentication model is built to switch between the centralized authentication model and the decentralized authentication model based on the application scenario and the corresponding performance requirement. The simulation results prove the superiority of the proposed scheme in terms of reducing the authentication devices, decreasing the training period and guaranteed performance requirements as compared to the existing solutions.

Co-Authorship Statement

The content of this thesis is either published or in preparation for submission in peer-reviewed journals as listed below:

Chapter 3: **Safeguarding Cluster Heads in UAV Swarm Using Edge Intelligence: Linear Discriminant Analysis-Based Cross-Layer Authentication**

Authors: Huanchi Wang, He Fang, Xianbin Wang

Author's Contribution: Huanchi Wang designed the algorithms, conducted the simulations, analyzed the results, and drafted the manuscript. Dr. He Fang was involved in generating the system model, reviewing the algorithms and editing the manuscript. Dr. Xianbin Wang was involved in defining the research problem and editing the manuscript.

Status: Published

Reference: H. Wang, H. Fang and X. Wang, "Safeguarding Cluster Heads in UAV Swarm Using Edge Intelligence: Linear Discriminant Analysis-Based Cross-Layer Authentication," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1298-1309, 2021.

Chapter 4: **Edge Intelligence Enabled Soft Decentralized Authentication in UAV Swarm**

Authors: Huanchi Wang, He Fang, Xianbin Wang

Author's Contribution: Huanchi Wang designed the algorithms, conducted the simulations, analyzed the results, and drafted the manuscript. Dr. He Fang was involved in reviewing the system model and algorithms as well as editing the manuscript. Dr. Xianbin Wang was involved in defining the research problem and editing the manuscript.

Status: Published

Reference: H. Wang, H. Fang, X. Wang, "Edge Intelligence Enabled Soft Decentralized Authentication in UAV Swarm," 2021 IEEE/CIC International Conference on Communications in China (ICCC), pp. 1-6, 2021.

Chapter 5: **Guaranteed Service-of-Security Provisioning with Minimized Complexity for Distributed Collaborative Authentication**

Authors: Huanchi Wang, Xianbin Wang, He Fang, Lajos Hanzo

Author's Contribution: Huanchi Wang designed the algorithms, conducted the simulations, analyzed the results, and drafted the manuscript. Dr. Xianbin Wang was involved in defining the research problem and editing the manuscript. Dr. He Fang and Dr. Lajos Hanzo were involved in editing the manuscript.

Status: In preparation for submission

Reference:N/A

Acknowledgments

I would like to express my deepest appreciation to my supervisor, Dr. Xianbin Wang, for all his patient guidance, selfless supports and precious time in developing my research. He encouraged me to explore the novel research areas and reminded me that I should remember that the engineering problem is always objective-driven. This guided me through my research and will always be memorized to make me a better engineer. It was a wonderful experience to learn from him during these two years.

I would like to thank everyone in our research group for their professional suggestions and comments.I want to especially express my gratitude to Dr. He Fang for all the inspirations and the help in improving my research works. Her passion in research significantly influenced me to set a higher standard in all my works.

Additionally, I would like to thank all graduate course instructors and administrative staff at Western University. I cannot complete this degree without their professional assistance and kindness during the past years.

As always, I feel so grateful to my parents who supported me and encouraged me to become a better person. This is the seventh year abroad and they have always tried their best to help me overcome all the difficulties. I wish you will always be happy and healthy.

Contents

List of Figures

List of Tables

List of Abbreviations

CFO	carrier frequency offset
CH	cluster head
CIR	channel impulse response
CPU	central processing unit
DL	deep learning
DoS	Denial-of-service
FA	false alarm
FANET	flying ad hoc network
GPU	graphic processing unit
IoT	Internet-of-Things
I/Q	in-phase/quadrature
KNN	k-nearest-neighbor
LDA	linear discriminant analysis
LOF	local outlier factor
MANET	mobile ad hoc network
MD	miss detection
ML	machine learning
NN	neural network
OSI	open systems interconnection
PER	packet error rate
RSSI	received signal strength indication
SoS	service-of-security
UAV	unmanned aerial vehicle
VANET	vehicular ad hoc network
WSN	wireless sensor network

Chapter 1

Introduction

1.1 Overview

With the proliferation of the Unmanned Aerial Vehicles (UAVs), the range of applications has been widely increased due to the cost reduction of the wireless technologies such as Wi-Fi modules, micro-computer and sensors [1]. The operational flexibility and risk reduction in personal injury enables many cutting edge applications in commercial, military and civil fields which generates billions of revenue in the recent years [2, 3]. To be more specific, the UAV technology has been used for more than 25 years in the military for border surveillance, reconnaissance and strike. On the other hand, the public also use the UAV technology to perform goods delivery, disaster warning and law enforcement and some of the examples are demonstrated in Fig. 1.1 [4, 5, 6].

The UAV comes in different sizes and costs which means some of the UAVs can carry out more severe tasks than the others. Even though the more powerful UAVs can be used singly to accomplish the applications, the collaborative UAV system consisting of multiple UAVs, which is also known as the UAV swarm, has been considered as the enabler of many emerging applications. To allocate resources and route the intra-swarm communication to the ground station, a cluster head (CH) is selected as the central node of the UAV swarm. All the other

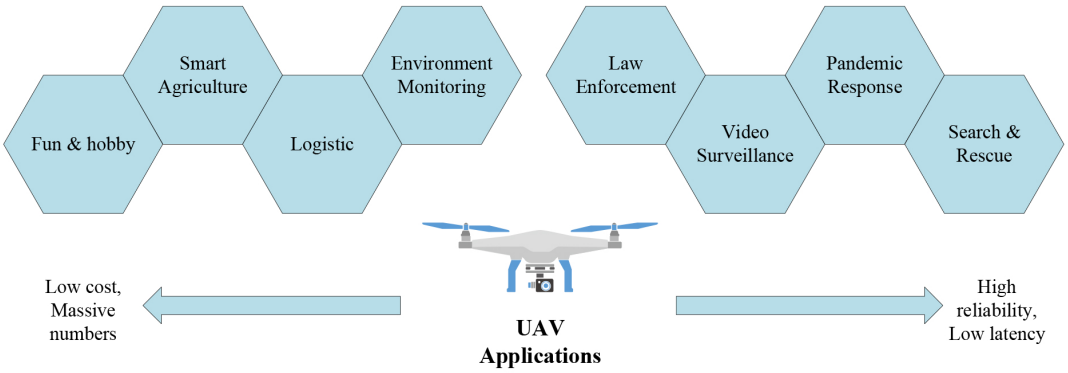

Figure 1.1: Applications of the UAVs

UAVs within the swarm are considered as member UAVs and are connected to the CH which forms an ad hoc network. Other than the advantages of the single UAV applications, the UAV swarm extends the advantages to the following:

- **Time efficiency:** The efficiency for the tasks such as search and rescue can be significantly improved with the use of the UAV swarm. By using multiple UAVs, the efficiency of searching a designated area can be significantly improved. On the other hand, the searching radius and coverage can also be extended with respect to the amount of UAVs in the swarm [7].

- **Complementarity:** Instead of using an advanced UAV loaded with all equipment together, the UAV swarm can use cheaper and smaller UAVs that carry a specific type of equipment individually and become a complement to each other. A good example is that in a fire detection and extinguishing mission, some of the UAVs can carry the fire detectors while the others can carry the infrared cameras [8].

- **Fault tolerance:** In the single UAV application, the mission has to be terminated if the UAV malfunctions. However, the loss of a UAV can be mitigated by the algorithm or the backup UAVs which vastly increases the reliability of the system.

In conclusion, the UAV swarms have many advantages over the single UAV applications

in both civil and military fields. However, there are still many challenges that need to be conquered in the future.

1.2 Thesis Motivations

The UAV swarm, which is a flying ad hoc network can be considered as a subsidiary of the mobile ad hoc networks (MANETs). However, unlike the other types of MANETs such as the vehicular ad hoc networks (VANETs), the UAV swarm suffers from high mobility where the maximum speed of a UAV can reach 460km/h with rapid physical topology change due to the 3-dimensional movement [9]. The typical MANETs or VANETS, on the other hand, are usually moving human users or cars which travel in the same direction with relatively slow physical topology change in 1-dimension [10]. The network topology of the MANET, VANET and the UAV swarm is shown in Fig. 1.2. To compensate for the high mobility, the unavoidable CH switching must become more frequent in order to supply the best service coverage to the member UAVs. The attackers can then target the CH switching process as a chance to impersonate the new CH and further compromise and control the entire UAV swarm. Hence, to protect the integrity of the UAV swarm, it is critical to ensure the security of the CH first.

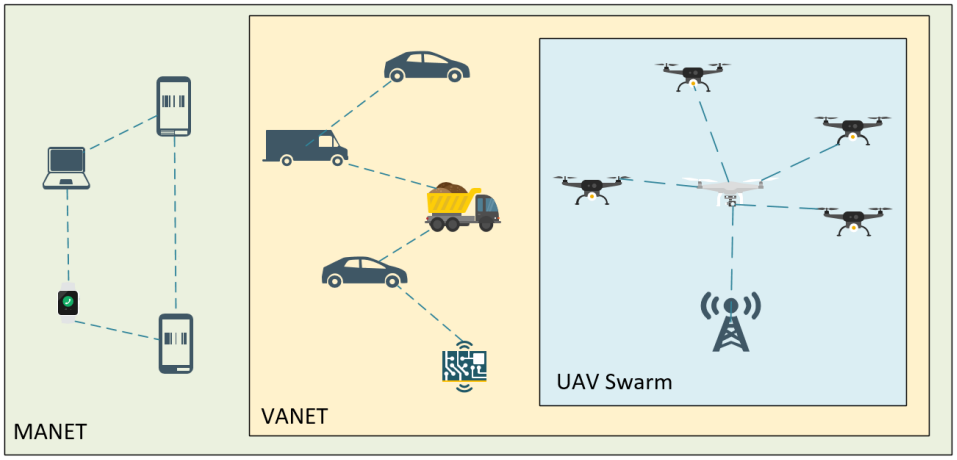

Figure 1.2: Network topology of MANET, VANET and UAV network

Additionally, the fast physical topology change may rise another critical challenge which is the intermittent connection between the member UAVs and the CH. The frequency of the re-connection is a lot higher compared to the other more stable MANETs which further increases the chance for the attackers to impersonate as a legitimate member UAV and initiate spoofing attacks. Although some more sophisticated authentication techniques such as the decentralized authentication using blockchain techniques have been developed in the recent years, the extra computational cost can create a severe overhead to the network and decrease the performance of the UAV swarm.

Moreover, the UAV swarm may also encounter more challenging operational conditions especially for the applications under the hostile environment with intermittent communication with the ground station. The UAV swarm has to utilize the limited on-site resources to enhance the security rather than relying on the cloud-based security enhancement. Hence, it is critical to develop an on-site security enhancement to protect the wireless communication of the UAV swarm under the resource constraint environment with minimal computational complexity.

In order to address these challenges, an intelligent collaborative authentication mechanism that guarantees the authentication performance by utilizing the limited on-site resources with minimal security overhead becomes a critical dilemma.

1.3 Thesis Objectives

To solve the challenges of the UAV swarm as listed above, this thesis explores a fluid authentication model that can switch between the decentralized authentication model and the centralized authentication model seamlessly with situational awareness. Besides, the security performance is also guaranteed by utilizing minimal computational cost. The sub-objectives are listed as follows:

Securing the role of CH in the UAV swarm: The CH of the UAV swarm serves a critical role in controlling the swarm and relaying the data packets. Hence, it usually contains more

sensitive data and has more interest of being attacked or impersonated by the attacker for illegal purposes [11]. On the other hand, the UAV swarm usually operates under a hostile environment with limited spectrum resources where the connection with the ground station is intermittent which means it is extremely hard to implement a cloud-based security enhancement. Hence, instead of using the cloud-based security enhancement, it is extra important to utilize the limited on-site resources to verify the identity of the new CH and protect the UAV swarm being compromised and controlled by the attackers.

Improve the authenticating performance of the member UAVs: The traditional cryptographic-based systems are built around unproven assumptions about the hardness of certain functions; hence, some of these schemes, such as the asymmetric key encryption, may be vulnerable to quantum attacks [12]. On the other hand, it is extremely hard for the system to verify the identity of the device once the security key is compromised [13]. Therefore, it is critical to utilize the unique characteristics of each UAV such as the physical layer attributes and upper layer attributes to prevent the attackers from impersonating the legitimate devices.

Minimize the computational overhead utilizing situational-aware collaborative authentication: The extra authentication security enhancement such as the decentralized authentication techniques usually increases the computational cost by comparing to the conventional centralized cryptography-based authentication [14]. By utilizing more authentication nodes, a better authentication performance can be achieved under severe conditions. However, it is unnecessary to utilize the sophisticated authentication techniques across the different environments and it is extremely important to maintain a low latency communication for both the intra-swarm communication and inter-swarm communication in some critical tasks such as the search and rescue mission. Hence, it is critical to reach an equilibrium between the authentication performance and the extra computational cost when designing the authentication schemes under the UAV applications.

1.4 Contributions of the Thesis

In this thesis, a novel collaborative authentication mechanism is proposed to protect both the role of CH and the member UAVs from being impersonated by the attackers. Only the necessary authentication resources are utilized to continuously guarantee the authentication performance throughout the different environments. In particular, only the on-site resources are utilized for the authentication decision without any help from the cloud server to compensate for the limited spectrum resources. The proposed mechanism can switch between the centralized authentication model and the decentralized authentication model based on situational awareness to compensate for the single-point failure when the CH cannot generate a confident decision while not utilizing excessive computational cost. The soft authentication decisions are generated at each authentication node to further improve the robustness and reliability of the UAV swarm. The main technical contributions of this thesis are summarized as follows:

- A linear discriminant analysis-aided (LDA) centralized authentication scheme is proposed to analyze and select the most reliable combination of cross-layer attributes under the time-varying environment. An information threshold is designed to select the least amount of attributes that can achieve the authentication performance requirement based on the situational awareness.

- Instead of a binary authentication decision, a soft authentication decision algorithm is proposed to generate a continuous authentication decision between 0 and 1 in the decentralized network. The soft authentication decision evaluates the legitimacy of a device by calculating the probability for a UAV to be legitimate. This improves the robustness of the authentication scheme by accepting the uncertainty of the edge decision.

- We propose a novel concept of Service-of-Security (SoS) to specifically achieve the defined level of authentication performance continuously to guarantee the security requirement. The computational complexity can be ultimately minimized by eliminating both

the redundant or excessive collaborators and authentication attributes across different environments based on the situational-awareness.

- An edge intelligence-enabled collaborative authentication mechanism is proposed to customize create different authentication models across the differnet environments based on situation awareness. A Gini-impurity-based attributes evaluation algorithm is paired with the authentication node evaluation algorithm as a two-factor process to evaluate and then select the most suitable combination of authentication nodes as well as the attributes being used at each node.

1.5 Thesis Outline

The rest of the thesis is organized as below:

In Chapter 2, a literature survey starts from the introduction to the physical layer authentication by discussing the advantages and disadvantages comparing to the conventional cryptographic-based authentication scheme. Then, the cross-layer authentication scheme is introduced to compensate the disadvantages of the physical layer authentication such as the imperfect estimations. After that, to further improve the reliability of the authentication in UAV swarm under a hostile environment, the decentralized authentication scheme is discussed to avoid the potential single-point failure which is a critical challenge for the centralized authentication schemes.

In Chapter 3, we propose a LDA-aided cross-layer centralized authentication scheme to eliminate the unnecessary attributes so that the authentication performance can be improved while the computational cost can be decreased. The eigenvalue of each cross-layer attribute is calculated to evaluate the usability of each cross-layer attributes and an adaptive cross-layer attributes selection algorithm is introduced to select the most informative combination of cross-layer attributes based on the situational awareness.

Considering the centralized authentication techniques may cause the single-point failure

under the more severe authentication environment, the decentralized authentication techniques have been considered to improve the overall authentication reliability and robustness. However, the increased amount of edge authentication decisions may create more ambiguity when the authentication nodes cannot provide confident authentication decisions. In Chapter 4, a probability-based soft authentication scheme is proposed at each authentication node to improve the reliability of the edge authentication decision by including the uncertainty. This can also further relax the imperfect estimations collected at each authentication node and lowers the impact of the less confident authentication node when forming the final authentication decision.

In Chapter 5, we propose a novel concept of Security-of-Service (SoS) and a collaborative authentication mechanism where only the necessary authentication resources are utilized to continuously promise the authentication performance requirement across the different environments. The objective of the fluid authentication model is to reach an equilibrium between the SoS and the computational cost. The Gini-impurity of the attributes at each authentication node, the relative distance and the past authentication record between the authentication node and the authentication requester are utilized and designed into a two-step process to achieve the design objective. The simulation is conducted in MATLAB and Python to evaluate the proposed intelligent decentralized authentication mechanism and demonstrate that the proposed mechanism can achieve the authentication requirement with minimum computational overhead based on the situation awareness.

Finally, Chapter 6 concludes the work of this thesis and reviews the future possible research direction.

Chapter 2

Security Challenges and Existing Solutions in UAV Networks

The UAV network serves as the backbone of the UAV swarm which supports diverse applications by connecting all the UAVs together. The network security enhancement techniques have been researched for a long time; however, different challenges and risks arise due to the fast development of technologies. In this chapter, an overview of the UAV network is introduced firstly. Then some details about the risks and threats in the UAV network are presented to understand the challenges. Moreover, some state-of-the-art solutions have been discussed to demonstrate both the advantages and the disadvantages. Based on these reviews, an intelligent authentication scheme for the UAV swarm will be further studied to achieve the objectives of this thesis in the following chapters.

2.1 UAV Network Overview

UAVs have been found in many new applications in recent years. In supporting surveillance and disaster relief, a collaborative group of UAVs can for a swarm to provide a self-managed FANET and rapidly be deployed for the missions [15, 16, 17]. Security provisioning in moving UAV swarm can be extremely challenging given their low cost, flexible maneuvering capability

and harsh operating environment, it brings many unique challenges by comparing to the other IoT networks such as fast network topology change, intermittent connection with the ground station and risk of being discovered by the adversaries [18, 19, 20, 21]. Although the CH of the FANET can access the ground station and use it as a centralized authentication server as shown in Fig. 2.1, the high-power long-distance wireless transmission and the increased latency make the cloud-based authentication schemes less feasible under the FANET. Hence, the on-site resources, which are the resources within the UAV swarm (i.e., using the CH as the central authentication server), should be utilized to achieve a fast and reliable security provisioning.

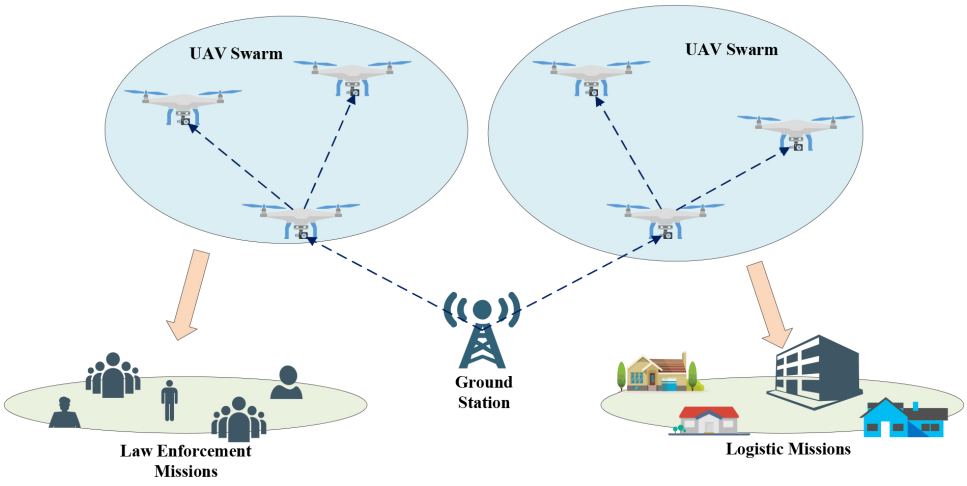

Figure 2.1: Topology, challenge and application of the flying UAV networks.

To further elaborate the uniqueness of the FANET, we conclude the characteristics in point form as shown below:

- **Topology:** Unlike the MANET whose topology is random with no centralized topology required, the topology of the UAV network is usually a star topology with a central node called a cluster head (CH) [22]. The CH aims not only to relay the intra-swarm communication between the member UAVs but also the inter-swarm communication to the ground station. Therefore, instead of a mesh topology, the CH has to provide reliable communication links to all member UAVs which is challenging throughout the entire application.

- **Mobility:** Since the UAV travels in the air, the freedom of travelling is much higher than the other types of MANETs. The nodes within the MANETs usually travel in the same direction which can be summarized as a 1-dimensional movement; nevertheless, the UAVs can travel in any direction and can be considered as a 2-dimensional or 3-dimensional movement. Moreover, the nodes within the MANETs are usually moving human users while the maximum speed of the UAV can reach 460 km/h [19].

- **Dynamic topology:** Due to the high mobility and the different types of applications, the topology change may be much more frequent in the UAV networks than the MANETs. For example, during a military application, new targets can show up unexpectedly; hence, the UAV swarm may get frequently partitioned to accommodate the application requirement. In this case, when a new UAV swarm is partitioned from the existing UAV swarm, it is extremely important to make sure that the sensitive information is transferred to the legitimate UAVs.

- **Energy constraints:** In the MANETs, the nodes are usually battery powered and wireless communication is the major battery consumption. Similarly, some of the UAV swarms may be constructed by the mini UAVs which are also energy-constrained. However, some of the applications require larger UAVs whose major battery consumption is the motor and the UAV management system (i.e., the autopilots system and navigation system). In this case, the power consumption of the motor may take up to 200 watts/kg while the communication module only takes 0.8 to 5 watts which is negligible [23, 24, 25]

Hence, with these unique characteristics, more security challenges arise with respect to the UAV networks.

