Collaborative Authentication for 6G Networks: An Edge Intelligence Based Autonomous Approach

He Fang, *Member, IEEE*, Zhenlong Xiao, *Member, IEEE*, Xianbin Wang, *Fellow, IEEE*, Li Xu, *Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

Abstract—**The conventional device authentication of wireless networks usually relies on a security server and centralized process, leading to long latency and risk of single-point of failure. While these challenges might be mitigated by collaborative authentication schemes, their performance remains limited by the rigidity of data collection and aggregated result. They also tend to ignore attacker localization in the collaborative authentication process. To overcome these challenges, a novel collaborative authentication scheme is proposed, where multiple edge devices act as cooperative peers to assist the service provider in distributively authenticating its users by estimating their received signal strength indicator (RSSI) and mobility trajectory (TRA). More explicitly, a distributed learning-based collaborative authentication algorithm is conceived, where the cooperative peers update their authentication models locally, thus the network congestion and response time remain low. Moreover, a situation-aware secure group update algorithm is proposed for autonomously refreshing the set of cooperative peers in the dynamic environment. We also develop an algorithm for localizing a malicious user by the cooperative peers once it is identified. The simulation results demonstrate that the proposed scheme is eminently suitable for both indoor and outdoor communication scenarios, and outperforms some existing benchmark schemes.**

Index Terms—**Authentication, Location-related features, Autonomous collaboration, Distributed learning**

I. INTRODUCTION

The sixth generation (6G) technologies are expected to evolve from personal communication towards the full realization of the Internet of Things (IoT) paradigm, interconnecting not only people, but also machines, vehicles, computing resources, industry processes, and even robotic agents [1]. Due to the open broadcast nature of radio signal propagation and the standardized transmission schemes used, wireless communications are extremely vulnerable to security threats [2]–[4]. More specifically, the highly heterogeneous network structure, time-varying topology, and ubiquitous resource-constraint devices used in 6G networks leave many loopholes for potential eavesdropping, spoofing, forgery, interception, and denial of service attacks [5]–[7]. These security threats may lead to privacy leakage, interruption of intelligent services, and even to overall system breakdown. In preventing these malicious attacks, authentication is imperative to confirm the identities of communicating devices, to check the validity of their access to the network, to maintain the integrity and trustworthiness of their communications [8].

A. Challenges for Existing Authentication Methods

The conventional authentication methods usually apply classic symmetric/asymmetric-key cryptography [9]–[12]. The Public Key Infrastructure (PKI) has been widely studied in the literature [13], [14], where the security relies on a set of globally trusted authorities. The identity-based signature techniques allow a user's public key to be readily computed from its known identity information, thus eliminating the need for public-key/certificates [15]. The Diffie-Hellman key agreement protocol is known to be vulnerable to the "man-in-the-middle" attack, if two users involved in the protocol do not share any authenticated information about each other, e.g. shared keys, certificates, and passwords, prior to the protocol's execution [16]. The information-theoretic secret key agreement between a pair of legitimate parties guarantees a certain level of security, while relying on no computational restrictions concerning the eavesdropper [17]–[22]. As a design alternative, physical layer authentication exploits the unique random nature of communication links and devices-related features between a pair of transceivers to identify transmitters [23]–[25].

However, most of the existing security mechanisms feature network-specific, stand-alone, and isolated designs, which are typically deployed in a particular network, application, and certain layer of the protocol stack. Such mechanisms typically involve two parties, where one of the entities has to be authenticated, while the other one performs the verification. These isolated authentication schemes validate the devices without any cooperation from other devices. Their performance usually suffers from the limited knowledge and computational resources of the specific device performing the authentication. Moreover, the performance of physical layer authentication

This work was supported in part by the National Natural Science Foundation of China under Grants 62271430; in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Program under Grant RGPIN2018-06254, and the Canada Research Chair Program; in part by the Engineering and Physical Sciences Research Council projects EP/W016605/1 and EP/X01228X/1, and the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028).

H. Fang is with the School of Electronic and Information Engineering, Soochow University, Soochow 215301, China (email: fanghe@suda.edu.cn)

Z. Xiao is with the Department of Informatics and Communication Engineering, School of Informatics, Xiamen University, Xiamen 361005, China (email: zlxiao@xmu.edu.cn)

X. Wang is with the Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada (email: xianbin.wang@uwo.ca)

L. Xu is with the College of Computer and Cyber Security and the Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350117, China (email: xuli@fjnu.edu.cn)

L. Hanzo is with School of Electronics and Computer Science, University of Southampton, SO17 1BJ, U.K (email: lh@ecs.soton.ac.uk)

TABLE I: Contrasting the novelty of the proposed solution to the state-of-the-art.

Key attributes	Schemes				
	Conventional schemes [13-16]	PHY key generation schemes [17-22]	PHY authentication schemes [23]-[25]	Cooperative authentication schemes [26-30]	Blockchain-based scheme [33]	Our scheme
Device/channel-specific feature		✓	✓	✓	✓	✓
Collaboration from other devices	✓			✓	✓	✓
Distributed architecture					✓	✓
Autonomous collaboration						✓

suffers from low reliability and robustness in highly dynamic networks due to the noisy time-varying observations of the radio frequency fingerprint.

To overcome the challenges of isolated methods, collaborative security frameworks have been proposed for solving many practical security problems [26]–[30]. The collaborative methods could provide more accurate and robust authentication decisions by enabling multi-dimensional information sharing among the collaborative devices. Moreover, security enhancement can be achieved by increasing the difficulty of being successfully cracked. The authors of [27] proposed a cooperative authentication scheme for underwater acoustic sensor networks, which relies on trusted nodes that independently help a sink node to evaluate the belief concerning each incoming packet and then to reach an authentication decision. A cooperative authentication scheme is designed for detecting the spoofed Global Positioning System (GPS) signals in [28]. The authors of [29] proposed a physical layer authentication scheme based on the cooperation of multiple landmarks, which collect the channel information of the transmitter for authentication.