2.2 Risks and Threats in the UAV Networks

To support the different types of UAVs, the UAV swarm has to adopt different wireless transmission protocols and form a heterogeneous network. Similar to the other mobile devices, the open nature of the wireless communication brings many typical security challenges to the UAV networks as shown in Figure 2.2 and listed below:

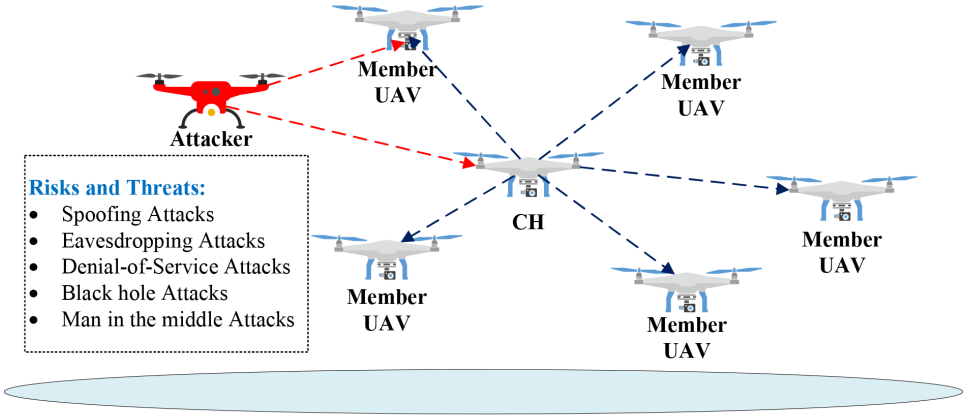

Figure 2.2: Typical risks and threats in UAV swarms.

- **Spoofing attacks:** Due to the openness of the wireless communications, an attacker can forge a legitimate identity and send signals to control or cheat a legitimate UAV which poses a serious threat to the UAV network [26]. A good example is that an attacker may impersonate a legitimate member UAV during a military task and send the forged data to the CH and create a false target. This may lead the whole UAV swarm into a dangerous situation and lead to a failed mission.

- **Eavesdropping attacks:** There are mainly two types of eavesdropping attacks which are the passive eavesdropping attack and the active eavesdropping attack. In the passive eavesdropping attack, the attackers aim to intercept the confidential communication silently without degrading the received signal quality. Hence, it brings security vulnerability since it is very hard for the other devices to detect the presence of the attacker. On the other hand, the active eavesdropping attacks aim to jam the main communication

channel and degrade the limited channel capacity which is more harmful by comparing to the passive eavesdropping attacks [27, 28].

- **Denial-of-service (DoS) attacks:** Similar to the active eavesdropping attacks, the DoS attacks aim to exhaust the UAV network resource by sending superfluous requests. The goal is to prevent the legitimate UAVs from accessing the CH for services or resources [29]. This is extremely harmful to the UAV network due to its simple implementation and will significantly degrade the efficiency.

- **Black hole attacks:** Similar to the eavesdropping attacks, instead of listening silently, the attacker actively lures the data packet by claiming that it can relay the data packet or it is the designated destination. After it receives the sensitive information, it drops all the data packets or certain packets for illegal purposes [30].

- **Man in the middle attack:** In this type of attack, the attacker monitors and then modifies the data packet between the member UAV and the CH. In this case, the attacker can not only modify the data being collected from the member UAVs but also changes the commands from the CH. Hence, it is extremely important to verify the true identity of the sender to avoid falsified information [31].

Other than these typical security risks during the mission, the UAV swarm also encounters some additional security risks. For example, due to the high mobility and the dynamic topology, a CH switching process is unavoidable to provide better coverage to all member UAVs. However, during the CH switching process, it gives the attackers chances to impersonate a legitimate UAV and becomes the new CH. Then, it can not only inherit the existing highly sensitive information but also forge and delete new data packets to control the entire UAV swarm.

Other than the security risks, the harsh operating environment is also a key challenge. Since the UAV swarm may operate under a hostile environment, the radio spectrum resource is extremely limited under this scenario [11]. Moreover, the wireless communication should

remain silent when unnecessary to prevent the enemy force from detecting the UAV swarm. Therefore, it is almost impossible to implement the cloud-based security enhancement and the UAV network can only rely on the limited on-site resources for security enhancements.

2.3 Existing Solutions for UAV Network Security and Their Challenges

In this section, we discuss both the centralized authentication techniques and the decentralized authentication techniques for solving the challenges above. We have also concluded their challenges within the UAV swarm respectively.

2.3.1 Centralized Authentication

Conventional wireless security provisioning is achieved by using a centralized server, such as an authentication server, or any trusted third party to provide the required credentials [32]. These centralized servers bring many benefits such as predictable overhead, high interoperability and compatibility with different platforms [33]. When using the centralized authentication in the FANET, the CH has to authenticate and authorize each member UAV when needed based on its own decision. To enhance the overall security of the UAV swarm, some state-of-the-art authentication techniques have been implemented at the CH as listed below:

2.3.1.1 Cryptographic-based Authentication

The digital-key cryptographic-based authentication techniques implemented in the network layer have an extensive history in the wireless communication authentication field. In the conventional approaches, the member UAV transmits the encrypted digital key to the CH where the key will be verified to gain access to the services. However, to further increase the security, the mutual authentication techniques with public and private keys have also been developed.

Although there exists many benefits for cryptographic-based authentication schemes, these techniques also suffer from the rapid development of computational power. To be more specific, in the UAV network, once the security key is compromised by the attacker via brute force attacks, it is extremely hard for the CH to verify the true identity of the device. To solve this problem, some cryptographic-based authentication schemes refresh the digital key periodically. However, to manage, generate, revoke and distribute these keys on a regular basis, the network latency will be increased and become intolerable especially under large-scale networks. Besides, the key distribution process may also increase the chance of being eavesdropped on by the attacker within the UAV swarm.

To further elaborate some of the state-of-the-art cryptographic-based authentication schemes, the author of [34] developed a secure mutual authentication scheme between robots and cloud servers using Elliptic Curve Cryptography with the key agreement for robots. Besides, the author of [35] developed a symmetric key-based mutual authentication scheme with a session key distribution system. In this scheme, instead of receiving a key from the key distribution center, each node agrees with the algorithm to generate session keys so that the session keys can be calculated in advance. Moreover, a lightweight privacy-preserving key establishment has been introduced in [36]. The proposed scheme aims to overcome the existing problems with trusted authority dependency and secure communication channel reliance during the registration. However, there still exist many drawbacks to these state-of-the-art authentication techniques such as forgery attacks, offline password guessing attacks and user traceability issues. Some of these schemes also suffer from higher latency due to the necessary key generation, distribution and refreshment.

2.3.1.2 Physical-layer Authentication

In contrast to the cryptographic-based authentication techniques relying on the upper layers in the network, the physical-layer authentication utilizes the randomness of signals, wireless channels and hardware impairments to provide information-theoretic security enhancement

[37]. The reciprocal channel properties and the analog front-end imperfections are directly related to the specific environment and the device hardware which improves the difficulty for the attackers to impersonate the legitimate devices. Other than the security enhancement, the physical-layer authentication techniques also bring many other advantages such as a lower computational complexity and latency since it does not need to consider how security protocols are implemented [38, 39].

There are mainly two types of physical-layer authentication schemes which can be classified as composite security key-based scheme or keyless scheme, according to whether a physical-layer attributes-based secret key is exploited and shared between the transmitter and receiver [40]. For the key-based physical layer authentication, the authors of [41] proposed a physical-layer challenge-response authentication mechanism that adopts orthogonal frequency-division multiplexing technique and separately modulates the higher layer information and shared keys on subcarriers' phases and amplitudes respectively. On the other hand, the authors of [42] proposed an adaptive physical-layer key generation scheme based on Received Signal Strength. By utilizing the group quantization, the randomness of the generated key was improved since the 0 and 1 in generated keys were more evenly distributed. The adaptive quantization has also been considered to design adaptive quantization intervals. Moreover, a pre-shared key generation algorithm under vehicular network has been proposed by the authors of [43], in which the key length is optimized to improve the performance in terms of time and energy.

The keyless physical-layer authentication is also widely studied by the researchers due to the low computational overhead compared to the key-based schemes. It focuses on exploiting the physical layer attributes of the communication links and device hardware such as the channel impulse response (CIR), carrier frequency offset (CFO), received signal strength indication (RSSI) and in-phase/quadrature (I/Q) imbalance [13, 44, 45, 46]. The authors of [47] explored fuzzy theory for modelling multiple physical-layer attributes together. The fuzzy theory-based model helped to compensate for the imperfectness and uncertainties of the physical layer esti-

mations to improve the overall performance. On the other hand, the authors of [48] utilized a deep learning-based physical layer authentication framework with three gradient descent algorithms which enables smaller computational overheads and lower energy consumptions. Moreover, the authors of [49] proposed a blind authentication scheme that combines the techniques of blind known interference cancellation and differential processing which suppresses the deteriorating effect of fading channels without additional preprocessing. Although there exist many advantages for the physical layer authentication schemes, there still exist many challenges as listed below for the UAV network:

- **Imperfect estimations:** The physical layer estimations can be severely affected by the decorrelated attributes caused by the mobility and dynamic interference. The unstable fluctuation increases the dynamic range of the physical-layer attributes which further leads to the insufficient range to separate each UAV from the other. Therefore, the overlap increases the tolerance for the attacker to impersonate the legitimate UAV to cheat the physical-layer-based authentication schemes [11].

- **Time-varying environment:** Due to the high mobility of the UAVs, some physical layer attributes may encounter a sudden change. Hence, the authentication scheme may accidentally reject a legitimate member UAV as an attacker. On the other hand, to compensate for the sudden change, some authentication models may increase the tolerance for the attributes which may give the attacker more chance to impersonate the legitimate UAVs.

- **Difficulty in authentication model generation:** The physical layer attributes are highly correlated to the specific operating environment; therefore, it is extra difficult for the system to generate an authentication model in advance. This requires the UAVs to keep collecting and updating the physical layer attributes of each other during the mission and generate a real-time authentication model. However, this may increase the overall network latency as well as the power-consuming which is undesirable in many types of

missions.

It can be concluded that the physical layer authentication techniques are more suitable to be implemented in a static environment where the attributes are stable throughout the mission. However, in practical UAV swarms, the member UAVs may move in and out of the swarm frequently due to the high mobility which requests the CH to constantly update the physical layer estimations to ensure the authentication performance. However, the frequent estimations require fast and massive computational overhead when the size of the UAV swarm grows which will lead to a bottleneck situation and degrade the advantages of the physical layer authentication.

2.3.1.3 Cross-layer Authentication

To improve the stability and robustness of the physical layer authentication in the dynamic environment, it is critical to combine extra upper layer attributes with the physical layer attributes. Other than the physical layer attributes as mentioned above, the upper layer attributes such as the Packet Error Rate (PER), position information (i.e., GPS coordinates) and pre-existing upper layer authentication schemes [50, 51, 52]. To utilize these attributes together, the researchers have come up with different methods to fuse and cascade the attributes together to fulfill the requirements of different implementations.

One of the popular techniques to combine the different layers is to use the upper layer attributes as a backup plan when the physical layer fails. For example, in [52], the authors proposed a fast cross-layer authentication scheme that utilizes pre-existing upper layer authentication scheme at reasonable time instants to compensate the physical layer authentication. The upper layer authentication scheme will verify the identity of the device again if the physical layer authentication scheme recognizes the device as an attacker. This technique can certainly decrease the probability of false alarming; however, it gives the attackers a second chance to impersonate the legitimate device for illegal purposes.

On the other side, instead of a two-step process, the authors of [50] fuse the PER and the

RSSI as a one-step process. The authentication system verifies both attributes at the same time since it is nearly impossible to impersonate a legitimate device at the same time. However, the performance of this method may degrade with respect to the increase of the UAV swarm size. Moreover, the authors of [53] proposed a cross-layer authentication framework based on hash access and quantum encryption in industry IoT 4.0. The framework included a device authentication system to defend against the preamble-aware attack and a privacy-preserving protocol to avert small data eavesdropping attacks.

In conclusion, although cross-layer authentication can improve both the robustness and reliability of the physical layer authentication, the extra computational overhead associated with the increased amount of upper layer attributes is still a major challenge. Therefore, it is critical to improve cross-layer authentication by balancing the performance and the computational complexity in the UAV network.

2.3.1.4 Analysis

Although centralized authentication has been widely inherited in many network security applications, the single-point failure is unavoidable when the security technique fails at the CH. In the cryptographic-based authentication techniques, if the digital key is leaked, the system security implemented at the CH will not be able to verify the identity. In the physical-layer and cross-layer authentication techniques, the CH may encounter imperfect physical layer estimations or miss some of the cross-layer attributes under the hostile environment which may further lead to authentication failure. Therefore, it is extremely important to increase the robustness and reliability of the network security by introducing more authentication nodes at the same time.

2.3.2 Decentralized Authentication

With the growing size of the UAV swarm, observing and analyzing multiple attributes and devices at the same instance may create a bottleneck and reduce application traffic [54]. On the

other hand, it is challenging for the existing centralized authentication scheme to manage identity security by presenting a single point failure. A peer-to-peer decentralized authentication scheme is a feasible solution where a symmetric relationship between the member UAV and the CH is provided. Instead of solely relying on the authentication decision of the CH, the member UAVs can be considered as authentication nodes that can contribute to the authentication decision as shown in Figure 2.3. Therefore, the challenges of some existing authentication schemes, such as the imperfect physical layer estimations, can be compensated by using multiple estimations by utilizing different UAVs.

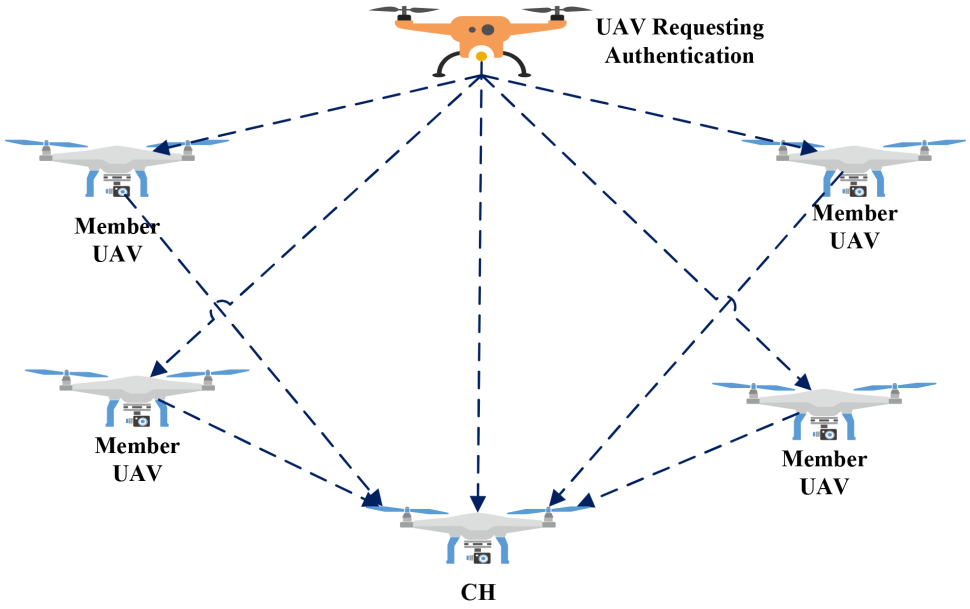

Figure 2.3: Basic structure of decentralized authentication in UAV network.

2.3.2.1 Blockchain-based Authentication

The blockchain-based authentication scheme has attracted extensive interest over the past few years in which duplicated transactional databases, or ledgers, are distributed over multiple nodes within a peer-to-peer network [14]. These nodes form a chain of ordered blocks and each block contains the cryptographic hash of the previous block as shown in Figure 2.4, in which

the longer the blockchain is the safer the system will become [55]. Therefore, it is extremely hard for the attacker to forge or delete the information since the attacker has to overwrite or remove the history from all nodes before the next block record arrives [56].

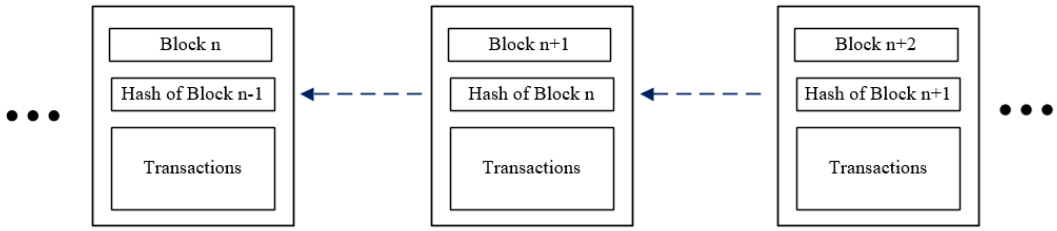

Figure 2.4: Basic structure of blockchain.

The authors in [57] constructed a private blockchain in each Internet-of-Things (IoT) network by utilizing the coin-based blockchain system. A hardware authenticator, which is not connected to the internet, is used to generate blocks and transfer a certain amount of coins to the authenticated device. Hence, a ledger is developed to store the authentication information across the network and is used to verify the identity of each device in the future. On the other hand, the authors in [58] proposed an out-of-band two-factor blockchain-based authentication scheme in the home IoT network. The out-of-band channel, such as light and acoustic are used to verify whether the access requestor is located within the home. Moreover, the authors of [59] proposed a hybrid blockchain-based authentication scheme for the sensor networks. The devices form a hierarchical network by being divided into base stations, cluster head nodes and ordinary nodes with respect to their capability differences. A hybrid model is then formed in which the cluster head node identity authentication is accomplished by the public blockchain while the ordinary node identity authentication is realized in the local blockchain.

Although the blockchain-based authentication brings many advantages to the network safety, the number of UAVs in a simple application may be small which is not sufficient to leverage the security enhancement amplified by using a private chain. Moreover, if the public chain is adopted in the UAV network, the process may become less efficient due to the transaction storage and delays. Therefore, it is critical to develop other types of decentralized authentication

schemes within the UAV network to enhance the authentication performance and maximize the efficiency of the network simultaneously.

2.3.2.2 Analysis

Although the decentralized authentication techniques were proposed to compensate for the challenges such as the single point failure, there are still a few drawbacks to this technique. Firstly, authentication by using more peers will consume more resources and time which increases the network latency when the size of the UAV swarm grows. The tasks such as the key distribution can become more complex to cover all the UAVs within the swarm [60].

On the other hand, some of the authentication nodes can be less reliable in one scenario than the others. A good example is when the authentication nodes are making decisions based on the keyless physical layer authentication schemes, some of the UAVs may receive the physical layer estimations with more interference than the others. This may lead to further confusion during the final authentication process which lowers the robustness of the authentication performance. Moreover, the increased amount of authentication nodes brings higher risk due to the larger attack surface. Instead of becoming the CH of the UAV swarm, the attacker can impersonate some of the member UAVs and initiate sybil attacks to influence the authentication decision by sending forged decisions. Therefore, it is critical to verify and select the authentication nodes within the UAV swarm to compensate for these challenges within the decentralized authentication scheme.

2.4 Chapter Summary

This chapter firstly went through the overview of the UAV network followed by the threats and risks. The existing solutions have been reviewed including the cryptographic-based authentication, physical-layer authentication, cross-layer authentication, and the blockchain-based authentication. The advantages and disadvantages of these techniques were presented to demon-

strate the criteria to design the new intelligent authentication scheme.

Although these state-of-the-art authentication techniques could achieve great performance, an open challenge is that these techniques are best-effort based which cannot provide a stable and guaranteed security performance across different application scenarios and environments. Some of these authentication schemes may cost an excessive amount of computational cost in simple applications. Hence, it is critical to find an equilibrium between the authentication performance and the computational cost. Based on the preliminaries provided in this chapter, new centralized and decentralized intelligent authentication schemes will be developed in the next following chapters.

Chapter 3

Situational-aware Linear Discriminant Analysis-based Authentication Scheme

To verify the true identity of all devices within the UAV swarm, the centralized cross-layer authentication technique can be utilized by verifying the unique attributes of each device, i.e., physical channel characteristics, hardware imperfection, location, data link layer characteristics and so on. By utilizing the different layers of the Open Systems Interconnection (OSI) Model, it significantly increases the difficulty for the attackers to impersonate the legitimate device. However, the cross-layer authentication techniques also have their own challenges in the UAV swarm such as the high computational complexity to collect and analyze the excessive amount of attributes in the resource constraint devices. Besides, some of the cross-layer attributes are not useful in specific scenarios which may reduce the performance by bringing ambiguity into the decision-making. To circumvent these unique challenges, a Linear Discriminant Analysis-based (LDA-based) authentication scheme is proposed as a smart process in this chapter to analyze and select the cross-layer attributes. Then, the selected attributes will be fused to compute a binary authentication decision which improves the reliability and robustness of the authentication performance while effectively reducing the unnecessary attributes.

3.1 Introduction

The UAV techniques enable many cutting-edge technologies in both military and civilian fields; hence, the UAV networks may contain highly sensitive and personal information where the open broadcast nature of wireless channels allows attackers to initiate various types of attacks via the wiretap channels. Traditionally, conventional cryptographic-based authentication techniques have been adopted to enhance the network security by mainly generating, exchanging and employing secret keys. However, once the security keys are compromised, it is extremely difficult for the CH to realize in terms of key distribution and management. Moreover, with the rapid development of the computational power, the attacker's ability to decode the eavesdropped signals from the open-air has also been increased significantly. Therefore, an efficient authentication technique that can relate the unique characteristic of each UAV to its identity becomes a dilemma to prevent the attackers from impersonating the legitimate UAVs under the harsh resource constraint environment.

To extract the unique hardware-based and channel-based characteristics for each device, the physical-layer-based authentication technique has been developed. However, the imperfect estimations and the variation of the physical-layer attributes in a dynamic network can significantly degrade the performance of the physical-layer authentication schemes [61, 62, 63]. When the channel is unstable, especially under a hostile environment, the physical-layer authentication may be severely affected by the sudden change of the physical-layer estimations due to the decorrelated attributes collected from a different time and operating environment. For example, the CIR in the open-air environment may be significantly different from the non-line-of-sight condition. Hence, rather than simply increasing the number of physical-layer attributes, it is critical to consider the more stable upper layer attributes. However, the increased amount of attributes may bring challenges for the operating. To be more specific, instead of observing the physical-layer attributes seamlessly in the background, a protocol has to be designed to transmit the required higher layer attributes [38, 39]. Also, it is challenging to decide which attributes should be observed in advance; hence, the CH may need to estimate the num-

ber of attributes and eliminate the unnecessary ones before fusing the authentication decision. Hence, the concept of situational-aware cross-layer authentication is extremely important to select and customize the adaptive authentication scheme which maximizes the authentication performance while minimizing the computational cost.

To overcome these difficulties, the LDA algorithm is introduced in which the dimensionality of the cross-layer attributes is reduced by applying a linear transformation that only keeps the most relevant attributes in the specific scenario. A projection of the original data is then formed such that the between-class variance is maximized and the within-class variance is minimized thereby maximizing the class separability [64, 65, 66]. Hence, the LDA algorithm can help to extract useful information from the high dimensional estimations with the maximized efficiency due to the calculation simplicity. However, the LDA algorithm needs input from the operator to specify the number of attributes being kept after the attributes selection process. Hence, a situational-aware attributes selection algorithm has to be developed simultaneously to compute the number of cross-layer attributes being selected for the LDA algorithm so that an adaptive cross-layer authentication scheme can be achieved. On the other hand, unlike the other 2-step cross-layer authentication schemes where the upper-layer authentication scheme is only utilized to verify the decision of the physical-layer authentication, our proposed scheme uses all selected attributes at the same time to fuse the authentication decision.

Hence, the contribution of the situational-aware LDA-based authentication scheme can be summarized as follows:

- A novel edge intelligence enabled cross-layer authentication scheme is proposed to provide an on-site multi-dimensional assessment that verifies the true identity of each device within the UAV swarm. By utilizing the cross-layer attributes, it is significantly more difficult for the attackers to predict the authentication model and impersonate the legitimate UAVs.

- A novel LDA-based authentication scheme is proposed to fuse multiple cross-layer attributes and minimize the complexity of the authentication system by reducing the di-

mensionality. A novel situational-aware cross-layer attributes selection algorithm is also proposed to select a minimum amount of attributes to be used in the LDA-based authentication scheme while maintaining the authentication performance.

- Various simulations are performed to demonstrate the stability and robustness under a travelling UAV swarm. The results also demonstrate that the computational overhead of our proposed scheme is lower than the other 2-step cross-layer authentication schemes.

The main symbols used in this chapter are summarized in Table 3.1

Table 3.1: Main Symbol Table of Chapter 3

Symbol	Definition
I_m^{ini}	Digital identity of the m-th UAV
M	Number of member UAVs in the swarm
N	Number of cross-layer attributes
t	Time instance that the authentication is required
$\boldsymbol{H_m^I}$	Cross-layer estimations of the m-th UAV in phase I
$\boldsymbol{H_m^{II}}$	Cross-layer estimations of the m-th UAV in phase II
δ	Distance threshold
ψ_0	UAV is legitimate
ψ_1	UAV is a spoofing device
$\mathcal{E}$	Error rate of the authentication process
w_1	Weight of false alarm rate
w_2	Weight of miss detection rate
$\boldsymbol{h}$	A single cross-layer estimation
S_m	Scatter matrix of the m-th class
$\bar{\boldsymbol{h}}_{\boldsymbol{m}}$	Mean of the cross-layer estimations for the m-th class
k_m	Number of cross-layer estimations for the m-th class
$\mathcal{W}$	Intra-class scatter matrix
$\mathcal{B}$	Inter-class scatter matrix
$\boldsymbol{\Phi}$	Linear transformation matrix of the original dataset
$\boldsymbol{\lambda}$	Eigenvalue of the transformation matrix
ν	The number of cross-layer estimation selected
τ	Information threshold

3.2 System Model

As shown in Fig. 3.1, we consider a UAV swarm that consists of M member UAVs and an on-duty CH. There exists a spoofing device that aims to intercept and impersonate a legitimate UAV for illegal purposes. The CH aims to verify the true identity of each device within the UAV swarm accurately to prevent the sensitive data from leaking by utilizing the cross-layer attributes. A situational-aware authentication process is also designed to increase the difficulty for the attackers to predict the authentication model and impersonate the legitimate UAVs.

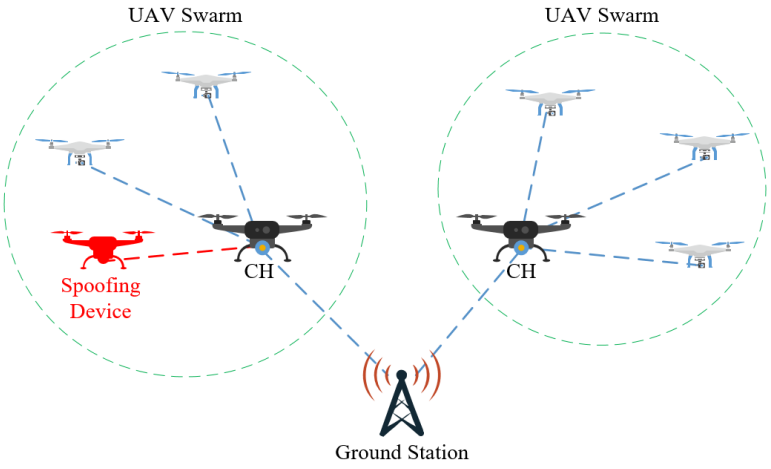

Figure 3.1: System model. M legitimate member UAVs exist within the UAV swarm with one on-duty CH. The on-duty CH focuses on continuously verifies the identity of each device within the network to prevent the sensitive data from being leaked.

The process of authentication relying on multiple cross-layer features contains two phases: *Phase I*: The on-duty CH collects the trusted cross-layer estimations from all M UAVs, when they first join the network, as $\boldsymbol{H_1^I}, \boldsymbol{H_2^I}, ..., \boldsymbol{H_M^I}$. These estimations are paired with their digital identities $(I_1^{ini}, I_2^{ini}, ..., I_M^{ini})$ during the collection. The trusted cross-layer estimation of the m-th UAV, whose digital identity is I_m^{ini}, can be denoted as:

$$\boldsymbol{H_m^I} = (H_{m1}^I, H_{m2}^I, \ldots, H_{mN}^I)^{\mathrm{T}}, \tag{3.1}$$

where N is the number of cross-layer attributes and $()^{\mathrm{T}}$ is the transposition of the vector. To ob-

tain the trusted cross-layer estimations, each UAV broadcasts data packets that include its GPS location at a certain time slot. The other UAVs receive the GPS coordinates as the application layer attribute and calculates the PER of the received packets as the data link layer attributes. The physical-layer attributes can be estimated by using the embedded hardware to calculate the RSSI, I/Q imbalance, CIR, CFO and so on. The imperfect physical-layer estimation is acceptable as fluctuations.

Phase II: At time t, the on-duty CH collects a set of observations from the UAV that requires an authentication, where the cross-layer estimation of the the device m can be written as

$$\boldsymbol{H_m^{II}} = (H_{m1}^{II}, H_{m2}^{II}, \ldots, H_{mN}^{II})^{\mathrm{T}}. \tag{3.2}$$

To achieve the situation-awareness of authentication in the time-varying environment using cross-layer attributes, the cross-layer estimations should be collected periodically. Since the cross-layer attributes estimations represent the characteristic of the device, a measurement of the similarity between the estimation collected in *Phase II* and *Phase I* is critical and can be formulated as:

$$d(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}) = \sqrt{(H_{m1}^{II} - H_{m1}^{I})^2 + ... + (H_{mN}^{II} - H_{mN}^{I})^2}, \tag{3.3}$$

where $d(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}})$ is the Euclidean distance between the cross-layer estimation of the m-th UAV collected in *Phase II* and the trusted estimation collected in *Phase I*. Since the scale and distribution of each attribute may be different from the other attributes, it may increase the generalization error under the flat space. To be more specific, the authentication model may favour the attributes with larger weight and decrease the sensitivity of the smaller weight attributes. Therefore, it is critical to implement a scaling process such as normalization and standardization. After collecting and scaling the data, the authentication decision will be forged by judging the similarity between these collected estimations. A distance threshold δ can be introduced as the similarity judgement to separate the spoofing device from the legitimate

UAVs. The authentication decision can then be written as a binary hypothesis test:

$$\begin{cases} \Psi_0, & d(\boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{II}}, \boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{I}}) \leq \delta; \\ \Psi_1, & d(\boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{II}}, \boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{I}}) > \delta, \end{cases} \tag{3.4}$$

in which Ψ_0 represents the UAV is legitimate and Ψ_1 indicates the UAV is a spoofing device.

3.3 Problem Formulation

To evaluate the performance of the decentralized authentication, two potential errors are considered:

1) False Alarm (FA) rate: The probability that the legitimate UAV is rejected as a spoofing device. The function can be given as:

$$P_{\mathrm{FA}} = \Pr(d(\boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{II}}, \boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{I}}) \leq \delta | \Psi_{m1}). \tag{3.5}$$

2) Miss Detection (MD) rate: The probability that the spoofing device is approved as a legitimate UAV. It can be defined as:

$$P_{\mathrm{MD}} = \Pr(d(\boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{II}}, \boldsymbol{H}_{\boldsymbol{m}}^{\boldsymbol{I}}) > \delta | \Psi_{m0}). \tag{3.6}$$

To evaluate the accuracy and robustness of the decentralized authentication, the false alarm rate and the miss detection rate can be combined as the error rate ($\mathcal{E}$) as

$$\mathcal{E} = w_1 P_{\mathrm{FA}} + w_2 P_{\mathrm{MD}}, \tag{3.7}$$

where w_1 and w_2 are the costs of the false alarm and the miss detection. The false alarm and the miss detection can be treated equally; however, under certain applications, the miss detection

may cause more damage to the system than the false alarm and may have a higher cost. Hence, the operator can choose to set different weights for both scenarios under specific applications. To achieve the best authentication performance, both the false alarm rate and the miss detection rate should be minimized. The problem formulation of this chapter can then be formulated as:

$$\min_{\delta} \mathcal{E}, \tag{3.8}$$

where δ is the distance threshold as introduced above.

3.4 Situation-aware LDA-based Cross-layer Authentication

To solve the problem of (3.8) in a small group of UAVs, it is critical to authenticate each legitimate device correctly by distinguishing the spoofing device from the legitimate UAVs under a limited computational capability. To further improve the authentication performance, the uniqueness of each UAV should be improved by enhancing the separability of the original estimations. Hence, the LDA-based authentication scheme is proposed to project the original observations into a low dimensional space with maximum separability while reducing the computational overhead and time latency. Then, a situational-aware cross-layer attribute selection algorithm is proposed to select a minimum amount of cross-layer attributes that maintain the overall performance under the dynamic environment.

3.4.1 Authentication Based on LDA Algorithm

To extract the information from the multiple cross-layer attributes, we explore the LDA technique which transforms the initial verified cross-layer estimation into a low-dimensional space for better separability. After collecting the set of trusted cross-layer attributes ($\boldsymbol{H^I}$) in *phase I* and the cross-layer attributes ($\boldsymbol{H^{II}}$) for authentication at time t in *phase II*, all the observations are merged together to form the new set ($\boldsymbol{H}$) that are being used for the authentication. Each

estimation in $\boldsymbol{H}$ is denoted as $\boldsymbol{h}$ and the estimations of the m-th UAV is I_m^{ini}. The cross-layer estimations of each UAV can be considered as a class to be further used in the LDA algorithm. To analyze the estimations, the scatter matrix of each class which estimates the covariance matrix is formulated as:

$$S_m = \sum_{h \in I_m^{ini}} (\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})^{\mathrm{T}}, \tag{3.9}$$

where

$$\bar{\boldsymbol{h}}_{\boldsymbol{m}} = \frac{1}{k_m} \sum_{h \in I_m^{ini}} \boldsymbol{h}, \tag{3.10}$$

represents the mean for each class and k_m is the number of samples in I_m^{ini}. The scatter matrix is fundamental to LDA since it measures the distribution of the given data. Hence, the total intra-class matrix, which describes how far each class is away from each other, is calculated as:

$$\mathcal{W} = \sum_{m=1}^{M} \sum_{h \in I_m^{ini}} (\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})^{\mathrm{T}}, \tag{3.11}$$

The inter-class scatter matrix, which describes how close the data points within a class, can be given by:

$$\mathcal{B} = \sum_{m=1}^{M} k_m (\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}})^{\mathrm{T}}, \tag{3.12}$$

where $\bar{\boldsymbol{h}}$ is the total mean vector given by $\bar{\boldsymbol{h}} = \frac{1}{k} \sum_{m=1}^{M} k_m \bar{\boldsymbol{h}}_{\boldsymbol{m}}$. To find the best solution for (3.8), Fisher's criterion is adopted in which the means between each class after the projection should be as far as possible and the variance should be as small as possible. This criterion can be written as (3.13) by using the inter-class scatter matrix and the intra-class scatter matrix.

$$\max_{\delta} \frac{\boldsymbol{\Phi}^T \mathcal{B} \boldsymbol{\Phi}}{\boldsymbol{\Phi}^T \mathcal{W} \boldsymbol{\Phi}}, \tag{3.13}$$

where $\boldsymbol{\Phi}$ is the linear transformation matrix of the original dataset. To find the perfect linear transformation to minimize P_{MD} of (3.6), (3.13) can be reformulated with the help of General-

ized Rayleigh quotient [67] as:

$$\mathcal{B}\mathbf{\Phi} = \boldsymbol{\lambda}\mathcal{W}\mathbf{\Phi}, \tag{3.14}$$

where $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_N]^{\mathrm{T}}$ are the eigenvalues of the transformation matrix $\mathbf{\Phi}$. If W is non-singular, $\mathbf{\Phi}$ can be solved by calculating the eigenvalues and the eigenvectors of all attributes of the dataset. Each eigenvector describes one axis of the transformed space and the corresponding eigenvalue represents the ability to discriminate between different classes. The eigenvector with the highest eigenvalue carries the majority of information about the distribution of the data. Hence, the highest eigenvalues and the corresponding attributes are chosen to formulate the new space.

As described in (3.3), the Euclidean distance between the new estimation and the trusted estimation is calculated to verify if the characteristics of the m-th UAV has changed suddenly. In the authentication instance at time t, the cross-layer estimation can be written as $\boldsymbol{h}_t$. The Euclidean distance after the linear transformation between the new estimation and the trusted estimation can then be written as $d(\boldsymbol{h}_t\mathbf{\Phi}, \bar{\boldsymbol{h}}_m\mathbf{\Phi})$.

Therefore, the binary authentication decision described in (3.4) after the linear transformation can be transformed to:

$$C(\boldsymbol{h}_t) = \begin{cases} \Psi_0, & d(\boldsymbol{h}_t\mathbf{\Phi}, \bar{\boldsymbol{h}}_m\mathbf{\Phi}) \leq \delta; \\ \Psi_1, & d(\boldsymbol{h}_t\mathbf{\Phi}, \bar{\boldsymbol{h}}_m\mathbf{\Phi}) > \delta. \end{cases} \tag{3.15}$$

Hence, if the cross-layer attributes between the new estimation and the record is similar ($d(\boldsymbol{h}_t\mathbf{\Phi}, \bar{\boldsymbol{h}}_m\mathbf{\Phi}) \leq \delta$), the device will be authenticated as a legitimate device (Ψ_0). Similarly, if the cross-layer attributes are significantly different from the record ($d(\boldsymbol{x}_t\mathbf{\Phi}, \bar{\boldsymbol{h}}_m\mathbf{\Phi}) > \delta$), the device will be authenticated as a spoofing device (Ψ_1). However, a small δ value can increase the overall error rate of (3.7) since the fluctuation in the cross-layer attributes can lead to a false rejection. Similarly, a high δ value also increases the error rate since the difference of the cross-layer attributes between the legitimate devices and the attacker can be deemed as a

regular fluctuation. Hence, the choice of δ should be neither too sensitive nor too tolerant to the fluctuations and should be chosen accordingly across different scenarios. The proposed LDA-based authentication scheme is shown in Algorithm 3.1.

Remark To minimize P_{FA} and P_{MD} of (3.5) and (3.6), the cross-layer attributes between different UAVs should be separated far enough so that a correct authentication decision can be forged by using (3.15) with a appropriate δ value. Hence, the projection of the original space has to maximize the separation of the classes and minimize difference within the class which fulfills (3.13).

Algorithm 3.1 LDA-based Authentication

Given the total number of cross-layer attributes included for the authentication for each observation by N. The estimations observed of the m-th UAV are given as $\boldsymbol{H_m} = (H_{m1}, H_{m2}, \ldots, H_{mN})^{\text{T}}$, and the total number of UAVs in the network is M. The authentication happens at instance t.

1: The on-duty CH initializes the cross-layer attributes collection by broadcasting the "Initialization packet" to all UAVs in the system.
2: All UAVs constantly reply to the on-duty CH.
3: The on-duty CH collects all the "reply packets" as the initial dataset with trusted labels.
4: At instance t, an authentication process is triggered and the CH observes the cross-layer attributes.
5: The on-duty CH adds the observed data into the trusted dataset.
6: The on-duty CH calculates the in-class variance and between-class variance to obtain the linear transformation of the updated dataset according to (3.11) and (3.12).
7: The on-duty CH performs the linear transformation to get the projection of the original space then calculates the Euclidean distance between the observation.
8: **if** $d(t\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}) < \delta$ **then**
9: authenticates the m-th UAV as a legitimate device.
10: **else**
11: authenticates the m-th UAV as an attacker.
12: **end if**
13: Update the trusted dataset by adding the new estimations at instance t if they are from legitimate UAVs.

3.4.2 Adaptive Cross-layer Attribute Selection Algorithm

Although the LDA technique can reduce the dimensionality of the cross-layer estimations, it requires the operator to set the number of attributes being left after the linear transformation. However, the significance level of each attribute is different across the dynamic environment and the number of useful attributes can also vary from one time to another. Hence, a fixed amount of cross-layer attributes being used for the linear transformation is not suitable to achieve the best performance and minimize the overall latency. In this section, a situation-aware cross-layer attribute selection algorithm (see Algorithm 3.2) is developed to select the minimum amount of cross-layer attributes while maintaining the overall performance across different scenarios. The unique combination across different scenarios also increases the overall security of the entire system.

As shown in (3.14), the eigenvalue, which evaluates the level of significance of the cross-layer attributes, is required to compute the linear transformation matrix. The different choices of cross-layer attributes will result in an individual linear transformation matrix. Ideally, a minimum amount of cross-layer attributes should be selected to reduce the complexity while maintaining the maximum amount of information after the linear transformation. Hence, only the cross-layer attributes with high eigenvalues should be kept after the projection. To achieve this goal, a threshold can be set to only choose the necessary amount of eigenvalues under the dynamic environment. However, there is no upper limit for the eigenvalues ($\boldsymbol{\lambda}$), which indicates that it is impossible to set a fixed eigenvalue threshold. Therefore, we convert $\boldsymbol{\lambda}$ into a percentage scale as:

$$\boldsymbol{P}_{\lambda} = [P_{\lambda_1}, P_{\lambda_2}, ...P_{\lambda_N}]^{\mathrm{T}}, \tag{3.16}$$

such that $P_{\lambda_1} + P_{\lambda_2} + ... + P_{\lambda_N} = 100\%$. In this case, P_{λ_1} has the highest eigenvalue in percentage scale and P_{λ_N} has the lowest eigenvalue in percentage scale. The information threshold (τ) can then be chosen by the users according to the specific application scenario and then be used to

choose the minimum number of top cross-layer attributes as follows:

$$\tau \leq P_{\lambda_1} + P_{\lambda_2} + ... + P_{\lambda_\upsilon}, \tag{3.17}$$

where $\upsilon = 1, 2, ..., N-1$ and the goal of attribute selection can be rewritten as:

$$\min_{\upsilon}(P_{\lambda_1} + P_{\lambda_2} + ... + P_{\lambda_\upsilon} - \tau). \tag{3.18}$$

A higher τ value generally indicates that more attributes will be kept after the LDA process. However, a τ value that is close to 100% does not guarantee to use of all attributes since some of the attributes do not contribute or even have a negative impact on the authentication. For example, in a certain environment where the transmission switches between line-of-sight and non-line-of-sight frequently, the CIR can vary significantly even if the device is the same. Moreover, sometimes the authentication system does not require a highest τ value to reach the best performance; hence, the τ value should be selected based on the environment and the performance requirements accordingly. The characteristic of the τ value will be tested and shown in the performance evaluation. The detailed process is shown in Algorithm 3.2.

Algorithm 3.2 Adaptive Cross-layer Attribute Selection Algorithm

Given the combined cross-layer attributes ($\boldsymbol{H}$) which consists of the initial verified cross-layer estimation ($\boldsymbol{H^I}$) collected in *Phase I* and the cross-layer attributes ($\boldsymbol{H^{II}}$) freshly collected in *Phase II* at time t.