However, the above centralized methods do not consider the risk of single-point failure. Their further limitation is that they may suffer from long authentication latency and response time when numerous devices request authentication services at the same time. To address these issues, developing a distributed method to move security management from the cell-center to the cell-edge in the network is an efficient alternative. It will provide secure and low-overhead authentication by enabling a server to delegate its authentication authority to edge nodes [31], [32]. A blockchain empowered group authentication scheme is proposed in [33] for vehicles with decentralized identification based on a secret sharing and dynamic proxy mechanism. However, the blockchain-based schemes may suffer from long latency, high computation and communication cost, as well as high storage resources required for running a blockchain [34], [35].

To elaborate a little further on the challenges, the data collection and aggregation models of typical collaborative security schemes are usually fixed and stationary. They have limited capability in processing heterogeneous data, leading to potential failure in capturing the critical aspects of practical communication environments. These will also lead to limitations in intelligently exploiting heterogeneous security information in 6G communications requiring situation-aware services and flexible processes. More importantly, the information uncertainties and complex network topology will impose new challenges on the reliable authentication in mobile networks, such as vehicular ad hoc networks (VANETs) and Unmanned Aerial Vehicle (UAV) networks. In a nutshell, an autonomous distributed authentication technique is extremely helpful, where multiple devices govern the authentication process by sharing multi-dimensional information among them to improve the authentication accuracy and reliability.

B. Contributions

This paper proposes an edge intelligence-based collaborative authentication scheme for accurate identification and attacker localization by harnessing the cooperation of multiple edge nodes (peers). Each cooperative peer helps the service provider to authenticate its users by collecting and processing their observations of the users' location-related features, including the RSSI and TRA. The cooperative peers share their local observations with others and make real-time authentication decision based on a distributed learning algorithm. Consensus is achieved in the proposed scheme, where a group of cooperative peers will reach an agreement in the information collection and collaborative authentication process. Moreover, the learning models are updated locally at cooperative peers and only the final decision will be sent to the service provider. Then, a situation-aware secure group update algorithm is developed for adaptively updating the collaborative peers and the authentication features in the dynamic network. Finally, an attacker localization algorithm is developed for finding the position of the user, once it is identified as a spoofer.

The contributions of this paper are summarized as follows:
1) We propose an edge intelligence-based collaborative authentication scheme using multiple cooperating edge nodes to collect location-related features of the user for formulating their final decision. The proposed scheme decreases the time latency and network load by moving the security provision from center to edge of the network. It also enhances security by utilizing multiple cooperating devices and by using multi-dimensional security information.
2) The situation-aware group update algorithm autonomously updates the cooperative peers and authentication features by adaptively identifying the dynamic environment and network topology. Hence, the proposed scheme provides high robustness of collaborative authentication in the mobile network.

Moreover, the developed attacker localization algorithm can be used to immediately locate an identity spoofer, thus providing security enhancement.
3) Simulation results are provided for both indoor and outdoor communication scenarios. The results show that using more cooperative devices increases the authentication accuracy at the cost of higher communication overhead. The automation in updating the cooperating edge nodes and the robustness of the proposed scheme are verified in realistic noisy time-varying environments. It is also shown that the proposed scheme performs better than some existing counterparts.

TABLE II: Symbol definitions of this paper

Symbol	Definition
N	Number of cooperative edge nodes (peers).
$\boldsymbol{H}_n$	Feature estimation of the user observed by the n-th peer.
I	Identity (ID) of the user to be authenticated.
I_n	ID of the user observed by the n-th cooperative peer.
Φ_0	Case that the user to be authenticated is legitimate.
Φ_1	Case that the user to be authenticated is an identity spoofer.
ν	Collaborative authentication threshold.
F_{MD}	Misdetection (MD) rate of collaborative authentication.
F_{FA}	False alarm (FA) rate of collaborative authentication.
$f_n(\boldsymbol{x}_n)$	Local objective function of the n-th cooperative peer.
$\boldsymbol{x}_n$	Local variable of the n-th cooperative peer.
$\boldsymbol{x}_0$	Agreement of all cooperative peers.
$\boldsymbol{a}$	Real position of the legitimate user.
$\boldsymbol{b}_n$	Real position of the n-th cooperative peer.
$\boldsymbol{c}$	Real position of the spoofer.

The rest of this paper is organized as follows. In Section II, the system model used is presented. In Section III, we present the proposed edge intelligence-based collaborative authentication scheme. The authentication performance analysis is also given in Section III. The simulation results are discussed in Section IV. Finally, Section V concludes the paper. The symbol definitions of this paper are given in TABLE II.

II. SYSTEM MODEL

In this paper, we consider a wireless communication system associated with location-based services, where the service provider monitors its user's geographical location by positioning techniques, e.g. by the widely used GPS. The system contains massive edge nodes, e.g. gateways, servers, access points, and full-function devices.

A. Attack Model

As shown in Fig. 1, the system suffers from security threats caused by

◦ *Identity spoofer:* It performs identity spoofing attacks by imitating the legitimate user and then seeks to glean illegal benefits from the service provider;

◦ *Location spoofer:* It performs location spoofing attacks by misleading the service provider through pretending to be at a hypothetical position, e.g. GPS spoofer [28].

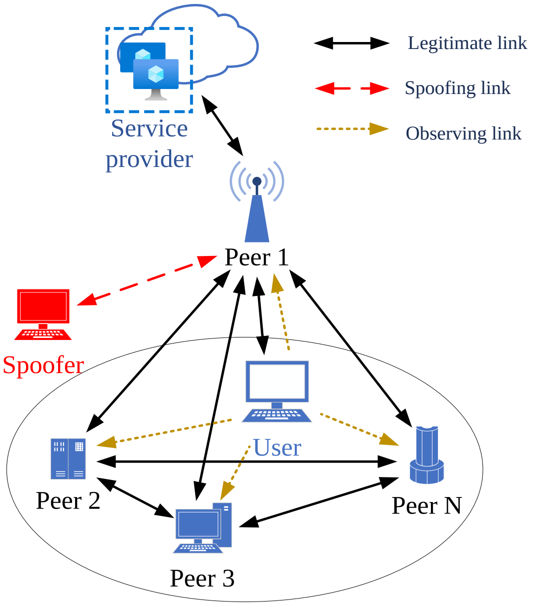


Fig. 1: A system providing location-based services, which suffers from either identity or location spoofing attacks. The service provider authenticates its users relying on the collaboration of multiple edge nodes near to the user.