1: Obtain the eigenvalue of each cross-layer attribute.
2: Covert the eigenvalues into a percentage scale $\boldsymbol{P}_\lambda$.
3: Rank the component of $\boldsymbol{P}_\lambda$ from high to low where P_{λ_1} has the highest percentage score.
4: Sum up P_{λ_1} to P_{λ_υ} such that the summation is greater or equal than τ with the minimum value of υ.
5: Use the top υ cross-layer attributes for LDA dimensional reduction.

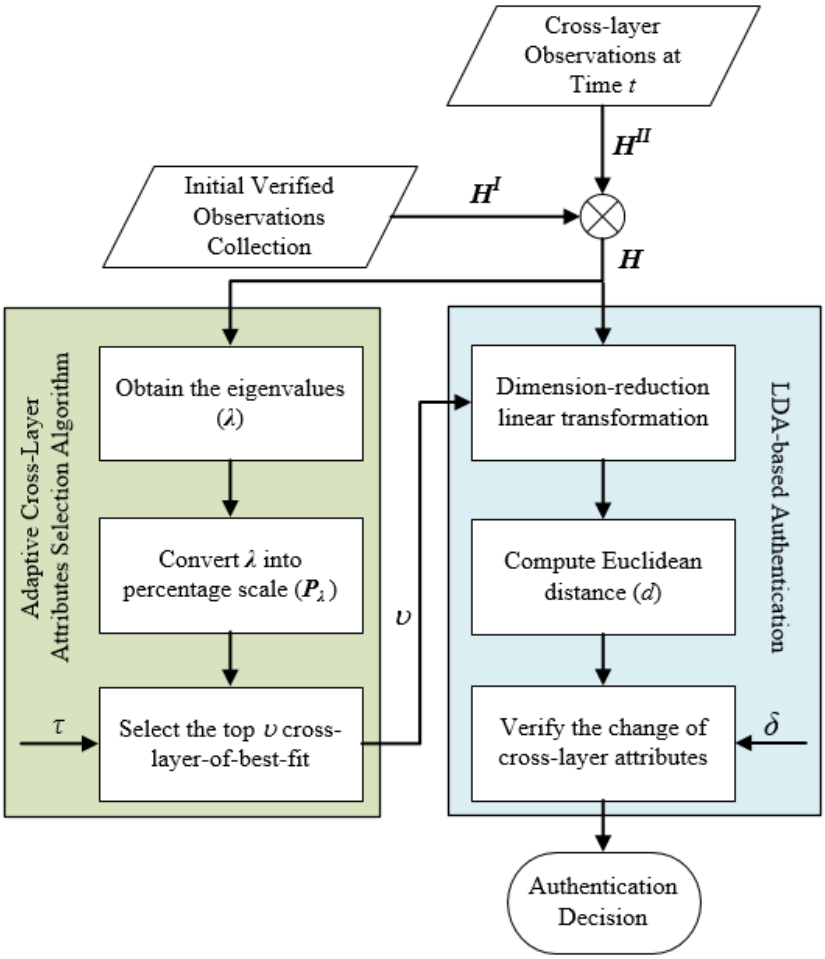

Figure 3.2: Flow chart of the adaptive LDA-based cross-layer authentication scheme

To summarize both algorithms together, a flow chart of the authentication at instance t is shown below in Fig. 3.2. In this case, the cross-layer observations ($\boldsymbol{H^{II}}$) collected at instance t before the CH selection and CH switching is combined with the trusted cross-layer attributes ($\boldsymbol{H^{I}}$) and forms the combined cross-layer attributes set ($\boldsymbol{H}$). The adaptive cross-layer attribute selection algorithm is used to find the minimum amount (υ) of the cross-layer attributes according to τ. The top υ attributes being selected are then passed to the LDA-based authentication scheme where the authentication output is generated by using the input $\boldsymbol{H}$ and δ.

3.5 Simulation Results

In this section, the performance analysis of the proposed scheme is given. A dynamic UAV swarm is constructed by using the MATLAB 2020a to simulate the cross-layer attributes data. Each UAV has a random motion path with 300 observations and the analysis represents the last of the 5 simulations that have been initialized differently. All simulations have similar results. We consider a 3D movement where the flight height varies between 150 to 300m in the urban area and 10m to 40m in the rural area [68]. The maximum diameter of the UAV swarm is 10m in the urban area and 30m in the rural area. The Friis equation is utilized to model the path-loss and the Doppler shift is considered due to the high relative velocity under the rural area [69]. The height-dependent Rician factor is considered in the line-of-sight condition under the rural area and the Rayleigh fading distribution is considered in the non-line-of-sight condition under the urban area. To construct the transition period, the flight height and the velocity of each UAV varies gradually; hence, the changes in relative locations lead to new channel conditions. The channel model is gradually switched from the non-line-of-sight condition to the line-of-sight condition. The cross-layer attributes contain RSSI, CFO, CIR and I/Q imbalance from the physical-layer, PER from the data link layer, latitude and longitude from the application layer. The cross-layer attributes are stored into .CSV files to be analyzed in Python 3.8.

To study the performance of our proposed scheme, we consider 3 cases that include 4, 8 and 12 UAVs to represent the potential size of the UAV swarm. To evaluate the error rate of (3.7), we assume the cost of false alarm and the miss detection is the same which means w_1 and w_2 are both 0.5. We then compare our proposed scheme to the other state-of-the-art light-weight cross-layer centralized authentication techniques for both the accuracy performance and the computational complexity.

3.5.1 Performance Analysis of Proposed LDA-aided Authentication Scheme

To optimize the performance of LDA, an assumption is that the input attributes follow the normal distribution. Since some of the attributes do not follow this distribution, the box-cox transformation has been utilized to transform the original data into as close to a normal distribution as possible. Then, to equalize the weight of each attribute, the data standardization has been performed to rescale the attributes so that the mean equals 0 and the standard deviation equals 1.

3.5.1.1 Information Threshold (τ)

To understand the relationship between the proposed adaptive cross-layer attribute selection mechanism and τ, we conduct the simulation in Python by using the data harvests from MATLAB and the τ values we choose are between τ=1% and τ=99%. The reason that τ cannot reach 100% is that the converted percentage eigenvalue may not add up to 100% after being rounded. Hence, we summarize the τ ranges with the corresponding amount of cross-layer attributes being kept after the dimension reduction for 4 UAVs in Table 3.2, 8 UAVs in Table 3.3 and 12 UAVs in Table 3.4. The chosen sample is from a random instance in the early transition period since the channel condition is more complicated than the rural area or the urban area.

Table 3.2: Information Threshold Range (τ) and the Corresponding Number of Attribute(s) (4 UAVs)

τ range	attribute(s) selected	Total Number
$\tau < 91\%$	CFO	1
$91\% \leq \tau \leq 98\%$	CFO, RSSI	2
$98\% < \tau \leq 99\%$	CFO, RSSI, Longitude	3

Among the 7 cross-layer attributes contained in the dataset, only 3 attributes are selected by using our algorithm when 99% of the information is kept for analysis in all 3 scenarios. The eigenvalues range from 0.0001 which is PER in the case of 8 UAVs to 34.9226 which is CFO in the case of 4 UAVs. This demonstrates that the eigenvalue can have a significant weight

Table 3.3: Information Threshold Range (τ) and the Corresponding Number of Attribute(s) (8 UAVs)

τ range	attribute(s) selected	Total Number
$\tau < 82\%$	RSSI	1
$82\% \leq \tau \leq 98\%$	RSSI, CFO	2
$98\% < \tau \leq 99\%$	RSSI, CFO, Latitude	3

Table 3.4: Information Threshold Range (τ) and the Corresponding Number of Attribute(s) (12 UAVs)

τ range	attribute(s) selected	Total Number
$\tau < 73\%$	CFO	1
$73\% \leq \tau \leq 96\%$	CFO, RSSI	2
$96\% < \tau \leq 99\%$	CFO, RSSI, Latitude	3

difference; therefore, it is not feasible to utilize an eigenvalue threshold without transforming it into the percentaged scale. By using the LDA for dimensionality reduction, the amount of data is shrunk into half of the original data size which ultimately lowers the computational overhead when the estimations are getting bigger.

To further study the relationship between τ and the error rate, we plot all 9 cases as listed in Table 3.2, Table 3.3 and Table 3.4. To make it comparison more clear, we plot two separate figures as shown below.

As shown in Fig. 3.3, it can be observed that when τ is small, the performance is less accurate and less stable compared to the higher τ value. However, as shown in Fig. 3.4, it can be shown that when the τ value is at the higher range, there is not much performance increase. Therefore, it can be concluded that the computational overhead can be further decreased by adopting the proper τ range in each application. However, to select the τ value safely, $\tau = 99\%$ can always be used as a starting point. The cross-layer attributes can then be collected after each mission to compute a lower τ value to minimize the computational overhead in future applications.

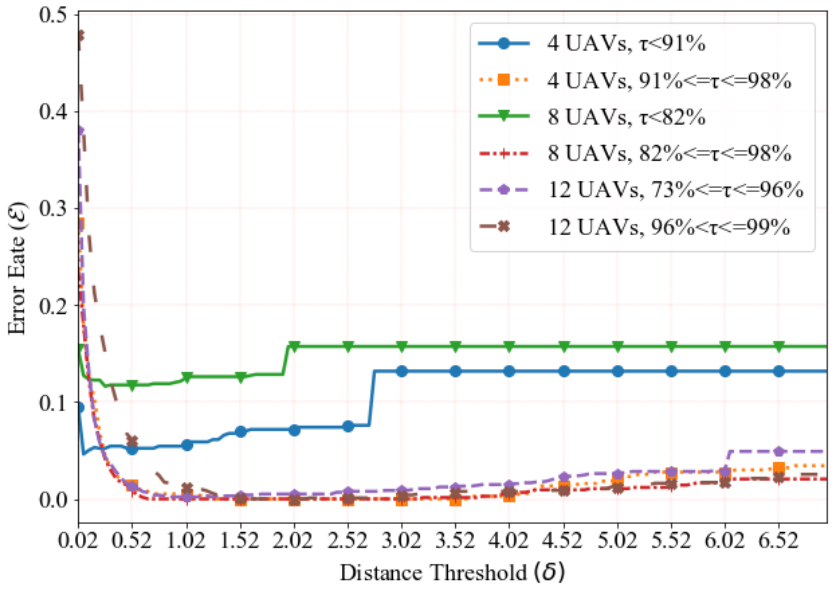

Figure 3.3: The error rate vs. the distance threshold at the lower τ ranges.

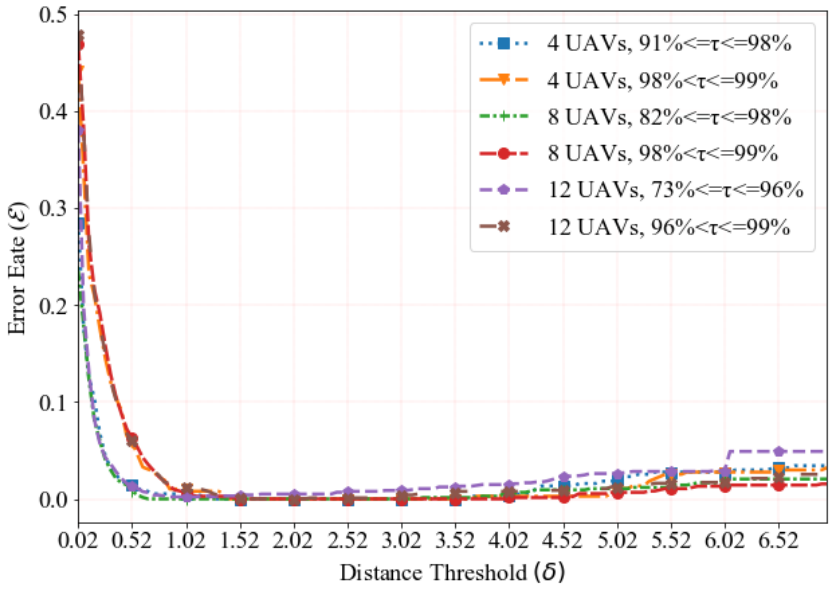

Figure 3.4: The error rate vs. the distance threshold at the higher τ ranges.

3.5.1.2 Euclidean Distance Threshold (δ)

As the security constraint of separating the eavesdropping device from legitimate UAVs, the choice of δ is critical. To study the impact of δ in different scenarios, we use the same Fig. 3.3 and Fig. 3.4 as shown in the previous section. The range of the distance threshold is [0.02, 7.02] with a step of 0.05. The threshold cannot start from 0 since it will reject all estimations with any difference.

It is demonstrated that δ has a different impact on the error rate of (3.7) across different scenarios. From the 2 figures above, we can conclude that when δ grows, the common trend of the error rate will decrease first, then become stable and increase at the end. The reason behind this is that when δ is too small, a small change of a legitimate device will be flagged as a spoofing device which increases P_{FA}. Similarly, when δ is too big, the difference between a spoofing device and a legitimate device will only be considered as a normal fluctuation which increases the P_{MD}. The best result for all 3 sizes of UAV swarms are shown in Table 3.5

Table 3.5: The relationship between δ and other parameters

Swarm size	τ range	Best $\mathcal{E}$ value	δ value
4 UAVs	$\tau < 91\%$	0.046	0.07
	$91\% \leq \tau \leq 98\%$	0	[1.27,3.62]
	$98\% < \tau \leq 99\%$	0	[1.42,3.67]
8 UAVs	$\tau < 82\%$	0.118	[0.32,0.67]
	$82\% \leq \tau \leq 98\%$	0	[0.67,3.17]
	$98\% < \tau \leq 99\%$	0	[1.52,3.97]
12 UAVs	$\tau < 73\%$	0.132	0.27
	$73\% \leq \tau \leq 96\%$	0.002	[0.87,1.12]
	$96\% < \tau \leq 99\%$	0	[1.57,2.12]

From Table 3.5, it can be concluded that the optimized δ value is subjective to the environment and the size of the UAV swarm. The reason is that the cross-layer attributes are rescaled after the LDA transformation. To fulfill (3.8), δ should be selected within the range where the calculated error rate is minimized by using the previously collected cross-layer attributes.

3.5.1.3 LDA-based Attributes Reduction

In Fig. 3.5, we compare the performance of the proposed LDA-based authentication scheme with the non-LDA-based authentication across the 3 cases that include 4, 8 and 12 UAVs. The non-LDA-based scheme goes through the same process for the Euclidean-distance-based authentication as the proposed scheme. It can be observed from Fig. 3.5 that the performance of the non-LDA-based authentication becomes less accurate when the number of UAVs grows. This demonstrates that the unnecessary attributes, such as the change of CIR under the environment where the multipath condition varies quickly, can negatively impact the authentication decision. Hence, it can be concluded that the accuracy performance can become more reliable and more stable across different scenarios by eliminating the unnecessary attributes with the help of the LDA.

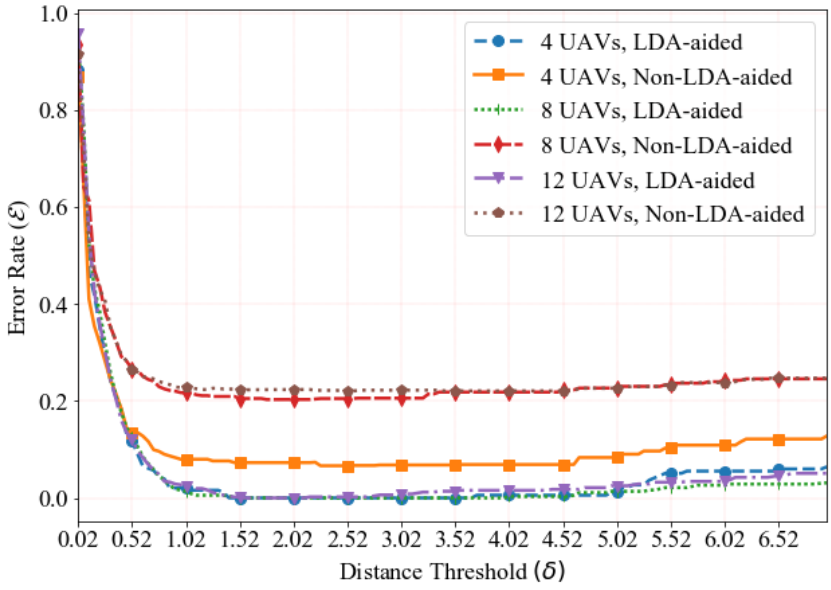

Figure 3.5: Error rate comparison results of our LDA-based scheme and the non-LDA-based scheme

3.5.1.4 Cross-layer Attributes

To test the significance of the cross-layer attributes, we extract separate physical-layer attributes based datasets from the original cross-layer dataset in all 3 scenarios. The LDA process is

applied to the physical-layer attributes only dataset for consistency. The best result of the LDA aided physical-layer attributes only dataset versus the best result of the LDA aided cross-layer attributes dataset are shown in Fig. 3.6 for all 3 scenarios.

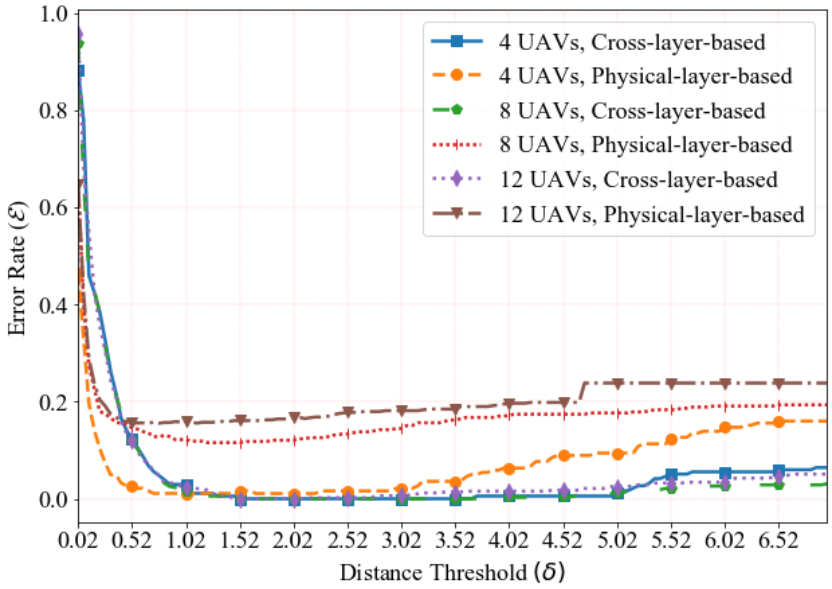

Figure 3.6: Error rate comparison results between the cross-layer observation and physical-layer observation

It can be observed from Fig. 3.6 that the LDA aided physical-layer attributes based dataset carries the same trend as the cross-layer attributes dataset. The performance of the cross-layer attributes dataset is significantly better than the physical-layer attributes only dataset when the number of UAVs grows to 12. More importantly, the error rate of the cross-layer attributes dataset is significantly more stable than the physical-layer attributes only dataset across different scenarios. This proves that the cross-layer attributes are more stable under a dynamic environment and are more robust when the number of UAVs increases compares to the physical-layer attributes.

3.5.2 Performance Comparison with Other Authentication Techniques

In this section, we compare our proposed scheme to the fast authentication scheme for the dynamic sensor networks proposed by Zhang *et al.* [70] and the enhanced cross-layer authen-

tication scheme proposed by Hao *et al.* [71] We first compare the best accuracy performance and then the computational complexity by using the same data collected in the MATLAB.

Fig. 3.7 characterizes the error rate comparison between our LDA-based authentication scheme and the other state-of-the-art cross-layer light-weight authentication techniques. It can be observed that our proposed scheme achieves an error rate of 0 in all 3 cases which are the highest among all. This demonstrates that the other 2 techniques are not suitable under the UAV network. The high mobility makes the physical-layer estimation less reliable and the final decision of the fast authentication for dynamic sensor networks is still based on the physical-layer estimation. Similarly, the RSSI collected in the enhanced cross-layer authentication scheme is not reliable. Since only 2 attributes are being selected, the overall stability and reliability are low in our UAV network.

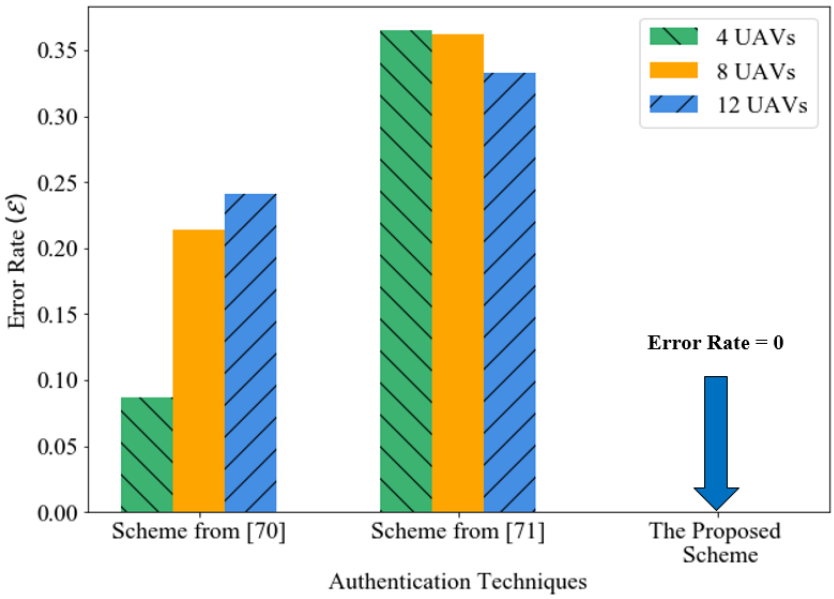

Figure 3.7: Accuracy performance comparison between different state-of-the-art cross-layer authentication techniques

Theoretically, the time complexity for all three schemes is $O(N)$ which means all three schemes should have a similar time complexity in the worst-case scenario. However, the actual overhead of our proposed scheme and the scheme proposed by Zhang *et al.* can vary a lot based on the environment. The scheme proposed by Hao *et al.* goes through all the attributes

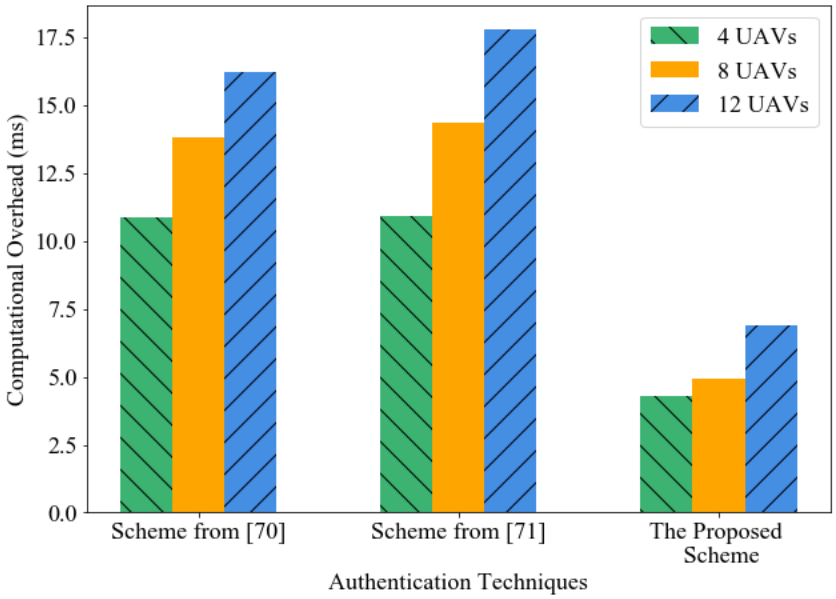

Figure 3.8: Computational overhead comparison between different state-of-the-art cross-layer authentication techniques

without dropping any attributes while the scheme proposed by Zhang *et al.* can switch between using physical-layer authentication only or using both the physical-layer and the upper-layer authentication to limit the overhead. The overhead of our proposed scheme is more subjective to the environment since it can select a different combination of attributes based on situational-awareness. To examine the computational overhead, we selected the worst scenario case in the transition period where both the physical-layer attributes and the upper-layer attributes need to be selected. The Central Processing Unit (CPU) processing time is measured to quantify the overhead in nanosecond level as shown in Fig. 3.8. It can be observed that our proposed scheme can have a relatively low computational overhead by eliminating the unnecessary attributes.

3.6 Chapter Summary

In this chapter, an edge intelligence-enabled centralized authentication mechanism has been proposed to enhance the security in the UAV swarm. This multi-dimensional authentication scheme was planted in the on-duty CH to verify whether the candidate UAVs are legitimate

across different environments. The cross-layer attributes have been utilized to enhance security by providing more reliable and unique characteristics of each UAV. Our novel LDA-aided authentication scheme increases the trust value while decreasing the computational overhead by eliminating the unnecessary attributes. Since the LDA technique could not decide the number of attributes being left after the dimensionality reduction, a situation-aware attributes selection algorithm has been proposed to select the minimum amount of attributes without jeopardizing the performance. A series of simulations were conducted to demonstrate the impact of different parameters on the authentication performance of our proposed scheme. A comparison with the other state-of-the-art light-weight cross-layer authentication techniques is also included. The results showed that our proposed scheme can remove the unnecessary cross-layer attributes and vastly improve the authentication accuracy in the UAV network.

In the next chapter, the soft authentication scheme will be comprehensively designed that can be further compatible with the decentralized authentication scheme. To be more specific, the centralized authentication techniques may not be sufficient to support the authentication performance requirement under a harsh environment. The decentralized authentication scheme may be further considered so that a more accurate authentication decision can be fused from utilizing multiple edge authentication nodes. To carry forward the uncertainty of each authentication node, a probability-based soft authentication decision scheme is designed to be implemented at the authentication node to quantify the probability of legitimacy for the authentication requester. By introducing the soft authentication decisions, the less confident authentication nodes will have less impact on the final authentication decision which increases the reliability and robustness of the authentication mechanism.

Chapter 4

Soft Edge Authentication Scheme in Decentralized UAV Network

In the LDA-based centralized authentication designed in the last chapter, the cross-layer attributes have been utilized to compensate for the imperfect estimations of the physical-layer observations. However, the single-point failure is still an unsolved challenge for the centralized topology. In this chapter, the decentralized authentication topology has been considered to fuse multiple physical-layer-based edge authentication decisions into a final authentication judgement. Since each node has a different level of authentication accuracy, it is unwise to give each node an equal weight when fusing the final authentication decision. Therefore, we propose a probability-based soft authentication scheme that can be implemented at each collaborative node to combine the weight into the edge authentication decision. This soft authentication decision is then utilized to fuse the edge authentication where the more confident nodes have more impact on the final authentication decision and vice versa. A performance evaluation is also included in the simulation section.

4.1 Introduction

The conventional authentication techniques usually generate a binary decision to judge whether the authentication requester is legitimate or not. This is suitable in the digital security schemes, such as the cryptographic-based authentication scheme, since the security key either matches or not matches the record. However, it is almost impossible for the central collaborative node to verify the true identity of the authentication requester once the security key is compromised by the brute force attack [72]. Hence, the analog-based physical-layer authentication schemes are developed to utilize the unique channel-based and hardware-based attributes to differentiate the legitimate devices from the attackers. Nevertheless, the attackers may initiate active eavesdropping attacks to jam the main communication channel and degrade the physical-layer estimation accuracy and may result in a single-point failure under the centralized authentication topology [27].

To compensate for the single-point failure, various types of decentralized authentication techniques have been developed in which multiple collaborative nodes are utilized to form a final authentication decision. Rather than using the digital-based authentication scheme, the physical-layer authentication scheme can be implemented at each node to seamlessly generate edge authentication decisions. However, the varying channel and potential attacks increase the difficulty for the analog-based authentication schemes to formulate equally reliable authentication decisions at each collaborative node. Hence, the uncertainty at each collaborative node should be considered as a factor when fusing the final authentication decision such that the more confident collaborative nodes can have more impact on the final authentication decision and vice versa.

In this chapter, we propose an algorithm to generate a soft authentication decision that reflects the level of confidence as a factor to fuse the final authentication decision by considering the authentication uncertainty. The probability of legitimacy is generated as the soft authentication decision and is evaluated between [0,1]. To be more specific, 0 indicates that the authentication requester is absolutely illegitimate and 1 indicates that the authentication requester

is absolutely legitimate. It is unlikely to achieve the extreme boundaries due to the imperfect estimations and environmental changes. By submitting a soft authentication decision, the less reliable collaborative nodes will have less impact on the final authentication decision which then improves both the reliability and robustness in the decentralized authentication applications.

4.2 System Model

As shown in Fig. 4.1, we consider a UAV swarm that consists of M UAVs including a CH and coexisted spoofing devices that try to impersonate a legitimate UAV for illegal purposes. At an instance t, the CH aims to authenticate the claimed UAV m by fusing the edge authentication decisions from the available collaborative nodes. The soft authentication decisions are generated to include the uncertainty from each collaborative node and reflect the level of confidence as a factor to fuse the final authentication decision. The process of the decentralized authentication contains three phases:

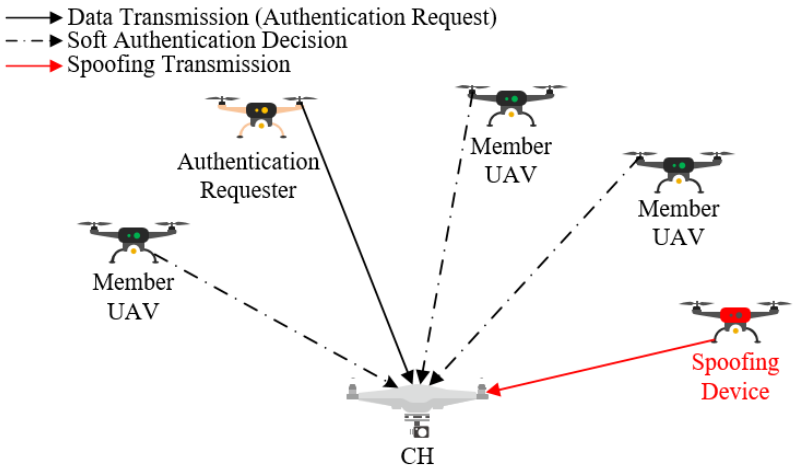

Figure 4.1: System model. Decentralized UAV swarm network topology. The final authentication decision utilizes the physical-layer-based edge authentication decisions from the available collaborative nodes.

Phase I: At the time t_1, either a legitimate UAV or an attacker transmits one or more messages to the CH. All the UAVs observe a noisy physical-layer estimation and the estimation at UAV m is given as:

$$\boldsymbol{H_m^I} = (H_{m1}^I, H_{m2}^I, \ldots, H_{mN}^I)^{\mathrm{T}}, \tag{4.1}$$

where N is the number of physical-layer attributes and $()^{\mathrm{T}}$ is the transposition of the vector. The attributes may include the RSSI, CFO, I/Q imbalance and so on.

Phase II: At the time t_2, the selected collaborative node, for example UAV m, a soft edge authentication ϕ_m is generated and passed to the CH where $\phi_m = [0, 1]$.

Phase III: At time t_3, since some of the member UAVs may be busy at the moment, the CH generates the final authentication decision based on the K received edge authentication decision as:

$$\begin{cases} \Phi_0, & \frac{1}{K}\sum_{k=1}^{K}\phi_k > \nu; \\ \Phi_1, & \frac{1}{K}\sum_{k=1}^{K}\phi_k \leq \nu, \end{cases} \tag{4.2}$$

where v is the authentication decision threshold in the range of $[0, 1]$.

4.3 Problem Formulation

To evaluate the performance of the decentralized authentication, the False Alarm rate and the Miss Detection rate are considered and can be expressed as:

1) False Alarm (FA) rate: The probability that the legitimate UAV is rejected as a spoofing device. The function can be given as:

$$P_{\mathrm{FA}} = \Pr(\frac{1}{K}\sum_{k=1}^{K}\phi_k \leq \nu|\Phi_0). \tag{4.3}$$

2) Miss Detection (MD) rate: The probability that the spoofing device is approved as a

legitimate UAV. It can be defined as:

$$P_{\mathrm{MD}} = \Pr(\frac{1}{K}\sum_{k=1}^{K}\phi_k > \nu|\Phi_1). \tag{4.4}$$

To evaluate the accuracy and robustness of the decentralized authentication, the false alarm rate and the miss detection rate can be combined as the error rate ($\mathcal{E}$) as

$$\mathcal{E} = w_1 P_{\mathrm{FA}} + w_2 P_{\mathrm{MD}}, \tag{4.5}$$

where w_1 and w_2 are the costs of the false alarm and the miss detection. The false alarm and the miss detection can be treated equally; however, under certain applications, the miss detection may cause more damage to the system than the false alarm and may have a higher cost. Hence, to achieve the best authentication performance, both the false alarm rate and the miss detection rate should be minimized. Hence, the problem formulation of this chapter can then be formulated as:

$$\min_{v} \mathcal{E}, \tag{4.6}$$

where v is the authentication threshold in the final binary hypothesis test..

4.4 Soft Authentication Decision Algorithm

The classical authentication only outputs two decisions, true or false, while the soft authentication produces gradual decisions. This further reflects the uncertainty of each node which ultimately enhances the robustness of the final authentication decision if the authentication decisions from multiple collaborative nodes are fused together. To generate a continuous soft authentication decision, the probability of legitimacy is considered to be evaluated at the collaborative node with respect to the authentication requester. To be more specific, this soft authentication decision evaluates how likely the authentication requester is legitimate where a

value of 0 indicates that the authentication requester is absolutely an attacker and a value of 1 indicates that the authentication requester is absolutely a legitimate device. The soft authentication decision can be anywhere between 0 and 1 to reflect the probability of legitimacy under different authentication techniques. In our case, we would like to design a soft authentication scheme that evaluates the probability of legitimacy by utilizing the physical-layer estimations. The uncertainty caused by the inaccurate estimations in the time and spatial domain can be carried forward to fuse the final authentication decision which enhances the overall system robustness.

Ideally, to generate the soft authentication decision, there exists an optimized regression model that maps the physical-layer attributes to the probability of legitimacy. However, it is extremely difficult to fit such a model to calculate the probability between [0,1] since the boundary of the regression model is usually $(-\infty, \infty)$ [73]. Hence, to simplify the regression model, we utilize the natural logarithmic of the odd, also known as the logit, so that the domain is relaxed to $(-\infty, \infty)$ [74]. The logit (L) is the natural log of the ratio between the probability of being legitimate and the probability of being illegitimate. Since the identity of the UAV obeys Bernoulli distribution, the logit can be derived as:

$$L = ln(\frac{P(\Phi_0)}{P(\Phi_1)}) = ln(\frac{P(\Phi_0)}{1 - P(\Phi_0)}), \tag{4.7}$$

where Φ_0 means the device is legitimate and Φ_1 means the device is illegitimate. To find the probability ($P(\Phi_0)$), we assume that there exists an optimized regression model that maps the physical-layer attributes to the logit. This regression model can be calculated by different regression techniques such as linear regression, multivariate regression and non-linear regression such that the authentication system can be further customized. Therefore, (4.7) can be rewritten as:

$$ln(\frac{P(\Phi_0)}{1 - P(\Phi_0)}) = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{X}, \tag{4.8}$$

where $\boldsymbol{B}$ is the vector of the optimized regression coefficient that can be estimated by the operator selected regression technique. $\boldsymbol{X}$ is the vector of the physical-layer attributes. Therefore, by combining (4.7) and (4.8), the probability $P(\Phi_0)$ can be calculated as:

$$\begin{aligned} P(\Phi_0) &= e^{(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{X})}(1 - P(\Phi_0)) \\ &= e^{(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{X})} - e^{(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{X})}P(\Phi_0) \\ &= \frac{e^{(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{X})}}{1 + e^{(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{X})}}, \end{aligned} \tag{4.9}$$

where $P(\Phi_0)$ can then be deemed as the soft authentication output (ϕ_m) at the member UAV m. This soft authentication decision algorithm is given in Algorithm 4.1.

Algorithm 4.1 Soft Authentication Decision Algorithm

1: compute the optimized regression coefficient ($\boldsymbol{B}$) via the operator defined regression technique;
2: compute the soft edge authentication decision (ϕ_m) via (4.9);
3: **if** the UAV is a member UAV **then**
4: transmit ϕ_m to CH;
5: **end if**

4.5 Performance Evaluation

In this section, the performance analysis of the proposed scheme is given. The UAV network is constructed using MATLAB 2020a. A dynamic environment with 600 observations is constructed in which both the urban area and rural area are considered with a transition period. Each UAV has a random motion path and the analysis represents the last of the 5 simulations that have been initialized differently. All simulations have similar results. We consider a 3D movement where the flight height varies between 150 to 300m in the urban area and 10m to 40m in the rural area [68]. The Friis equation is utilized to model the path-loss and the Doppler shift is considered due to the high relative velocity under the rural area [69]. The height-dependent Rician factor is considered in the line-of-sight condition under the rural area

and the Rayleigh fading distribution is considered in the non-line-of-sight condition under the urban area. To construct the transition period, the flight height and the velocity of each UAV varies gradually; hence, the changes in relative locations lead to new channel conditions. The channel model is gradually switched from the non-line-of-sight condition to the line-of-sight condition. A sudden environment change is also included by tuning the multipath condition (i.e., from a rich multipath environment to a low multipath environment) within the transition period to test the robustness of our proposed scheme.

To examine the performance of our proposed scheme, we compare our scheme to the traditional binary hypothesis test utilizing the K-nearest-neighbour (KNN) technique from [75]. The w_1 and w_2 in (4.5) are considered to have a equal weight of 0.5 in this case. We consider 3 different cases where 2, 4, and 6 collaborative nodes are involved in generating the soft and binary authentication decisions. The physical-layer attributes used to generate both authentication decisions are exactly the same. The linear regression, logistic regression and multivariate regression have been considered at each node to compute the soft authentication decision. To make sure the comparisons between different UAV swarm sizes are clear, we plot two separate figures as shown below. The same UAV swarm with 4 UAVs is included in both figures as a benchmark.

As shown in Fig. 4.2 and Fig. 4.3, we compare the KNN-based binary authentication decision with our proposed scheme under the 2 UAVs 4 UAVs and 6 UAVs scenario. It can be observed that both schemes can reach an optimized performance with sufficient observations. However, our proposed scheme can reach the optimized performance with fewer observations which shortens the training stage. On the other hand, it can be observed that when the number of collaborative nodes increases, the error rate at the beginning is usually higher. The reason is that the collaborative nodes need to adjust their confidence level gradually at the beginning to reach maximum performance. However, even though our proposed scheme requires a training period, the performance is still better than the binary authentication decision at the same time instant. Moreover, to further test the robustness and reliability of our proposed scheme,

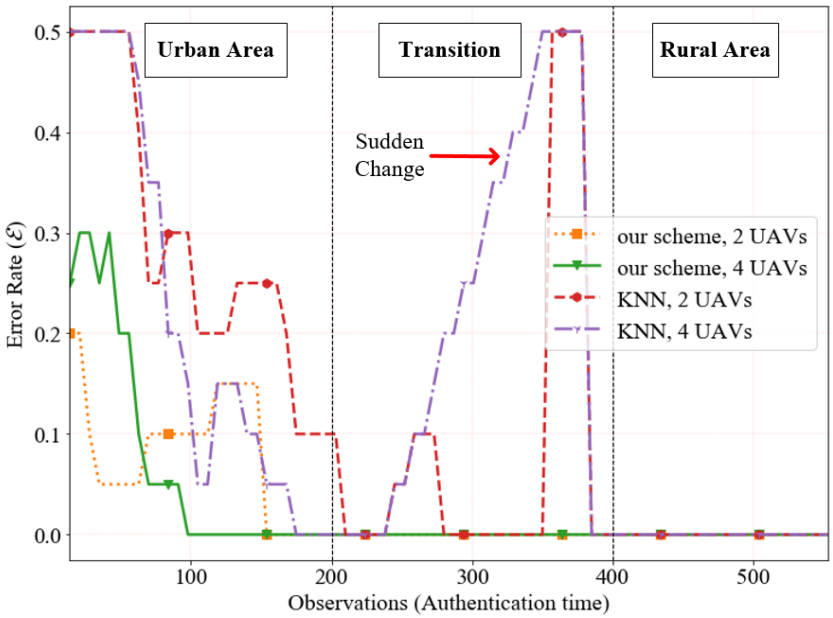

Figure 4.2: Performance comparison between the binary authentication scheme and our proposed scheme (2 and 4 UAVs)

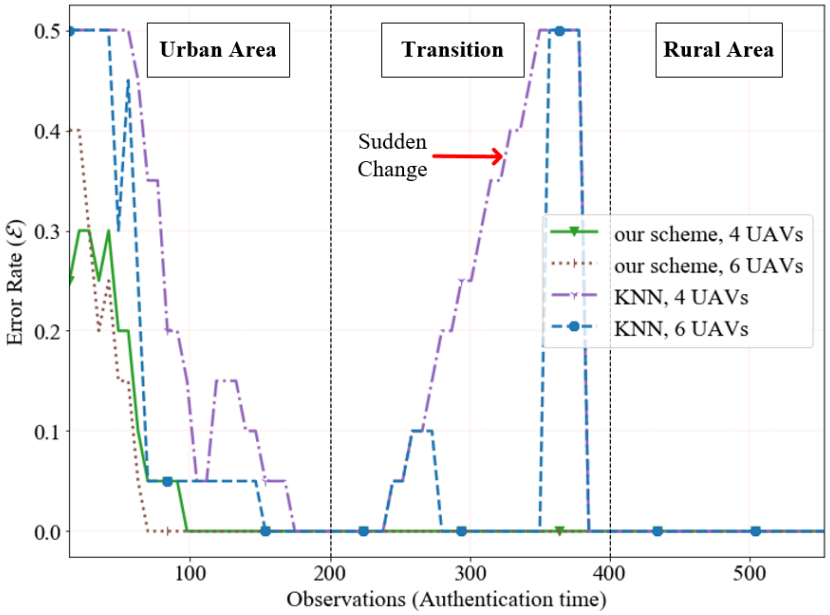

Figure 4.3: Performance comparison between the binary authentication scheme and our proposed scheme (4 and 6 UAVs)

a sudden environment change is added within the transition stage by changing the multipath characteristics as highlighted in the figure. This proves that the imperfect physical-layer estimations and the sudden environment change can be compensated by keeping the uncertainty at each collaborative node.

4.6 Chapter Summary

In this chapter, a soft authentication scheme is proposed to enhance the system robustness by including the uncertainty caused by the imperfect estimations of the analog attributes. To be more specific, by evaluating the probability of legitimacy of the authentication requester at each collaborative node, the less confident collaborative nodes will have less impact on the final authentication decision which ultimately improves the authentication reliability and robustness. From the simulation result, it can be observed that the proposed algorithm can significantly improve the authentication performance under a more complex operating environment.