The attack model considered in this paper is similar to the traditional Alice-Bob-Eve model [3]–[5], the service provider can be seen as Bob who needs to identify its users, while a user can be seen as Alice or Eve. The following assumptions are stipulated concerning the attack model:
Assumption 1. The attacker is a single malicious node, capable of performing any kind of signal processing techniques, and it has unlimited transmission power capabilities;
Assumption 2. The attacker knows the positions of all edge nodes and of the legitimate user;
Assumption 3. The attacker is located at a different position from the legitimate user, which is a smart device and focuses on maximizing its utility.

Note that when the spoofer is located close to the legitimate user, it may be readily spotted by the user. In order to maximize its utility gained, the spoofer will be located at an appropriate distance from the user. Hence, the above assumptions are reasonable. Moreover, guarding against a powerful worst-case attacker clearly demonstrates the benefits of our scheme. The service provider has to authenticate its user to confirm that it is a legitimate device and it is indeed located at the reported position. The authentication between the service provider and its user is assisted by N trusted but heterogeneous edge nodes, which are located near to the user at the network edge. These edge nodes can be termed as cooperative peers, which collect information of the user to be authenticated and help the service provider to verify its user's identity and localization.

B. Location-related Features for Collaborative Authentication

Two location-related features are utilized for collaborative authentication in this paper, i.e. the RSSI and TRA. Specifically, the RSSI is determined by the transmission power, the distance between the transceivers, and the radio environment [4]. Path loss models [42] are typically of the form

$$PL = A\log_{10}(D) + B + C\log_{10}(\kappa_c/5), \tag{1}$$

where D is the distance between the transceivers, κ_c is the carrier frequency, the fitting parameter A includes the path-loss exponent, B is the intercept and environment-specific term, and C describes the path loss frequency dependence. The TRA of the user can be observed by cameras or laser radars [43], [44], which are widely used in the mobile networks, such as VANETs, flying ad-hoc networks (FANETs), aeronautical ad hoc networks (AANETs), and UAV networks.

Each cooperative peer locally estimates one of these features of the user for identification. The observation of the n-th cooperative peer is denoted as

$$(I_n, \boldsymbol{H}_n),\ n \in \{1, 2, ..., N\}, \tag{2}$$

where I_n is the ID of the user to be authenticated observed by the n-th cooperative peer.

$$\boldsymbol{H}_n = (H_{n1}, H_{n2})^\dagger \tag{3}$$

represents the feature estimation of the user to be authenticated at the n-th cooperative peer. † denotes the transposition symbol. If the i-th feature is not selected by the n-th cooperative peer, we denote $H_{ni} = 0$, where $i \in \{1, 2\}$. The RSSI and TRA are listed as the 1st and 2nd feature, respectively.

Given the estimates of the above features, the distance between the user to be authenticated and each cooperative peer can be derived. The location of the user to be authenticated can be derived based on the estimates of location-related features by multiple cooperative peers [45]–[47]. Note that more location-related features can be selected in different application scenarios, e.g. angle-of-arrival (AoA). The RSSI and TRA are utilized as examples in this paper.

C. The Proposed Collaborative Authentication System

Our objective is to achieve accurate authentication and to locate the attacker based on the cooperation of multiple edge nodes. Upon denoting the real position of the legitimate user as $\boldsymbol{a} = (a_1, a_2, a_3)^\dagger$, the collaborative authentication based on the observations $(I_n, \boldsymbol{H}_n), n = 1, 2, ..., N$, is formulated as

$$\begin{cases} \forall n, I_n = I \text{ and } \parallel \boldsymbol{x}_0(\boldsymbol{H}_1, ..., \boldsymbol{H}_N) - \boldsymbol{a} \parallel_2 \le \nu & \Phi_0 \\ \exists n, I_n \neq I \text{ or } \parallel \boldsymbol{x}_0(\boldsymbol{H}_1, ..., \boldsymbol{H}_N) - \boldsymbol{a} \parallel_2 > \nu & \Phi_1 \end{cases}, \tag{4}$$

where ν is a collaborative authentication threshold. Φ_0 represents that the user to be authenticated is legitimate, while Φ_1 indicates that it is an identity spoofer. Moreover, $\boldsymbol{x}_0(\boldsymbol{H}_1, \boldsymbol{H}_2, ..., \boldsymbol{H}_N) = (x_{01}, x_{02}, x_{03})^\dagger$ represents an agreement of all cooperative peers concerning the authentication decision based on the observations of (2). If the user to be authenticated cannot be observed by the cooperative peers, $\boldsymbol{x}_0$ is set to $(+\infty, +\infty, +\infty)^\dagger$. The performance of the proposed scheme is evaluated by the following criteria:

1) Authentication Accuracy: It can be evaluated by the MD rate and FA rate, which are formulated, respectively, as

$$F_{\text{MD}} = \Pr(\parallel \boldsymbol{x}_0(\boldsymbol{H}_1, \boldsymbol{H}_2, ..., \boldsymbol{H}_N) - \boldsymbol{a} \parallel_2 \le \nu \mid \Phi_1) \tag{5}$$

and

$$F_{\text{FA}} = \Pr(\parallel \boldsymbol{x}_0(\boldsymbol{H}_1, \boldsymbol{H}_2, ..., \boldsymbol{H}_N) - \boldsymbol{a} \parallel_2 > \nu \mid \Phi_0), \tag{6}$$

where $\Pr(\cdot)$ is the probability notation. The prerequisite of the above formulation is that the user's ID observed by all cooperative peers is correct, i.e. $\forall n, I_n = I$. Otherwise, the user to be authenticated will be directly identified as a spoofer by the cooperative peers, i.e. $\exists n, I_n \neq I$.