In the next chapter, a cost minimizing collaborative security provisioning mechanism will be comprehensively designed to guarantee the authentication requirement. Since the centralized authentication techniques may suffer from single point failure while the decentralized authentication techniques increase the overall computational complexity, it is critical to design a fluid authentication topology to balance the performance and the computational cost. To be more specific, when the CH is confident about the authentication decision, a centralized authentication scheme can be adopted. On the other hand, a soft authentication decision-based decentralized authentication scheme will be customized to guarantee performance.

Chapter 5

Guaranteed SoS Provisioning with Minimized Complexity in UAV Swarm

In the previous chapters, a centralized cross-layer-based authentication scheme and a physical-layer-based decentralized authentication scheme have been proposed to enhance the authentication security within the UAV swarm. However, the nature of best-effort-based authentication may not provide a stable and guaranteed security performance across different environments with minimum computational cost. In this chapter, we propose a novel concept of Service-of-Security (SoS) in a decentralized UAV network to guarantee the authentication performance with minimal computational cost based on situational-awareness. The simulation results demonstrate that our scheme can constantly achieve the operator defined authentication performance with a minimum amount of collaborative nodes and better robustness against sudden environmental change.

5.1 Introduction

Due to the open broadcasting nature of the wireless devices, different authentication techniques have been developed to make the UAV networks more secure. To protect the networks from malicious attacks, one of the conventional on-site authentication techniques that can be imple-

mented between the CH and member UAVs is the cryptographic-based centralized authentication scheme. However, these security provisioning techniques can be insufficient once the digital key is compromised by the brute force attack, it is almost impossible for the central node to verify the true identity of the authentication requester and degrade the security performance [76, 77].

To mitigate the security risks caused by the compromised security key, the physical-layer authentication techniques have been developed to extract the unique hardware and channel characteristics of each device for the authentication purpose [78, 79, 44, 45, 46, 80, 81, 82]. However, the performance of the physical-layer authentication schemes cannot be guaranteed due to the imperfect estimation of the specific attribute being used for authentication. The limited dynamic range of the specific attribute is also not sufficient to provide a guaranteed authentication result when the number of devices increases [13]. Ultimately, observing and analyzing multiple attributes and devices at the same instance can create a bottleneck and reduce application traffic [54].

To compensate for the single-point failure and increase the overall reliability, the decentralized authentication technique is developed where a group of collaborative nodes are utilized to fuse a final authentication decision. The physical-layer security provisioning techniques can also be integrated into the decentralized topology [83, 84, 85]. The estimations from multiple devices can compensate for the uncertainty caused by the time-varying environment and imperfect estimations. To optimize the performance of each collaborative node, a different number of physical-layer attributes can be selected at each node based on the hardware computational capability. The difficulty for the attacker to impersonate the legitimate devices is increased since it is extremely hard to predict and impersonate different physical-layer attributes at the same time. Moreover, the distributed authentication techniques do not require a static topology for the authentication process. This can significantly improve the reliability and the robustness of the authentication scheme, especially under a hostile environment, where the connection link between the member UAVs and the CH is intermittent. However, by involving more devices in

the authentication process, the computational complexity and overall network latency will be increased dramatically which raises many challenges in the resource constraint devices.

In a nutshell, one of the major challenges is that the conventional authentication schemes are best-effort based and cannot provide a stable and guaranteed security performance across different application scenarios and environments. On the other hand, some state-of-the-art authentication schemes are capable of achieving robust security performance, but it increases the computational cost and the overall network latency. More importantly, it is extremely challenging to utilize a static authentication scheme across different environments to fulfill the complex distributed collaboration involved, time-varying environment and dynamic nature of the UAV network.

To solve the above challenges, we propose a novel concept of Service-of-Security (SoS), where a defined level of authentication performance is achieved by involving a necessary and minimal amount of authentication resources, i.e., authentication collaborative nodes and physical-layer attributes at each node. The performance might not be maximized when using less collaborative nodes and physical-layer attributes; however, the security requirement can still be guaranteed while the computational cost can be minimized. A fluid authentication topology can be customized at different time-varying environments so that the most reliable, robust and efficient model can be selected to perform the security provisioning.

The contributions of this chapter are summarized as follows:

- We propose a novel concept of Service-of-Security (SoS) to specifically achieve the defined level of authentication performance continuously to guarantee the security requirement. The computational complexity can be ultimately minimized by eliminating both the redundant or excessive collaborators and authentication attributes across different environments based on the situational-awareness.

- To select the collaborative nodes and the corresponding authentication attributes, a Gini-impurity-based attributes evaluation algorithm is proposed to evaluate the reliability of each time-varying physical-layer authentication attribute at each collaborative node. A

collaborative node evaluation algorithm is also developed to evaluate the usability of the collaborative nodes based on their relative locations and past contribution to the authentication.

- An intelligent authentication customization algorithm is proposed to integrate the above two factors for achieving SoS. By running this algorithm at each authentication instance, a customized authentication model will be generated to select the best combination of collaborative nodes. Authentication decisions can then be generated at these selected collaborative nodes and fused into the final authentication decision.

The rest of this chapter is organized as follows: Section 5.2 and 5.3 introduce the system model and problem formulation. Section 5.4 overviews the proposed Gini-impurity-based attributes evaluation algorithm, the collaborative node evaluation algorithm, and the two-factor intelligent authentication customization algorithm. The simulation and performance analysis are presented in Section 5.5. Ultimately, Section 5.6 concludes this chapter.

5.2 System Model

To elaborate on the proposed authentication technique, the decentralized authentication within a flying UAV network is considered in this chapter. As shown in Fig. 5.1, a flying UAV swarm is consists of M legitimate UAVs including the CH. Spoofing devices coexist in the same network which aims to impersonate the legitimate UAV for malicious purposes. Due to the potential connectivity outage or long separation distance from the ground server, on-site authentication within the UAV swarm is always preferred to avoid the related delay. As discussed earlier, an authentication process coordinated by the CH of the UAV swarm becomes most appropriate due to the limited security related information and computational resources at every single UAV. In a nutshell, the major objective is to authenticate the devices with a guaranteed performance by utilizing a minimum amount of authentication resources within the

flying UAV swarm. The CH selects multiple collaborative nodes to generate edge authentication decisions and fuses these decisions into a final authentication judgement. The process of the intelligent authentication contains three phases:

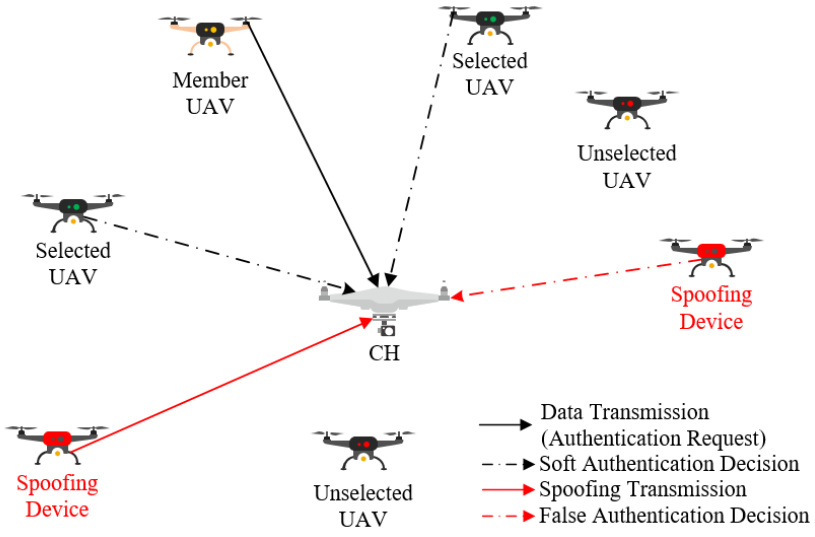

Figure 5.1: System model of the decentralized flying UAV network. The physical-layer-based soft authentication decisions from the selected collaborative nodes are utilized to generate a final authentication decision.

Phase I: At the time t_1, one or more messages have been transmitted to the CH and the CH aims to customize select the available collaborative nodes for authentication based on the observations of the message. Due to the interference or noise from the environment and the availability, some collaborative nodes including the CH could observe a noisy physical-layer estimation $\boldsymbol{H^I}$. The estimation at UAV m is given as:

$$\boldsymbol{H_m^I} = (H_{m1}^I, H_{m2}^I, \ldots, H_{mN}^I)^{\mathrm{T}}, \tag{5.1}$$

where N is the number of observed physical-layer attributes and $()^{\mathrm{T}}$ is the transposition of the vector. The attributes may include the carrier frequency offset (CFO), in-phase/quadrature (I/Q) imbalance, received signal strength indication (RSSI) and so on. Since some of the authentication attributes are less accurate, an attributes reliability evaluation becomes critical at each available collaborative node such that only J reliable attributes are kept to improve

the performance with minimal computational complexity. By evaluating the reliability of the attributes at each node, the unavailable nodes or the nodes with no reliable estimation will be temporarily removed from the authentication process. Then, the CH selects K collaborative nodes among the reliable and available collaborators based on the relative location and past contribution.

Phase II: At time t_2, each selected collaborative node generates an edge authentication decision and report back to the CH. For example at the selected UAV m, a soft edge authentication ϕ_m is generated where $\phi_m = [0, 1]$. The collaborative node evaluates how likely the authentication requester is legitimate based on the physical-layer observations. For example, $\phi_m = 0.5$ means that the UAV m indicates there is a 50% probability for the authentication requester to be legitimate.

Phase III: At time t_3, the CH generates the final authentication decision based on the K received edge authentication decision as:

$$\begin{cases} \Phi_0, & \frac{1}{K}\sum_{k=1}^{K}\phi_k > \nu; \\ \Phi_1, & \frac{1}{K}\sum_{k=1}^{K}\phi_k \leq \nu, \end{cases} \tag{5.2}$$

where K is between 1 and $M-1$. Φ_0 represents the transmitter is legitimate and Φ_1 indicates the data transmission is sent by a spoofing device. ϕ_k represents the soft authentication decision from the k-th received node. Moreover, ν is the authentication decision threshold in the range of $[0, 1]$ and can be altered dynamically between different cases.

5.2.1 Problem Formulation

To evaluate the performance of the collaborative decentralized authentication, the False Alarm rate and the Miss Detection rate are considered and can be expressed as:

1) False Alarm (FA) rate: The probability that the legitimate UAV is rejected as a spoofing

device, which is formulated as:

$$P_{\mathrm{FA}} = \Pr(\frac{1}{K}\sum_{k=1}^{K}\phi_k \leq \nu|\Phi_0). \tag{5.3}$$

2) Miss Detection (MD) rate: The probability that the spoofing device is approved as a legitimate UAV. It can be defined as:

$$P_{\mathrm{MD}} = \Pr(\frac{1}{K}\sum_{k=1}^{K}\phi_k > \nu|\Phi_1). \tag{5.4}$$

To define and security requirement and evaluate the accuracy and robustness of the actual authentication decision, the false alarm rate and the miss detection rate can be combined as the authentication error rate ($\mathcal{E}$) as:

$$\mathcal{E} = w_1 P_{\mathrm{FA}} + w_2 P_{\mathrm{MD}}, \tag{5.5}$$

where w_1 and w_2 are the costs of the false alarm and the miss detection. The false alarm and the miss detection can be treated equally; however, under certain applications, the miss detection may cause more damage to the system than the false alarm and may have a higher cost. Hence, to guarantee the SoS, both the false alarm rate and the miss detection rate should be limited. On the other hand, to make sure that the SoS is fulfilled without utilizing an excessive amount of authentication resources, the number of selected collaborative nodes (K) and the number of attributes selected at each node (J) should be as few as possible. Simultaneously, the operator-designed target error rate ($\mathcal{E}_D$) and the actual error rate ($\mathcal{E}_A$), which are both defined by (5.5), should be as close as possible. Hence, the SoS, which is also the problem formulation of this chapter can then be formulated as:

$$\min_{J,K,\nu} \mathcal{E}_D - \mathcal{E}_A, \tag{5.6}$$

where v is the authentication threshold in the final binary hypothesis test at the CH and $\mathcal{E}_D > \mathcal{E}_A$. Therefore, it is critical to select the more reliable collaborative node to compute the soft edge authentication decision so that the SoS can be guaranteed with minimum effort.

5.3 Cost Minimizing SOS Guaranteed Collaborative Authentication

To solve the problem of (5.6) by forming a customized authentication model, it is critical to eliminate the unavailable collaborative nodes and utilize the trustworthy attributes at the selected nodes only. Therefore, quantifying and evaluating the reliability of each collaborative node and its corresponding physical-layer estimations becomes a dilemma. A usability index ($\mathcal{U}$) can be formulated across the authentication process so that the most suitable authentication model can be structured. To summarize the proposed mechanism, we first aim to evaluate the reliability of the attributes at each available collaborative node. This helps to eliminate the nodes that could not collect reliable physical-layer estimations for various reasons. Besides, it can also help to eliminate the unnecessary attributes if the collaborative node is selected to make a soft authentication decision. After eliminating some of the collaborative nodes, a collaborative node evaluation algorithm is further developed to evaluate and rank the available and reliable nodes by considering the relative locations and past authentication contributions. These two attributes are continuously updated so that the hidden spoofing device which injects the false authentication decision will be discovered and eliminated. Finally, to achieve the SoS with minimum effort, the two-factor intelligent authentication customization algorithm is proposed to select the minimum amount of collaborative nodes and the attributes at each node by considering both algorithms.

5.3.1 Gini-impurity-based Attributes Evaluation Algorithm

To guarantee the SoS with minimum effort, we first need to verify whether the physical-layer attributes are reliable at each available collaborative node that observed the physical-layer attributes. An attribute evaluation algorithm that can quantify the contribution of the attributes to the security performance becomes a dilemma to eliminate the redundant and excessive authentication resources. To achieve this goal, the past obtained observations have to be stored

and utilized to continuously monitor the behaviour of each attribute at the collaborative nodes. If no estimation is observed or none of the observed attributes are reliable, the collaborative node should not be considered to contribute to the authentication process based on the performance requirement. This can not only help to eliminate the ambiguity caused by the uncertain decision but also decrease the overall computational cost.

Some popular machine-learning-based attributes evaluation techniques include the tree-based feature importance techniques [86, 87, 88]. However, instead of computing an independent value for each attribute, these methods measure the performance gain at each node and compute an importance value for each attribute that sums up to 1. This means that it can only compute a relative importance value that distinguishes the more reliable attribute from the less reliable one rather than an absolute evaluation that can be generalized. Hence, if the attributes are equally reliable or unreliable, they will all have similar values according to the tree-based feature importance techniques.

The attributes selection algorithm proposed in chapter 3 also suffers from a similar issue. Since the algorithm is developed for a centralized authentication scheme where the CH is always optimized to provide the best service, it is reasonable to assume that there will be at least one reliable attribute. However, in decentralized authentication techniques, it might be challenging for certain collaborative nodes to collect a reliable physical-layer attribute for a specific authentication requester. Hence, instead of measuring the relative importance level, it is critical to quantify the reliability of each attribute with an absolute standard at each collaborative node which can also be further used to evaluate the importance level of the collaborative node.

To generate an attribute reliability evaluation criteria that can be generalized, we utilize the Gini impurity, which represents the probability for an attribute to mislead the authentication decision [89]. To be more specific, a high Gini impurity means the attribute has a high probability to mislead the authentication decision; hence, the attribute is less reliable. The Gini

impurity of the n-th attribute can be calculated as:

$$\begin{aligned} G_n &= \sum_{c=1}^{C} f_c(1 - f_c) = \sum_{c=1}^{C} (f_c - f_c^2) \\ &= \sum_{c=1}^{C} f_c - \sum_{c=1}^{C} f_c^2 = 1 - \sum_{c=1}^{C} f_c^2, \end{aligned} \tag{5.7}$$

where C is 2 in our case since the authentication decision can only be legitimate or illegitimate. f_c is the frequency of being legitimate and illegitimate. Hence, to evaluate whether an attribute is reliable to be selected, a Gini impurity threshold (τ) can be introduced in which the attributes with a lower Gini impurity ($G_n < \tau$) is deemed as reliable. If no observation is made or none of the attributes is reliable at a collaborative node, the node will not be considered by the CH temporarily and get a usability index of 0. Meanwhile, it will keep collecting the physical-layer estimation and rejoin the authentication process until it meets the minimum performance requirement. Hence, to find the optimized amount of selected attributes (J) in (5.6), an optimized τ value need to be set based on the security requirement by the operator. The proposed Gini-impurity-based attributes evaluation algorithm is shown in Algorithm 5.1.

5.3.2 Collaborative Node Evaluation Algorithm

After selecting the attributes at each collaborative node, the next step is to optimize the number of collaborative nodes (K) for making the final authentication decision. Since the objective of (5.6) is to guarantee the SoS rather than maximize the security performance, some of the collaborative nodes can be eliminated to lower the computational cost. Hence, it is critical to evaluate the usability of the remaining collaborative nodes by introducing a usability index at the authentication instance so that some less important collaborative nodes can be sacrificed to optimize the computational cost.

To evaluate the usability of the remaining collaborators, the factors that cause the accuracy fluctuation of the physical-layer observations have to be studied. The analog physical

Algorithm 5.1 Gini-impurity-based attributes evaluation algorithm

Given each collaborative node has previous observations of the other devices and the authentication decision feedback of those devices from the CH. The total amount of attributes at a selected collaborative node is denoted by N.

1: Gini impurity (G_n) is calculated using (5.7) for each physical-layer attribute;
2: **if** $G_n < \tau, n = 1, 2, ..., N$ **then**
3: n-th attribute will be deemed as non-informative and dropped from the edge authentication scheme;
4: **else**
5: n-th attribute will be utilized in the proposed scheme;
6: **end if**
7: the collaborative node calculates the number of attributes being selected (J);
8: **if** $J \neq 0$ **then**
9: self-report to the CH as an available and reliable collaborative node;
10: update the local authentication scheme to utilize J selected attributes for the next authentication instance;
11: **else**
12: temporarily eliminated from the authentication process.
13: **end if**

attributes estimations are more environment-dependent by comparing to the upper layer attributes. For example, some of the physical-layer attributes may become less accurate with respect to the location. For example, a longer distance between the authentication requester and the collaborative node results in lower received signal strength while the noise level is almost constant. Therefore, the noise may significantly increase the measurement deviation and increase the uncertainty. On the other hand, different locations also result in various channel fading. The measured physical-layer estimations may become significantly different from the previous contributions and can result in a wrong edge decision. Hence, from the challenges listed above, the relative location between the collaborative node (p) and the authentication requester (q) is chosen as one of the evaluation attributes to measure the usability of the collaborative node. The longitude (X), latitude (Y) and altitude (Z) are utilized to define the location of each node. By analyzing the relative location as an attribute to evaluate the usability index, the collaborator that cannot observe reliable physical-layer estimations will be eliminated from the authentication temporarily as an outlier.

To detect an outlier that leads to an unreliable physical-layer estimation based on the rela-

tive location, the Local Outlier Factor (LOF) can be utilized to define the local neighbourhood of the data point [90]. It can reveal how isolated a data point is with respect to the surrounding neighbourhood based on a single parameter $\mathcal{K}$, which is the number of nearest neighbours used in defining the local neighbourhood. The distance between the data point (α) and the $\mathcal{K}$-th neighbour can be given as $kdist(\alpha)$. The judgement of the outlier is based on the density between each data point and its neighbour points [91]. If the density of reliable estimation is lower than normal, it is more likely to be identified as the outlier since it has a lower probability to make a correct edge authentication decision [92]. Then, the reachability distance, which is an intermediate parameter, can be expressed as:

$$rdist(\alpha,\beta) = \max\{dist(\alpha,\beta), kdist(\beta)\}, \tag{5.8}$$

where α is the current data point and β is the target point. The reachability distance is a conversion for Euclidean distance $dist(\alpha,\beta)$ since a bias ratio of distance can be given when the Euclidean distance of two data points is very small. Since there are 3 attributes, namely longitude, latitude and altitude, in each data point, the $dist(\alpha,\beta)$ can be given as:

$$dist(\alpha,\beta) = \sqrt{(X_\alpha - X_\beta)^2 + (Y_\alpha - Y_\beta)^2 + (Z_\alpha - Z_\beta)^2}. \tag{5.9}$$

Then, local reachability density ($lrd(\alpha)$) of the data point α, which calculates the average reachability distance of $\mathcal{K}$ neighbours can be given as:

$$lrd(\alpha) = \frac{|R(\alpha)|}{\sum_{\beta\in R(\alpha)} rdist(\alpha,\beta)}, \tag{5.10}$$

where $|R(\alpha)|$ denotes the size of $R(\alpha)$ which can be written as:

$$R(\alpha) = \{\beta | dist(\alpha,\beta) < kdist(\alpha)\}. \tag{5.11}$$

Lastly, the LOF can be calculated as:

$$lof(\alpha) = \frac{\sum_{\beta \in R(\alpha)} \frac{lrd(\beta)}{lrd(\alpha)}}{|R(\alpha)|}. \tag{5.12}$$

If the LOF is near or smaller than 1, it is more likely to be a normal data point. If the LOF is higher than 1, it is more likely to be an outlier. To be more specific, the relative location will be converted to a factor of either 1 or 0 where 1 means the collaborative node can generate a reliable edge authentication decision at this location as a normal data point and 0 means the collaborative node cannot generate a reliable edge authentication as an outlier. The binary decision can be formulated as:

$$D_{pq} = \begin{cases} 0, & lof(\alpha_p) > \mathcal{L}; \\ 1, & lof(\alpha_p) \leq \mathcal{L}, \end{cases} \tag{5.13}$$

where D_{pq} is the binary index that judges whether the collaborative node (p) can make a reliable physical-layer estimation at the relative location with respect to the authentication requester (q). $\mathcal{L}$ is the LOF threshold selected by the operator and the data points used to calculate LOF are previous authentication contributions collected at the CH.

On the other hand, there exists a scenario in which some of the soft authentication decisions are transmitted from the attackers. It is critical to monitor the behaviour of each collaborative node and eliminate the suspicious collaborative nodes. To achieve this goal, the authentication contribution of each collaborative node has to be considered. If a collaborative node has a high probability of giving a wrong authentication decision, the usability index should be adjusted to reflect the unreliable behaviour. Therefore, the authentication reliability rate (R_{pq}) of a collaborative node (p) with respect to the authentication requester (q) can be calculated by using the U last authentication decisions as:

$$R_{pq} = 1 - w_1 \Pr(\phi_{pq} \leq \nu | \Phi_0) - w_2 \Pr(\phi_{pq} > \nu | \Phi_1), \tag{5.14}$$

where v is the authentication threshold at the CH to better evaluate whether the contribution of the collaborative node is positive or negative. w_1 and w_2 are the weight used in (5.5) to reflect the different importance level of the miss detection case and false alarm case. Then, to formulate the usability index of collaborative node (p) to the authentication requester (q), the distance judgement and the reliability rate can be fused as:

$$\mathcal{U}_{pq} = R_{pq} D_{pq}, \tag{5.15}$$

where $\mathcal{U}_{pq} = [0, 1]$. Therefore, if the collaborative node is deemed unreliable due to the relative location, the usability index will be 0 since $D_{pq} = 0$. The collaborative nodes that are eliminated in Algorithm 5.1 will automatically get a usability index of 0. Then, the calculated usability index will be passed to the next step to ultimately select the collaborative node and the combination of the attributes. The proposed algorithm is shown in Algorithm 5.2.

Algorithm 5.2 Collaborative Node Evaluation Algorithm

Given the collaborative node is denoted by p and the authentication requester is denoted by q. There exist at least U previous observations contributions where U can be adjusted dynamically based on different requirements.

1: acquire the relative location of the collaborative node (p) with respect to the authentication requester (q).
2: use the LOF technique from (5.13) to compute the binary distance index (D_{pq});
3: calculate the reliability index (R_{pq}) by using (5.14);
4: fuse the calculated D_{pq} and R_{pq} as the usability index ($\mathcal{U}_{pq}$) by using (5.15);

5.3.3 Two-factor Intelligent Authentication Customization Algorithm

After calculating the usability index of each collaborative node by using Algorithm 5.2, the set of usability can be formulated as $\boldsymbol{\mathcal{U}} = (\mathcal{U}_{1q}, \mathcal{U}_{2q}, ..., \mathcal{U}_{Mq})^{\mathrm{T}}$ in descending order where $\mathcal{U}_{1q}$ has the highest usability index and $\mathcal{U}_{Mq}$ has the lowest usability index. If multiple collaborative nodes have the same usability index, the node with more correct authentication decisions beyond the last U authentication decisions will have a higher rank. For example, if two collaborative nodes have a usability index of 1, the node with more correct authentication decisions

will be ranked as $\mathcal{U}_{1q}$ and the other one will be ranked as $\mathcal{U}_{2q}$. The usability index of all M devices are included in this set where the unreliable collaborative nodes flagged in Algorithm 5.1 and Algorithm 5.2 has a usability index of 0. To customize select the collaborative node based on situational-awareness, it is critical to understand the authentication performance requirement needed by the application. To be more specific, a military application usually has a lower tolerance for wrong authentication decisions than a civilian application due to the more severe outcomes caused by the fault. Therefore, the optimization goal of (5.6) can be concluded to find the minimum amount of collaborative node K.

To promise the SoS as given in the problem formulation (5.6), the usability index from Algorithm 5.2 can be utilized since the usability index can be converted to express the miss detection rate and false alarm rate which are the two attributes that construct the error rate. Therefore, the goal of the attributes selection can then be rewritten as:

$$\min_{K}(\mathcal{E}_D - (1 - \mathcal{U}_{1q})(1 - \mathcal{U}_{2q})...(1 - \mathcal{U}_{Kq})), \tag{5.16}$$

where $K = 1, 2, ..., M$ and $(\mathcal{E}_D - (1 - \mathcal{U}_{1q})(1 - \mathcal{U}_{2q})...(1 - \mathcal{U}_{Kq})) \geq 0$. A stricter security requirement generally indicates that more collaborative nodes need to be utilized to fuse the final authentication decision. To elaborate on the authentication models, if multiple UAVs have a usability index of 1, including the CH, only the CH will be utilized to perform a centralized authentication process. On the other hand, if multiple UAVs have the same usability index and the algorithm decides it does not need all of them, the collaborative node with a higher rank will be selected. The proposed two-factor intelligent authentication customization algorithm is given in Algorithm 5.3.

After the authentication model is customized, each selected collaborative node computes a soft authentication decision (ϕ_k) based on Algorithm 4.1 proposed in Chapter 4. By transmitting these soft edge authentication decisions, the CH can then perform the final binary hypothesis test given in 5.2. The optimization of this algorithm is to find the best ν value that

fulfills (5.6). Ultimately, after the final authentication decision is made, the CH will transmit the judgement back to each collaborative node for future analysis and update the authentication record used in Algorithm 5.2.

Algorithm 5.3 Intelligent Authentication Customization Algorithm

The authentication fault tolerance (τ) is set by the operator.

1: rank the usability index into a set of usability in descending order as $\boldsymbol{\mathcal{U}} = (\mathcal{U}_{1q}, \mathcal{U}_{2q}, ..., \mathcal{U}_{Mq})^{\mathrm{T}}$ where $\mathcal{U}_{1q}$ has the highest usability index and $\mathcal{U}_{Mq}$ has the lowest usability index;
2: **if** there exists multiple collaborative nodes that have the same usability index **then**
3: the collaborative node with more correct authentication decisions in the past will have a higher rank;
4: **end if**
5: select the top K collaborative nodes from the set of usability index that meet the requirement of $\min_K(\tau - (1 - \mathcal{U}_{1q})(1 - \mathcal{U}_{2q})...(1 - \mathcal{U}_{Kq}))$;

Algorithm 5.4 Final Decision Fusion Algorithm

1: obtain the direct soft edge authentication decision from the selected collaborative nodes;
2: **if** $\frac{1}{K}\sum_{k=1}^{K}\phi_k > \nu$ **then**
3: authenticate the UAV as legitimate;
4: **else**
5: authenticate the UAV as a spoofing attacker;
6: **end if**
7: update the authentication record for Algorithm 5.2
8: transmit the final authentication decision as a feedback to all member UAVs for future use.

5.4 Performance Evaluation

In this section, the performance analysis of the proposed scheme is studied. Same as the previous chapter, the UAV network is constructed using MATLAB 2020a. A dynamic environment with 600 observations is constructed in which both the urban area and rural area are considered with a transition period. Each UAV has a random motion path and the analysis represents the last of the 5 simulations that have been initialized different relative location. All simulations have similar results. We consider a 3D movement where the flight height varies between 150

to 300m in the urban area and 10m to 40m in the rural area [68]. The Friis equation is utilized to model the path-loss and the Doppler shift is considered due to the high relative velocity under the rural area [69]. The height-dependent Rician factor is considered in the line-of-sight condition under the rural area and the Rayleigh fading distribution is considered in the non-line-of-sight condition under the urban area. To construct the transition period, the flight height and the velocity of each UAV varies gradually; hence, the changes in relative locations lead to new channel conditions. The channel model is gradually switched from the non-line-of-sight condition to the line-of-sight condition. A sudden environment change is also included by tuning the multipath condition (i.e., from a rich multipath environment to a low multipath environment) within the transition period to test the robustness of our proposed scheme. To evaluate the error rate in (5.5), the w_1 and w_2 are considered to have a equal weight of 0.5 in this case.

In order to select the collaborative node with reliable attributes for promising the SoS, the Gini-impurity-based attributes evaluation algorithm is first proposed to evaluate the reliability of each physical-layer attribute at each collaborative node. To examine whether the Gini-impurity measurement can reflect the different characteristics of each attribute, we select a random member UAV within the network and plotted the relationship between the Gini-impurity and the time-varying environment as shown in Fig. 5.2. The physical-layer attributes included in the figure include RSSI, CFO and IQI. It can be observed that the Gini impurity of each physical-layer attribute fluctuates with respect to the environmental change. This supports that each attribute may contribute differently with respect to the time-varying environment.

Moreover, to examine the relationship between the Gini-impurity-based attributes evaluation algorithm and the authentication performance, we select a random member UAV and studied the error rate of its edge authentication decision. The error rate of (5.5) is computed with respect to the authentication decision threshold as shown in Fig. 5.3. It can be concluded that our proposed scheme can increase the optimized authentication decision threshold interval at the selected collaborative node. Hence, it is easier to find a common optimized authentica-

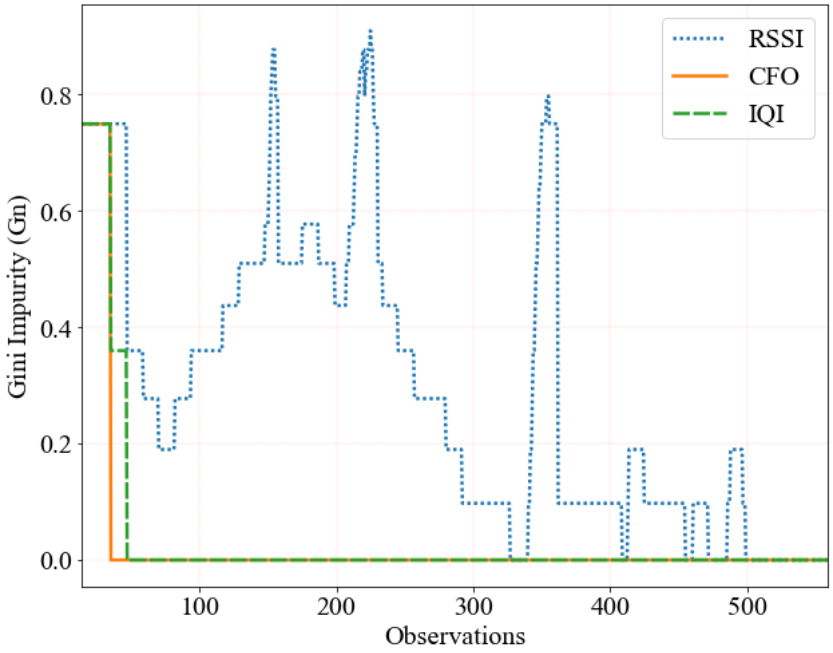

Figure 5.2: Gini impurity measurements across different environments

tion threshold (ν) among different collaborative nodes at the concave of the plot.

From Fig. 5.4, it can be observed that although all techniques can achieve an optimized authentication performance when the observations increase, the Gini-impurity-based attributes evaluation algorithm can accelerate the training period in the beginning. The lower training overhead is extremely beneficial to the resource constraint applications where it is harder to spare the collaborative nodes for training purposes.

Since the computational complexity is proportional to the number of selected collaborative nodes, one of the objectives in (5.6) is to minimize the number of selected collaborative nodes (K). To examine the ability to select the minimum amount of collaborative node, we considered 3 different security requirement evaluated by the operator defined error rate as $\mathcal{E}_D = 0.001$, $\mathcal{E}_D = 0.00001$ and $\mathcal{E}_D = 0.0000001$. This reflects the unique security requirements across different scenarios such as from civilian applications to military applications.

As shown in Fig. 5.5, when $\mathcal{E}_D = 0.001$, only 1 collaborative node is selected across different environments to guarantee the SoS. This demonstrates that only a few authentication resources are required to achieve a low authentication requirement. As shown in Fig. 5.6,

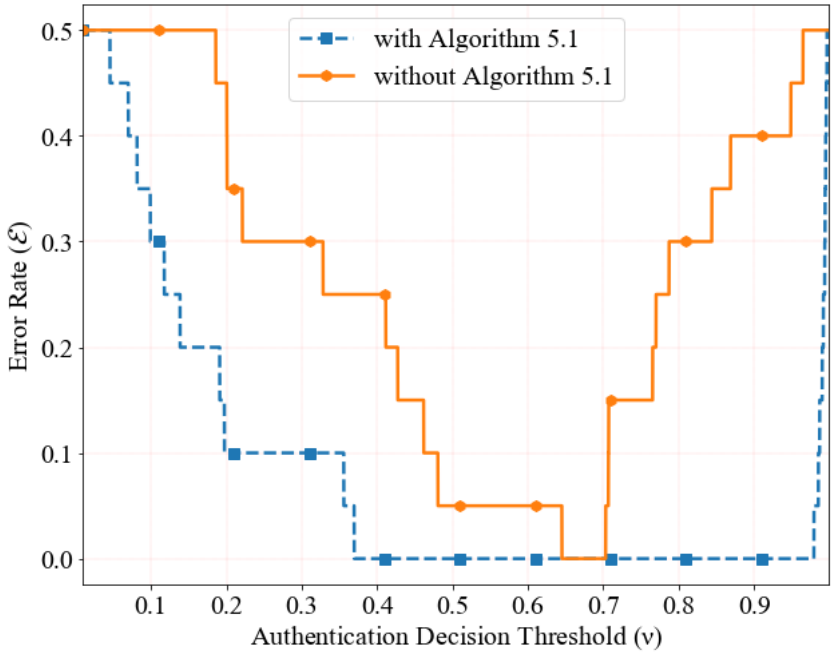

Figure 5.3: Error rate comparison results with and without using Algorithm 5.1 at a collaborative node

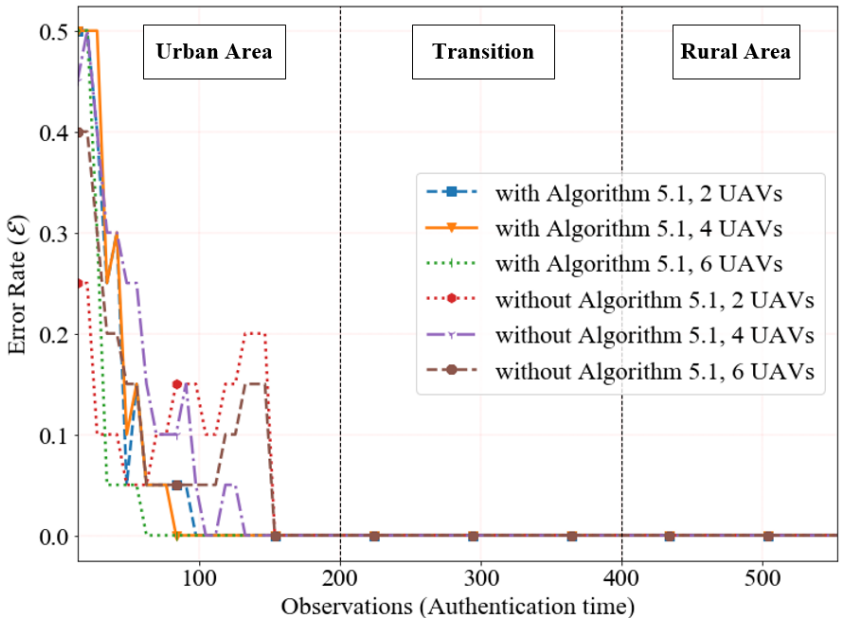

Figure 5.4: Error rate comparison results with and without using Algorithm 5.1 in the UAV swarm

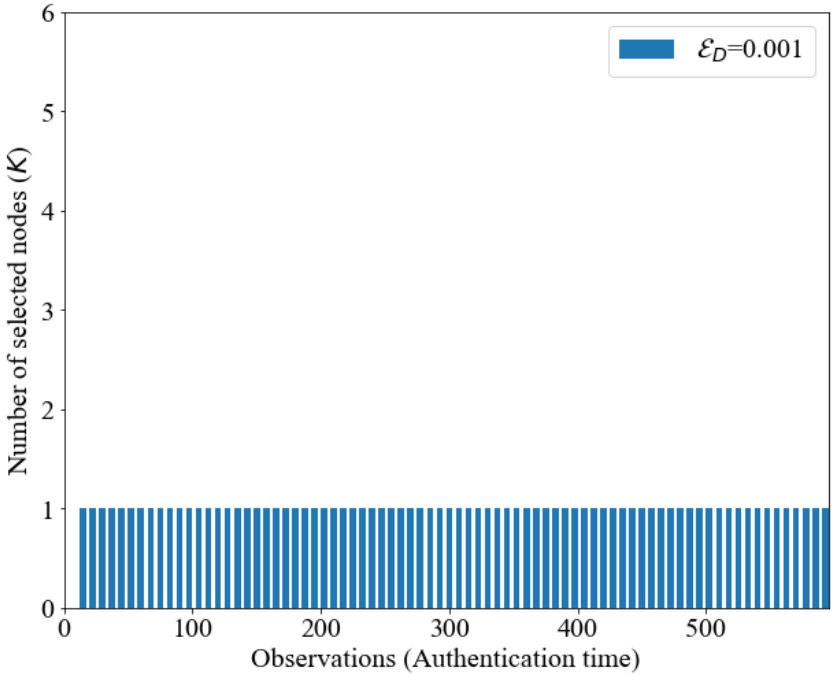

Figure 5.5: Security requirement ($\mathcal{E}_D = 0.01$) and the number of selected collaborative node(s)

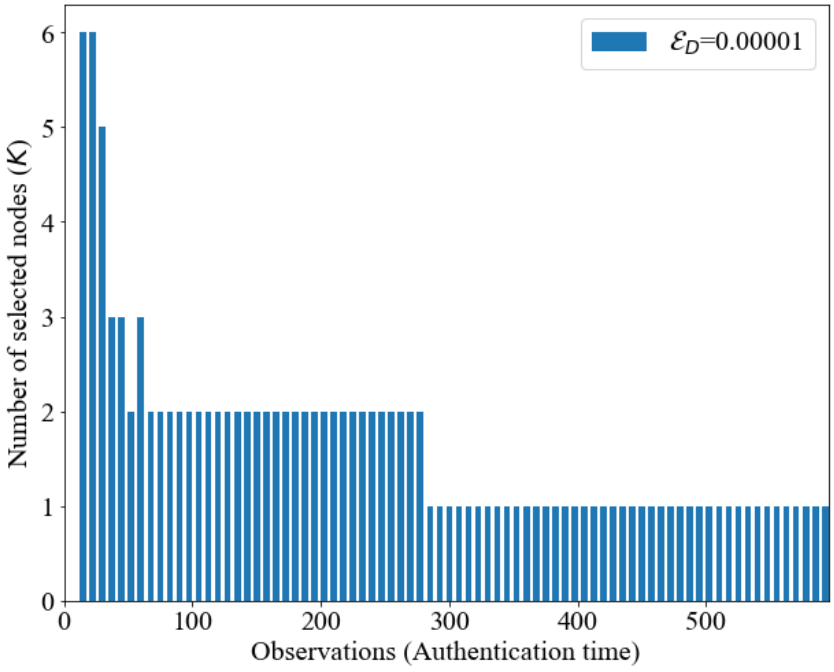

Figure 5.6: Security requirement ($\mathcal{E}_D = 0.00001$) and the number of selected collaborative node(s)

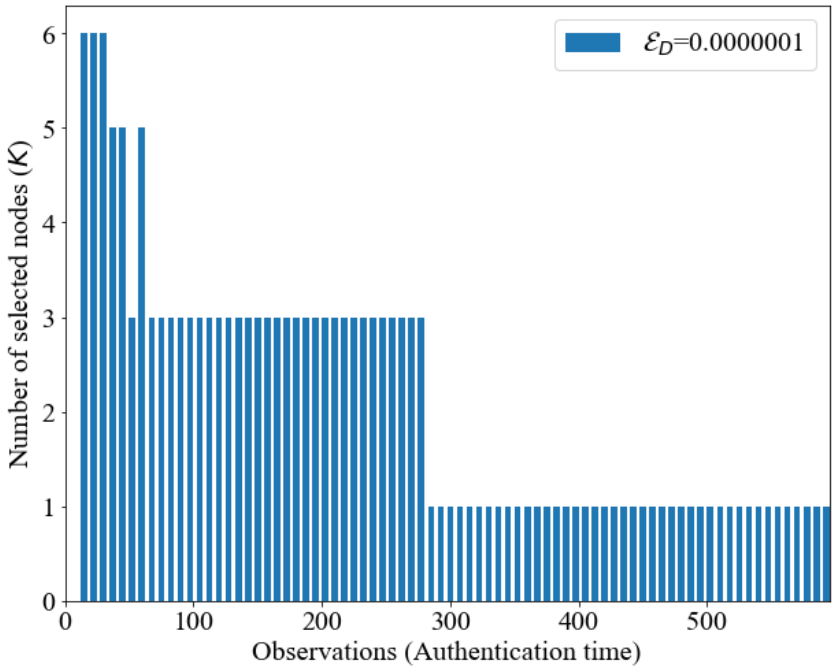

Figure 5.7: Security requirement ($\mathcal{E}_D = 0.000001$) and the number of selected collaborative node(s)

when $\mathcal{E}_D = 0.00001$, it can be observed that more collaborative nodes are selected at the beginning by comparing to Fig. 5.5. This demonstrates that a training stage is required at each node to achieve optimized performance. Then, to study the computational cost under the extreme harsh authentication performance requirement, Fig. 5.7 is plotted to demonstrate the collaborative node selection at $\mathcal{E}_D = 0.0000001$. It can be observed that more collaborative nodes are selected at the early stage and the authentication performance can be achieved by not utilizing all possible authentication resources. Also, when the collaborative nodes are well trained, our proposed scheme can still decrease the number of selected nodes to 1.