2) Collaboration Cost: The collaborative authentication recruiting more cooperative peers results in higher cost. This is because longer time and higher overhead will be required to request the collaboration and to achieve an agreement on the authentication decision. To achieve low collaboration cost, while maintaining high authentication accuracy, the optimal number of cooperative peers will be determined.

3) Authentication Robustness: In the mobile network, the network topology could be rapidly fluctuating, where the neighbors of the user to be authenticated dynamically vary. Hence, the automatic update of the heterogeneous cooperative peers list and authentication features is extremely helpful for improving the authentication robustness with guaranteed decision accuracy.

D. Problem Formulation

According to the proposed authentication system relying on the cooperation of multiple edge devices, our problem can be formulated as follows. Specifically, the objective function (OF) of collaborative authentication is denoted as $f(\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_N)$ with respect to the local variables of N cooperative peers.

$$\begin{aligned} &\min f(\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_N), \\ &\text{s.t. } \boldsymbol{x}_n - \boldsymbol{z} = 0, n = 1, 2, ..., N, \end{aligned} \tag{7}$$

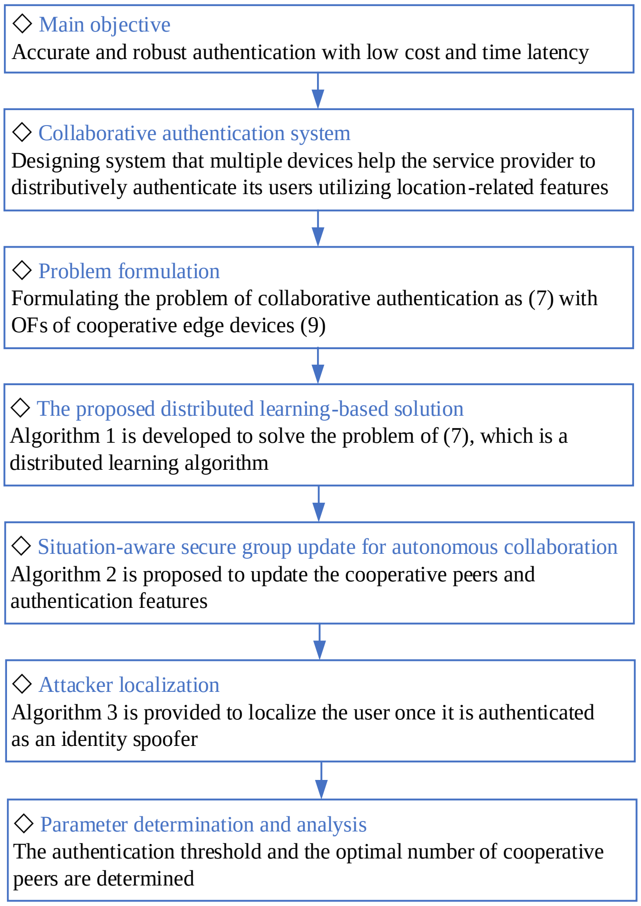
where $\boldsymbol{x}_n = (x_{n1}, x_{n2}, x_{n3})^\dagger$ are local variables and $\boldsymbol{z} = (z_1, z_2, z_3)^\dagger \in \Re^3$ is the global variable. Since the cooperative peers are at different locations and their observations are independent, the $f(\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_N)$ is separable. Then, we have

$$f(\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_N) = \sum_{n=1}^{N} f_n(\boldsymbol{x}_n), \tag{8}$$

where $f_n(\boldsymbol{x}_n)$ is the OF of the n-th cooperative peer. Upon denoting the real position of the n-th cooperative peer as $\boldsymbol{b}_n = (b_{n1}, b_{n2}, b_{n3})^\dagger$, its local OF is given by

$$f_n(\boldsymbol{x}_n) = \begin{cases} \parallel \boldsymbol{x}_n - \boldsymbol{b}_n \parallel_2 - H_{n1} & \text{RSSI} \\ \parallel \boldsymbol{x}_n - \boldsymbol{b}_n \parallel_2 - H_{n2} & \text{TRA} \end{cases}. \tag{9}$$

It can be observed that the local OF is designed as a closed, proper, and convex function based on the observations of the user's features. H_{n1} and H_{n2} represent the n-th cooperative peer's observations of distance between the user to be authenticated and itself relying on the RSSI and TRA, respectively. Hence, $f_n(\boldsymbol{x}_n)$ represents the difference between the local variable and real observation. Before detailing the proposed scheme further, we have provided a diagram in Fig. 2 for visualizing the detailed flow of our solution in the sequel.



◇ Main objective
Accurate and robust authentication with low cost and time latency

◇ Collaborative authentication system
Designing system that multiple devices help the service provider to distributively authenticate its users utilizing location-related features

◇ Problem formulation
Formulating the problem of collaborative authentication as (7) with OFs of cooperative edge devices (9)

◇ The proposed distributed learning-based solution
Algorithm 1 is developed to solve the problem of (7), which is a distributed learning algorithm

◇ Situation-aware secure group update for autonomous collaboration
Algorithm 2 is proposed to update the cooperative peers and authentication features

◇ Attacker localization
Algorithm 3 is provided to localize the user once it is authenticated as an identity spoofer

◇ Parameter determination and analysis
The authentication threshold and the optimal number of cooperative peers are determined

Fig. 2: Visualizing the proposed solution.

III. Edge Intelligence-Based Autonomous Collaborative Authentication

In achieving the accurate security provision, we propose an edge intelligence-based collaborative authentication scheme. Firstly, a distributed learning-based framework is developed, which relies on training harvesting by multiple cooperative peers. An information sharing and fusion strategy is designed in this framework to amalgamate the information collected and to train the models at the network edge, so that the network congestion and response time can be reduced. Then, a situation-aware secure group update algorithm is developed for autonomously updating both the set of cooperative peers and the resultant features, so that the authentication robustness and reliability can be improved. Finally, an algorithm is proposed for localizing the attacker once it is identified.