Ultimately, to demonstrate that our proposed scheme can satisfy the authentication performance requirement, Fig. 5.8 is plotted by considering the same security requirement where $\mathcal{E}_D = 0.001$, $\mathcal{E}_D = 0.00001$ and $\mathcal{E}_D = 0.0000001$ as used in the previous step. It can be observed from the zoom-in plot that the actual security performance ($\mathcal{E}_A$) can promise the defined requirement which successfully demonstrates that the SoS can be guaranteed with fewer authentication resources after the training stage. A nearest-neighbor-based centralized authen-

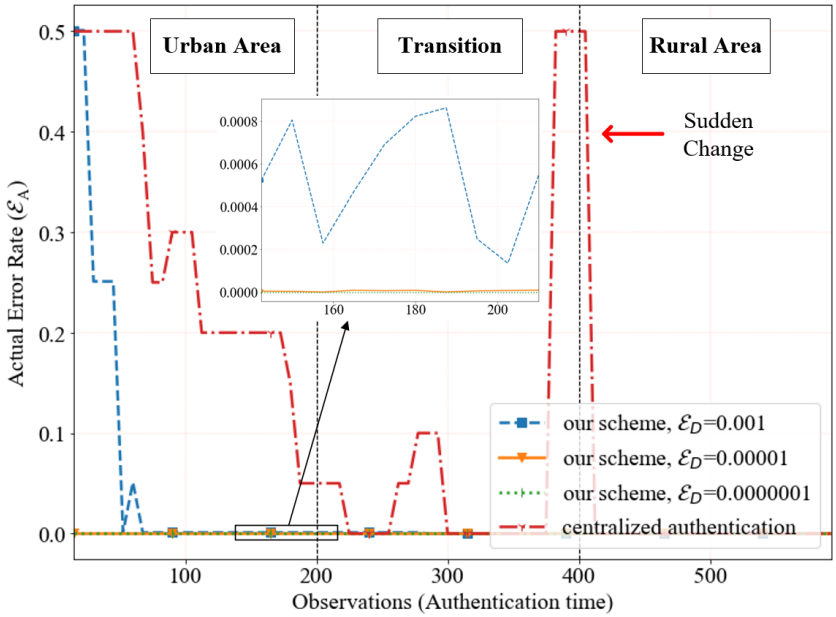

Figure 5.8: Performance comparison between our proposed scheme and the centralized authentication scheme

tication scheme proposed in [75] is selected as the benchmark testing. It can be observed that the training stage can be decreased significantly when the collaborative nodes are utilized in the training stage. Besides, by comparing to Fig. 5.4, the training stage of our proposed scheme is also shorter since the excessive unreliable collaborative nodes are eliminated. Moreover, to demonstrate the robustness of our proposed scheme, a sudden environment change is added within the transition stage as labelled on the plot. It can be observed that with the increasing number of observations, although all techniques can achieve an optimized performance when the number of observations increases, the performance of our proposed scheme is significantly more robust and reliable against the sudden environmental change happens. It can also be demonstrated that the performance requirement can be guaranteed throughout the different environments with minimal computational cost after the training stage based on the SoS. Lastly, there still remains a limitation of our proposed scheme when the operator-defined authentication performance is extremely strict while there is only a few collaborative nodes available. When the performance requirement exceeds the possible maximum performance, the authentication scheme will become best-effort-based. Hence, the proposed scheme is more suitable to

be implemented under the situation where the maximum authentication performance exceeds the security requirement so that an equilibrium can be achieved between the actual authentication performance and the computational cost.

5.5 Chapter Summary

In this chapter, a collaborative security provisioning mechanism was proposed to customize create authentication models at different environments so that the defined security performance can be guaranteed with minimal computational complexity. By utilizing our proposed mechanism, an equilibrium between the SoS and the computational cost can be found to construct a fluid authentication model. To achieve this goal, the usability index of each collaborative node has to be evaluated so that only the minimum number of reliable collaborative nodes are utilized at each authentication instance. To quantify the usability index, a Gini-impurity-based attributes evaluation algorithm was first developed to evaluate the physical-layer attributes. If none of the attributes are deemed as reliable, the collaborative node will be temporarily removed from the authentication process. a collaborative node evaluation algorithm further evaluates the usability index of each collaborative node by considering the relative distance and the authentication history with respect to the specific authentication requester. Then, the intelligent authentication customization algorithm utilizes the calculated usability index and selects the most suitable combination of collaborative nodes and attributes at each node to guarantee the SoS with minimal computational cost. Finally, the proposed scheme was verified and compared with the other state-of-the-art centralized authentication schemes to demonstrate its superior authentication performance and computational cost.

Chapter 6

Conclusion and Future Work

This chapter presents the conclusion of this thesis. Some future works are also presented in this chapter.

6.1 Conclusion

In this thesis, a centralized cross-layer authentication scheme was first proposed based on the LDA technique as an intelligent process to eliminate the less informative cross-layer attributes so that the authentication performance can be improved while the computational overhead can be limited. The cross-layer attributes have been utilized to enhance security by providing more reliable and unique characteristics of each UAV. Our novel LDA-aided authentication scheme increases the trust value while decreasing the computational overhead by eliminating the unnecessary attributes. This process significantly increases the difficulty for the attackers to impersonate the legitimate UAVs within the swarm due to the different attributes selection based on the situational-awareness. Since the LDA technique could not decide the number of attributes being left after the dimensionality reduction, a situation-aware attributes selection algorithm has been proposed to select the minimum amount of attributes without jeopardizing the performance.

Then, the decentralized authentication techniques have been considered to improve the

authentication performance under a harsh environment. However, the reliability of the edge authentication decision at each node may not be equivalent to each other. Hence, an edge soft authentication decision scheme was proposed to evaluate the probability for the authentication requester to be legitimate at each authentication node. This scheme can effectively relax the uncertainty at each authentication node which ultimately improves the reliability and robustness when fusing the edge authentication decision into a final authentication decision.

Finally, to meet the stringent security requirements while maintaining a low computational cost within the resource constraint UAV swarm, the novel concept of SoS was first proposed. A collaborative security provisioning scheme was also proposed to customize create authentication models across different environments based on the SoS. These estimations are then used to compute the usability index through the two-factor process where the first process is to verify whether the collected attributes are reliable enough to generate an authentication decision and eliminate the less informative attributes. The second process is to further calibrate the usability index by considering the relative distance between the authentication requester and the authentication node as well as the past authentication contributions. By utilizing the proposed scheme, the authentication model can be fluid so that the decentralized authentication model and centralized authentication model can be switched seamlessly.

6.2 Future Work

With the rapid development of 5G-and-beyond networks, the number of smart devices is becoming more and more common. Human lives can be significantly improved when all these devices can work jointly. More machine-to-machine communications will be involved where the communication security needs to be guaranteed with minimal cost to improve the quality of the service. In this thesis, we only considered the authentication under the UAV network; however, there are many more types of networks in real world applications. For future work, some aspects of the proposed schemes are still worthwhile to be further developed to be generalized

into more authentication applications. A range of future research ideas can be summarized as follows.

Edge authentication scheme optimization: Although the upper-layer attributes, such as the application layer attributes, might be forged and injected by the attackers. It is still worthy to further utilize more upper-layer attributes when the physical-layer estimations are imperfect. Although we proposed a smart authentication mechanism in Chapter 5 that can switch between decentralized authentication schemes and centralized authentication schemes by utilizing the physical-layer attributes, we can further work on more edge authentication schemes at each authentication node to increase the diversity. For example, the authentication nodes can switch between encryption-based authentication techniques and the physical-layer or cross-layer authentication techniques based on the performance requirement and computational capability.

Large-scale IoT network authentication: The size of the UAV swarm in civilian or military missions may be limited; therefore, it is feasible to collect the physical-layer attributes between each UAV along with the mission. However, in large-scale networks with hundreds of devices, such as the industry IoT networks, the computational capability cannot support each device to observe the physical-layer attributes at all times. Hence, the smart authentication mechanism proposed in Chapter 5 can be further developed to limit the physical-layer estimations to smaller blocks and becomes compatible with large-scale networks.

Attributes inheritance: In the real world ad hoc network applications, existing devices may leave the network and new devices may join the network during the mission. The new devices may not have enough observations when it freshly joins the network. Therefore, if a similar device can share some of the observations with the new devices, it can contribute to the authentication process instantaneously. An attribute inheritance algorithm can be developed to study how to select the observations that can be inherited to the new devices or the rejoin devices.

Bibliography

[1] S. Bhandari, X. Wang, and R. Lee, "Mobility and location-aware stable clustering scheme for uav networks," *IEEE Access*, vol. 8, pp. 106364–106372, 2020.

[2] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.

[3] G. Sachs, "Drones reporting for work," *Goldman Sachs*, 2016.

[4] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in uav communication networks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

[5] I. Jeelani and M. Gheisari, "Safety challenges of uav integration in construction: Conceptual analysis and future research roadmap," *Safety science*, vol. 144, p. 105473, 2021.

[6] H. Nawaz, H. M. Ali, and A. A. Laghari, "Uav communication networks issues: a review," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1349–1369, 2021.

[7] G. Skorobogatov, C. Barrado, and E. Salamí, "Multiple uav systems: a survey," *Unmanned Systems*, vol. 8, no. 02, pp. 149–169, 2020.

[8] L. Merino, J. R. Martínez-de Dios, and A. Ollero, *Cooperative Unmanned Aerial Systems for Fire Detection, Monitoring, and Extinguishing*, pp. 2693–2722. Springer Netherlands, 2015.

[9] A. Srivastava and J. Prakash, "Future fanet with application and enabling techniques: Anatomization and sustainability issues," *Computer Science Review*, vol. 39, p. 100359, 2021.

[10] X. Wang, Y. Weng, and H. Gao, "A low-latency and energy-efficient multimetric routing protocol based on network connectivity in vanet communication," *IEEE Transactions on Green Communications and Networking*, 2021.

[11] H. Wang, H. Fang, and X. Wang, "Safeguarding cluster heads in uav swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2021.

[12] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*, pp. 129–150, Springer, 2021.

[13] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2019.

[14] M. T. Hammi, P. Bellot, and A. Serhrouchni, "Bctrust: A decentralized authentication blockchain-based mechanism," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2018.

[15] S. Rosati, K. Krużelecki, G. Heitz, D. Floreano, and B. Rimoldi, "Dynamic routing for flying ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1690–1700, 2016.

[16] T. Alam and B. Rababah, "Convergence of manet in communication among smart devices in iot," *Authorea Preprints*, 2020.

[17] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in internet of things," *Sensors*, vol. 19, no. 6, p. 1467, 2019.

[18] S. Bhandari, X. Wang, and R. Lee, "Mobility and location-aware stable clustering scheme for uav networks," *IEEE Access*, vol. 8, pp. 106364–106372, 2020.

[19] U. S. D. of Defense, *Unmanned Systems Roadmap: 2007-2032*. AD-a475 002, Department of Defense, 2007.

[20] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, "Smart iot control-based nature inspired energy efficient routing protocol for flying ad hoc network (fanet)," *IEEE Access*, vol. 8, pp. 56371–56378, 2020.

[21] K. A. Hafeez, L. Zhao, Z. Liao, and B. N. Ma, "A fuzzy-logic-based cluster head selection algorithm in vanets," in *2012 IEEE International Conference on Communications (ICC)*, pp. 203–207, 2012.

[22] P. K. Deb, A. Mukherjee, and S. Misra, "Xia: Send-it-anyway q-routing for 6g-enabled uav-leo communications," *IEEE Transactions on Network Science and Engineering*, 2021.

[23] E. Bertran and A. Sànchez-Cerdà, "On the tradeoff between electrical power consumption and flight performance in fixed-wing uav autopilots," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 8832–8840, 2016.

[24] B. Uragun, "Energy efficiency for unmanned aerial vehicles," in *2011 10th International Conference on Machine Learning and Applications and Workshops*, vol. 2, pp. 316–320, IEEE, 2011.

[25] N. Gao, Y. Zeng, J. Wang, D. Wu, C. Zhang, Q. Song, J. Qian, and S. Jin, "Energy model for uav communications: Experimental validation and model generalization," *China Communications*, vol. 18, no. 7, pp. 253–264, 2021.

[26] T. Li, J. Zhang, M. S. Obaidat, C. Lin, Y. Lin, Y. Shen, and J. Ma, "Energy-efficient and secure communication towards uavs networks," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[27] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in uav systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[28] J. Miao, H. Li, Z. Zheng, and C. Wang, "Secrecy energy efficiency maximization for uav swarm assisted multi-hop relay system: Joint trajectory design and power control," *IEEE Access*, vol. 9, pp. 37784–37799, 2021.

[29] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based dos attack-resilient control framework for real-time uav systems," in *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 1222–1227, 2019.

[30] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2018.

[31] G. Bansal and B. Sikdar, "S-maps: Scalable mutual authentication protocol for dynamic uav swarms," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12088–12100, 2021.

[32] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: A survey," in *2016 Cybersecurity and Cyberforensics Conference (CCC)*, pp. 28–34, 2016.

[33] N. Hong, "A security framework for the internet of things based on public key infrastructure," in *Advanced Materials Research*, vol. 671, pp. 3223–3226, Trans Tech Publ, 2013.

[34] S. Jain, C. Nandhini, and R. Doriya, "Ecc-based authentication scheme for cloud-based robots," *Wireless Personal Communications*, vol. 117, no. 2, pp. 1557–1576, 2021.

[35] N. Park, M. Kim, and H.-C. Bang, "Symmetric key-based authentication and the session key agreement scheme in iot environment," in *Computer Science and its Applications*, pp. 379–384, Springer, 2015.

[36] T. Nandy, M. Y. I. Idris, R. M. Noor, A. W. A. Wahab, S. Bhattacharyya, R. Kolandaisamy, and M. Yahuza, "A secure, privacy-preserving, and lightweight authentication scheme for vanets," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20998–21011, 2021.

[37] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020.

[38] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[39] Y. Chen, P.-H. Ho, H. Wen, S. Y. Chang, and S. Real, "On physical-layer authentication via online transfer learning," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[40] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical ofdm transmission," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6611–6625, 2016.

[41] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "Phy-cram: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817–1827, 2013.

[42] H. Zhao, Y. Zhang, Y. Xiang, X. Huang, and C. Su, "A physical layer key generation approach based on received signal strength in smart homes," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[43] J. Wan, A. Lopez, and M. A. A. Faruque, "Physical layer key generation: Securing wireless communication in automotive cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 2, pp. 1–26, 2018.

[44] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, 2016.

[45] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of i/q imbalance based wireless device authentication through collaboration of multiple receivers," in *2014 IEEE International Conference on Communications (ICC)*, pp. 939–944, IEEE, 2014.

[46] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[47] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach," *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, pp. 5420–5432, 2020.

[48] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, and M. Cao, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116390–116401, 2019.

[49] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1465–1479, 2018.

[50] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on per and rssi," in *2013 13th Canadian Workshop on Information Theory*, pp. 44–48, 2013.

[51] S. Biswas and J. Mišić, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[52] Z. Zhang, N. Li, S. Xia, and X. Tao, "Fast cross layer authentication scheme for dynamic wireless network," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2020.

[53] D. Xu, K. Yu, and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5g enabled iiot in industry 4.0," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2021.

[54] S. Xia, X. Tao, N. Li, S. Wang, T. Sui, H. Wu, J. Xu, and Z. Han, "Multiple correlated attributes based physical layer authentication in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1673–1687, 2021.

[55] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and iot environment," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116–2123, 2021.

[56] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, and D.-H. Kim, "Blockchain-based authentication in internet of vehicles: A survey," *Sensors*, vol. 21, no. 23, p. 7927, 2021.

[57] C. H. Lau, K.-H. Y. Alan, and F. Yan, "Blockchain-based authentication in iot networks," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, 2018.

[58] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 769–773, 2018.

[59] Z. Cui, F. XUE, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[60] M. Rodrigues and K. R. L. J. C. Branco, "Cloud–sphere: Towards secure uav service provision," *Journal of Intelligent & Robotic Systems*, vol. 97, no. 1, pp. 249–268, 2020.

[61] S. Sarıtaş, H. Forssell, R. Thobaben, H. Sandberg, and G. Dán, "Adversarial attacks on cfo-based continuous physical layer authentication: A game theoretic study," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, 2021.

[62] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Artificial noise-aided mimo physical layer authentication with imperfect csi," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2173–2185, 2021.

[63] L. Xiao, X. Wan, and Z. Han, "Phy-layer authentication with multiple landmarks with reduced overhead," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1676–1687, 2018.

[64] A. Tharwat, T. Gaber, A. Ibrahim, and A. E. Hassanien, "Linear discriminant analysis: A detailed tutorial," *AI Communications*, vol. 30, no. 2, pp. 169–190, 2017.

[65] C. Wang, B. Jiang, *et al.*, "On the dimension effect of regularized linear discriminant analysis," *Electronic Journal of Statistics*, vol. 12, no. 2, pp. 2709–2742, 2018.

[66] T. Li, S. Zhu, and M. Ogihara, "Using discriminant analysis for multi-class classification: an experimental investigation," *Knowledge and Information Systems*, vol. 10, no. 4, pp. 453–472, 2006.

[67] R. E. Prieto, "A general solution to the maximization of the multidimensional generalized rayleigh quotient used in linear discriminant analysis for signal classification," in *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03).*, vol. 6, pp. VI–157, IEEE, 2003.

[68] D. W. Matolak and U. Fiebig, "Uav channel models: Review and future research," in *2019 13th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, 2019.

[69] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, 2016.

[70] Z. Zhang, N. Li, S. Xia, and X. Tao, "Fast cross layer authentication scheme for dynamic wireless network," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2020.

[71] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on per and rssi," in *2013 13th Canadian Workshop on Information Theory*, pp. 44–48, IEEE, 2013.

[72] R. B. Thompson and P. Thulasiraman, "Confidential and authenticated communications in a large fixed-wing uav swarm," in *2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, pp. 375–382, IEEE, 2016.

[73] J. H. Aldrich and F. D. Nelson, *Linear probability, logit, and probit models*. No. 45, Sage, 1984.

[74] D. A. Hensher and W. H. Greene, "The mixed logit model: the state of practice," *Transportation*, vol. 30, no. 2, pp. 133–176, 2003.

[75] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1506–1521, 2021.

[76] H. N. Noura, R. Melki, and A. Chehab, "Secure and lightweight mutual multi-factor authentication for iot communication systems," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–7, 2019.

[77] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[78] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over mimo fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, 2012.

[79] F. Zhu, B. Xiao, J. Liu, and L.-j. Chen, "Efficient physical-layer unknown tag identification in large-scale rfid systems," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 283–295, 2017.

[80] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5g and beyond wireless networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, 2019.

[81] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4171–4182, 2016.

[82] H. Fang, X. Wang, and L. Hanzo, "Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2607–2620, 2020.

[83] X. Duan and X. Wang, "Fast authentication in 5g hetnet through sdn enabled weighted secure-context-information transfer," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2016.

[84] H. Wang, H. Fang, and X. Wang, "Edge intelligence enabled soft decentralized authentication in UAV swarm," in *2021 IEEE/CIC International Conference on Communications in China (ICCC) (IEEE ICCC 2021)*, (Xiamen, China), July 2021.

[85] H. Forssell and R. Thobaben, "Worst-case detection performance for distributed simo physical layer authentication," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[86] Z. Zhou and G. Hooker, "Unbiased measurement of feature importance in tree-based methods," *arXiv preprint arXiv:1903.05179*, 2019.

[87] A. Marcano-Cedeño, J. Quintanilla-Domínguez, M. G. Cortina-Januchs, and D. Andina, "Feature selection using sequential forward selection and classification applying artificial metaplasticity neural network," in *IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society*, pp. 2845–2850, 2010.

[88] P. Bermejo, J. A. Gámez, and J. M. Puerta, "Incremental wrapper-based subset selection with replacement: An advantageous alternative to sequential forward selection," in *2009 IEEE Symposium on Computational Intelligence and Data Mining*, pp. 367–374, IEEE, 2009.

[89] L. Jiang, B. Zhang, Q. Ni, X. Sun, and P. Dong, "Prediction of snp sequences via gini impurity based gradient boosting method," *IEEE Access*, vol. 7, pp. 12647–12657, 2019.

[90] O. Alghushairy, R. Alsini, and X. Ma, "An efficient local outlier factor for data stream processing: A case study," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1525–1528, 2020.

[91] Z. Cheng, C. Zou, and J. Dong, "Outlier detection using isolation forest and local outlier factor," in *Proceedings of the conference on research in adaptive and convergent systems*, pp. 161–168, 2019.

[92] W. Wang and P. Lu, "An efficient switching median filter based on local outlier factor," *IEEE Signal Processing Letters*, vol. 18, no. 10, pp. 551–554, 2011.

Curriculum Vitae

Name:	Huanchi Wang
Post-Secondary Education and Degrees:	University of Western Ontario London, ON, Canada 2019 - present, M.E.Sc University of Western Ontario London, ON, Canada 2014 - 2019 B.E.Sc
Honours and Awards:	Vector Scholarship in Artificial Intelligence 2019-2020
Related Work Experience:	Teaching Assistant University of Western Ontario 2019-2021 Secretary of Communication/Broadcast Chapter, IEEE London Section, 2021

Publications:

[1] H. Wang, H. Fang and X. Wang, "Safeguarding Cluster Heads in UAV Swarm Using Edge Intelligence: Linear Discriminant Analysis-Based Cross-Layer Authentication," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1298-1309, 2021.

[2] H. Wang, H. Fang, X. Wang, "Edge Intelligence Enabled Soft Decentralized Authentication in UAV Swarm," 2021 IEEE/CIC International Conference on Communications in China (ICCC), pp. 1-6, 2021.