A. Distributed Learning-based Collaborative Authentication

In order to solve the optimization problem of (7) associated with N objective terms, the consensus alternating direction method of multipliers (ADMM) [48] is applied. The consensus ADMM algorithm for solving the problem of (7) can be derived from the following augmented Lagrangian function

$$\begin{aligned} & L_{n,\rho}(\boldsymbol{x}_n, \boldsymbol{z}, \boldsymbol{y}_n) \\ & = f_n(\boldsymbol{x}_n) + \boldsymbol{y}_n^{\dagger}(\boldsymbol{x}_n - \boldsymbol{z}) + (\rho/2)\|\boldsymbol{x}_n - \boldsymbol{z}\|_2^2, \end{aligned} \tag{10}$$

where $\rho > 0$ is termed as the penalty parameter and $\boldsymbol{y}_n = (y_{n1}, y_{n2}, y_{n3})^{\dagger}$. Then, the consensus ADMM algorithm conceived for solving the problem of (7) is given by

$$\boldsymbol{x}_n^{k+1} := \arg\min_{\boldsymbol{x}_n} L_{n,\rho}(\boldsymbol{x}_n, \boldsymbol{z}^k, \boldsymbol{y}_n^k), \tag{11}$$

$$\boldsymbol{z}^{k+1} := \frac{1}{N}\sum_{n=1}^{N}(\boldsymbol{x}_n^{k+1} + (1/\rho)\boldsymbol{y}_n^k), \tag{12}$$

$$\boldsymbol{y}_n^{k+1} := \boldsymbol{y}_n^k + \rho(\boldsymbol{x}_n^{k+1} - \boldsymbol{z}^{k+1}). \tag{13}$$

Specifically, we can observe from (9) and (10) that the expression $L_{n,\rho}(\boldsymbol{x}_n, \boldsymbol{z}, \boldsymbol{y}_n)$ is a closed, proper and convex function. Hence, $\arg\min_{\boldsymbol{x}_n} L_{n,\rho}(\boldsymbol{x}_n, \boldsymbol{z}^k, \boldsymbol{y}_n^k)$ can be readily solved [50]. Moreover, observed from (12) that the update of $\boldsymbol{z}$ depends on the average values of $\boldsymbol{x}_n$ and $\boldsymbol{y}_n, n = 1, 2, ..., N$. Upon denoting them as $\overline{\boldsymbol{x}}$ and $\overline{\boldsymbol{y}}$, respectively, the learning process of (11)-(13) can be simplified as

$$\boldsymbol{x}_n^{k+1} := \arg\min_{\boldsymbol{x}_n} L_{n,\rho}(\boldsymbol{x}_n, \overline{\boldsymbol{x}}^k, \boldsymbol{y}_n^k), \tag{14}$$

$$\boldsymbol{y}_n^{k+1} := \boldsymbol{y}_n^k + \rho(\boldsymbol{x}_n^{k+1} - \overline{\boldsymbol{x}}^{k+1}). \tag{15}$$

To achieve efficient collaborative authentication relying on multiple cooperative peers, a consensus is required, which contains the information sharing and fusion as well as the variable update in the proposed scheme: 1) To reduce the communication overhead, the collected authentication information and training models of cooperative peers will not be uploaded to the service provider; 2) As we can observe from (11)-(13), the $\boldsymbol{x}$-update and $\boldsymbol{y}$-update depend on the average values $\overline{\boldsymbol{x}}$ and $\overline{\boldsymbol{y}}$. Hence, these local parameters are shared among all the cooperative peers. The variables are separately updated to drive the variables towards consensus, and quadratic regularization helps pull the variables toward their average values, while still attempting to minimize each local function $f_n(\boldsymbol{x}_n)$.

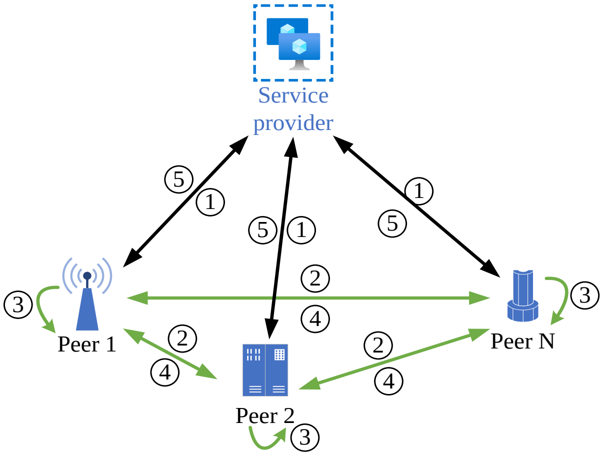


Fig. 3: Distributed learning-based collaborative authentication framework.

As shown in Fig. 3, the distributed learning-based collaborative authentication framework contains the following steps: *Step* ①. The service provider sends a collaboration request to multiple edge nodes, which are located in the vicinity of the user to be authenticated. The available devices send their agreements to the service provider, which will act as

cooperative peers;
Step ②. The associated cooperative peers estimate the features of the user to be authenticated, and share their estimates with other cooperative peers;
Step ③. All the cooperative peers locally update their variables via (14)-(15);
Step ④. All the cooperative peers share the learning parameters $\boldsymbol{x}_n^k$ with each other;
Step ⑤. If a convergence is achieved, i.e. $\boldsymbol{x}_0$, the authentication decision can be made at the cooperative peers via (4), and then they send their decisions to the service provider.

The proposed distributed learning-based solution is formulated in Algorithm 1.

Algorithm 1 Distributed learning-based collaborative authentication

```
Input: $N$ cooperative peers, authentication threshold $\upsilon$, error bound of learning $\varrho$;
Output: authentication results, i.e. legitimate user, identity spoofer, location spoofer;
for each cooperative peer $n$ in parallel
    estimates the authentication feature of user, i.e. RSSI or TRA;
    if the user cannot be observed
        it is identified as a location spoofer;
    end if
    shares feature estimations with others;
    while $\| \boldsymbol{x}_n^k - \boldsymbol{x}_n^{k-1} \| > \varrho$, do
        share parameters $\boldsymbol{x}_n^k$ with others;
        update local variables $\boldsymbol{x}_n$ and $\boldsymbol{y}_n$ via (14) and (15), respectively;
    end
end for
if a convergence $\boldsymbol{x}_0$ is achieved and $\| \boldsymbol{x}_0 - \boldsymbol{a} \|_2 \leq \nu$
    the user is authenticated as a legitimate device;
otherwise
    the user is identified as an identity spoofer;
end if
cooperative peers send the authentication decision to the service provider.
```

We can interpret the distributed learning-based solution of Algorithm 1 as a method for solving problems in which the objective and constraints are distributed across N cooperative peers. Each cooperative peer only has to handle its own objective and constraint term, plus a quadratic term which is updated each iteration. The quadratic terms (or more accurately, the linear parts of the quadratic terms) are updated in such a way that the variables converge to a common value, i.e. $\boldsymbol{x}_1 = \boldsymbol{x}_2 = \cdots \boldsymbol{x}_N = \boldsymbol{z}$, which is the solution of (7). Given the OF of each cooperative peer $f_n(\boldsymbol{x}_n)$ in (9), we can see that they are closed, proper, and convex. According to [48], [49], the proposed distributed learning-based algorithm can converge to the real position of the user to be authenticated relying on its feature observations. The convergence process can be expressed as

$$\boldsymbol{x}_n^k \rightarrow \boldsymbol{x}_0, n = 1, 2, ..., N, \text{as } k \rightarrow \infty. \tag{16}$$

Remark 1: It can be observed from Algorithm 1 that the collaborative authentication depends on the consensus of the cooperative peers relying on their observations. The user to be authenticated is only confirmed to be a legitimate one, when the convergence of the cooperative peers points to the real position of the legitimate user. Otherwise, it is deemed to be a spoofer. The proposed scheme moves the security provision to network edge without involving a centralized party. Moreover, the inherent features of the user to be authenticated are observed and exploited by the cooperative peers to enhance the security. Hence, it is extremely difficult for the attacker to crack the authentication method by imitating all the features as well as by misleading all the cooperative peers which are located near to the user.

B. Situation-Aware Autonomous Collaboration

To meet the stringent 6G networking demands, heterogeneous devices with time-varying position, network connection, and power/battery status will have to be supported in complex dynamic environments. To be more specific, when the user is moving, its cooperative peers may lose connection with it. Furthermore, due to the resource limitation of cooperative peers, e.g. battery and storage, some of them may be unavailable for helping the service provider after a while. To achieve flexible and robust collaborative security provision, a situation-aware secure group update algorithm is developed in Algorithm 2 to achieve autonomous collaborative authentication by adaptively updating the cooperative peers list and the associated authentication features.

Upon denoting the initial set of cooperative peers as $\Lambda[0]$, Algorithm 2 updates $\Lambda[t]$ by adaptively identifying the dynamic environment and network topology to achieve reliable and robust collaborative authentication at time instance t. Specifically, when one of the cooperative peers leaves set $\Lambda[t]$, another edge node will be asked to join in the collaborative authentication. The update of secure group is shown as

$$\Lambda[t+1] = \Lambda[t] - \{\widehat{\gamma}[t]\} + \{\gamma[t]\}, \tag{17}$$

where $\widehat{\gamma}[t]$ is the cooperative peer left the secure group at time t. The selection of new cooperative peer is formulated as

$$\gamma[t] = \arg\min_{j \in \Upsilon} \|\boldsymbol{x}_0[t] - \widehat{\boldsymbol{b}}_j\|_2, \tag{18}$$

which represents the available edge node located nearest to the user to be authenticated. Υ is the set of edge nodes, and $\widehat{\boldsymbol{b}}_j = (\widehat{b}_{j1}, \widehat{b}_{j2}, \widehat{b}_{j3})^\dagger$ denotes the real position of the j-th edge node, $j \in \Upsilon$.

It can be observed from Algorithm 2 that efficient authentication can be achieved through autonomous update of cooperative edge nodes and features. To be more specific, the service provider can supply a list of volunteering cooperative peers ahead of time, so that the latency of collaborative authentication can be reduced. Note that the proposed scheme will be suitable for those communication systems with sufficient edge nodes, e.g. intelligent building, Internet of Vehicles (IoV), VANETs, AANETs, and UAV networks, just to name a few.

Algorithm 2 Situation-aware secure group update

```
Input: initial set of cooperative peers $\Lambda[0]$, set of edge nodes
    $\Upsilon$ and their real positions $\widehat{\boldsymbol{b}}_j$;
Output: updated set of cooperative peers $\Lambda[t+1]$ and authen-
    tication result;
for authentication round $t = 1, 2, 3, ...$
    if a cooperative peer leaves the $\Lambda[t]$
        the service provider sends collaboration request
        to more devices located near the user to be
        authenticated;
        available devices send feedback to the service
        provider;
        the set of cooperative peers is updated via (17);
    end if
    all cooperative peers perform Algorithm 1 and send
    their availability for the next round of authentication
    to the service provider;
end for
```

C. Attacker Localization

Once an attacker, who performs identity spoofing attacks, is detected by the proposed collaborative authentication scheme via (4), it can also be localized by Algorithm 3. Upon denoting the real position of this attacker by $\boldsymbol{c} = (c_1, c_2, c_3)^\dagger$, the N cooperative peers can observe the location-related features of this attacker, i.e. its RSSI and TRA. Then, the convergence result of Algorithm 1 relying on the attacker's feature estimation can be formulated as

$$\boldsymbol{x}_n^k \to \boldsymbol{x}_0 = \boldsymbol{c} + \boldsymbol{\varepsilon}, n = 1, 2, ..., N, \text{as } k \to \infty, \tag{19}$$

where $\boldsymbol{\varepsilon}$ is the learning error due to the imperfect estimations of features used in the proposed scheme.

Algorithm 3 Attacker localization

```
Input: result of Algorithm 1;
Output: location of the identity spoofer;
if the user is authenticated as an identity spoofer
    if a consensus $\boldsymbol{x}_0$ is achieved among $N$ peers
        the attacker can be localized as $\boldsymbol{x}_0$ of (19);
    end if
end if
```

Note that the attacker cannot perfectly imitate the legitimate user and cheat all the cooperative peers when it locates at a different position from the legitimate user, especially when the proposed scheme utilizes more cooperative peers. This is not unexpected, because the cooperative peers locate near to the user to be authenticated and can observe different features as well as other information, e.g. certificate. It becomes more and more difficult for the attacker to spoof the legitimate user, when the number of cooperative peers is increased, demonstrating the benefit of the proposed scheme.

Remark 2: The attacker can only be localized, if it is an identity spoofer and at least one of the cooperative peers can identify the real ID of the attacker. If the attacker aims for performing location spoofing attacks, it cannot be localized by the cooperative peers, but it will be identified as a location spoofer directly. Moreover, once one of the cooperative peers is deceived by the attacker, the proposed collaborative authentication solution (i.e. Algorithm 1) will be divergent. In this case, the user to be authenticated will also be deemed to be an attacker.

D. Parameter Determination and Theoretical Analysis

In order to achieve improved authentication performance, including higher authentication accuracy and reduced collaboration cost, the authentication threshold ν and the number of cooperative peers N are determined in this subsection.

1) Determination of the threshold ν: As it is shown in (4), the authentication accuracy depends on the threshold ν. A lower threshold ν will lead to higher FA rate, while a higher ν will result in higher MD rate. Hence, there is a trade-off between the MD rate and FA rate with respect to authentication threshold ν. In order to achieve a better security performance, we formulate the threshold determination problem as

$$\begin{aligned} &\min_{\nu} F_{\text{FA}}, \\ &\text{s.t. } F_{\text{MD}} < \epsilon, \end{aligned} \tag{20}$$

where ϵ is the constraint of MD rate.

In this subsection, we consider an example, where the potential distances between the attacker and the legitimate user (denoted as d_a) obey the Log-normal distribution, which satisfies

$$\ln d_a \sim \aleph(\mu_a, \sigma_a^2), \tag{21}$$

where μ_a and σ_a^2 represent the mean and variance of the Gaussian distribution $\ln d_a$, respectively. $\aleph$ denotes the Gaussian distribution symbol. Then, the probability density function (PDF) of the above log-normal distribution is given by

$$g_{\Im}(\varsigma) = \frac{1}{\sigma_a \varsigma \sqrt{2\pi}} e^{-\frac{(\ln \varsigma - \mu_a)^2}{2\sigma_a^2}}, \tag{22}$$

where its mean and variance are $e^{\mu_a + \sigma_a^2/2}$ and $(e^{\sigma_a^2} - 1)e^{2\mu_a + \sigma_a^2}$, respectively.

Remark 3: It is reasonable to assume that the potential distances between the attacker and user obey Log-normal distribution, since a smart attacker focuses on observing and imitating the legitimate users, but it wants to avoid being spotted by the user at the same time. Hence, to glean increased utility, a spoofer will opt for a position having an appropriate distance from the user to be authenticated. Note that it is not critical to let the distances obey the Log-normal distribution - we only consider a reasonable example to provide an expression for the authentication threshold ν for the analysis in this section. In a specific communication application scenario, the distance distribution can be obtained according to the historical knowledge of the attacker detection by the service provider.

Given a specific application scenario, e.g. VANET and UAV network, if there is no knowledge of μ_a and σ_a^2, the initial authentication threshold is set to

$$\nu_{\text{Ini}} = \iota_0 + \iota, \tag{23}$$

where ι_0 and ι denote the error value of the positioning technique used in the system and the detection error value of Algorithm 1 in [m], respectively. In the other cases, the knowledge of μ_a and σ_a^2 could be inferred from the historical information of attackers detected by the service provider, e.g. the location information of attacks obtained by Algorithm 3. Then, the following Theorem can be formulated.

Theorem 1: Given μ_a and σ_a^2, the authentication threshold ν of the proposed scheme can be expressed as

$$\nu = \min\{\nu_{\text{opt}}, \nu_{\text{Ini}}\}, \tag{24}$$

where ν_{opt} satisfies

$$erf(\frac{\ln \nu_{\text{opt}} - \mu_a}{\sqrt{2}\sigma_a}) = 2\epsilon - 1. \tag{25}$$

$erf(\cdot)$ is the error function.

Proof: Please see Appendix 1.

Then, the FA rate of the proposed scheme can be calculated via (6), which depends on the number of cooperative peers N and their feature estimates.

2) Determination of number of cooperative peers N: The performance of collaborative authentication depends on the features estimated by the cooperative peers. Due to their imperfect estimations, utilizing more cooperative peers in the proposed scheme will reduce the learning loss and increase the authentication accuracy, but will impose high communication overhead and collaboration cost as well. Hence, there is a trade-off between the authentication performance and collaboration cost. To achieve the best performance, an optimal number of peers can be derived by maximizing the authentication accuracy under a given maximum collaboration cost threshold. Let us denote the number of iterations for one round of authentication in Algorithm 1 by K, the number of communication instances among cooperative peers for one round of collaborative authentication can be expressed as

$$\varphi = (K+1)N(N-1). \tag{26}$$

Then, the following theorem can be formulated.

Theorem 2: Given the collaboration cost constraint τ, the number of cooperative peers at time t is determined as

$$N[t] = \max\{N_{\min}, \min\{N_{\text{opt}}, N_0[t]\}\}, \tag{27}$$

where $N_{\min} = 3$ is the minimum number of cooperative peers. $N_0[t]$ is the maximum number of devices that are available to help the service provider at time instant t. The optimal number of cooperative peers is given by

$$N_{\text{opt}} = [\sqrt{\frac{\tau}{K_{\text{ave}}+1} + \frac{1}{4}} + \frac{1}{2}], \tag{28}$$

where $[\cdot]$ is the least integer function. K_{ave} represents the average learning steps of one-round of collaborative authentication by Algorithm 1.

Proof: Please see Appendix 2.

Note that the K_{ave} depends on the error bound of learning pre-set in Algorithm 1, i.e. ϱ. Given the above choice of parameters, improved security and reduced cost can be achieved based on the proposed scheme.

Remark 4: Corresponding to the given criteria in Section II-C, the determination of the threshold υ relies on the authentication accuracy, and the determination of N depends on the collaboration cost. To be more specific, there exists a trade-off between FA rate and MD rate with respect to threshold υ. We determine the threshold υ to achieve best authentication accuracy by solving the optimization problem of (20). Moreover, utilizing more cooperation peers will achieve better collaborative authentication accuracy while leading to higher cost. Hence, the determination of N is to achieve best security performance under the collaboration cost constraint.

IV. PERFORMANCE ANALYSIS AND EVALUATION

In evaluating the proposed scheme, two simulation examples are considered in this section, namely an indoor and an outdoor communication scenario. The results demonstrate the viability of the proposed scheme in the practical communication systems, such as the intelligent building, IoV, UAV networks, and so on.

A. Indoor Communication Scenario

In our first example, a 10×10 m indoor office is simulated, where the user to be authenticated is located at position [6,6] m. The service provider is located outside this office. 5 devices are located randomly in this indoor office acting as cooperative peers by harnessing the RSSI and TRA of the user to be authenticated for collaborative authentication.

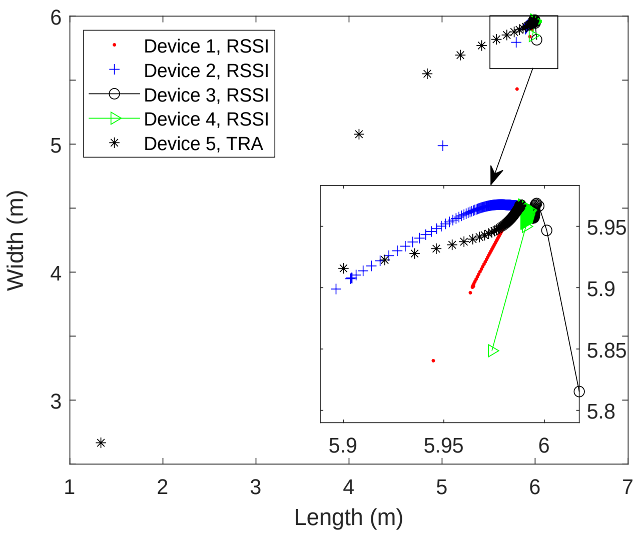


Fig. 4: Learning processes at the cooperative peers and the convergence of the proposed Algorithm 1 in an indoor communications scenario relying on 5 cooperative peers.

As shown in Fig. 4, Devices 1-4 use the RSSI and Device 5 utilizes the TRA for collaborative authentication, respectively. x-axis and y-axis represent the length and width of this indoor office in [m]. In this simulation, the service provider only has to know that Devices 1-5 are located in this office, so that the privacy of devices, including their location and mobility trajectory, can be concealed from the service provider while Devices 1-5 help the service provider to authenticate its user.

One can observe from Fig. 4 that all the learning parameters of Devices 1-5 converge to the real position of the legitimate user (i.e. [6,6] m) based on Algorithm 1 relying on their local RSSI and TRA information of the user. Hence, the user to be authenticated is identified as the legitimate user by the proposed scheme. This figure demonstrates the convergence results of Algorithm 1 and validate the proposed solution in collaboratively authenticating the users in a simulated indoor communication scenario.

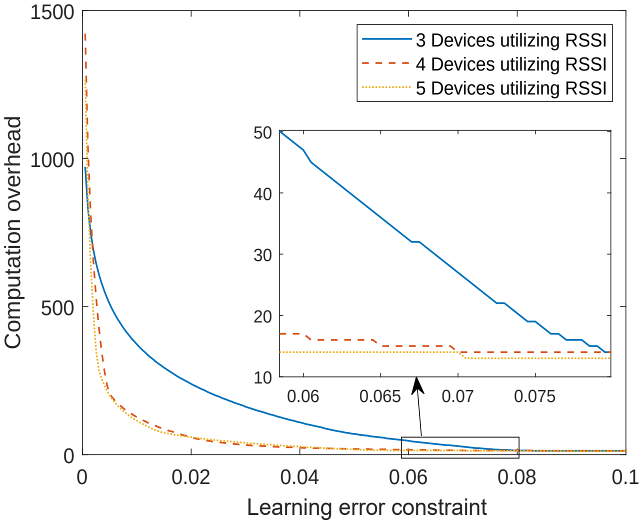


Fig. 5: Computation overhead of the proposed scheme with different numbers of cooperative peers utilizing RSSI.

Fig. 5 characterizes the computation overhead comparison results of the proposed scheme (i.e. Algorithm 1) relying on different numbers of cooperative peers utilizing the RSSI. We can observe from this figure that the proposed scheme requires lower computation overhead to achieve a consensus at a given error constraint by utilizing more cooperative devices for collaborative authentication. The reason for this trend is that more cooperative peers used can achieve better learning accuracy of Algorithm 1. Moreover, the number of computations required for achieving convergence decreases upon increasing learning error constraint. It also exhibits the trade-off between the learning accuracy and computation overhead in the proposed distributed learning-based solution (i.e. Algorithm 1).

The relationship between the threshold and authentication accuracy is characterized in Fig. 6. In this simulation, we assume that the potential distances between the attacker and the legitimate user obey the Log-normal distribution associated with different μ and σ values. Given the threshold of MD alert, the authentication threshold ν of the proposed scheme can be determined based on the result of Theorem 1. We can observe from Fig. 6 that the increased threshold of MD rate will result in an increased authentication threshold ν. It is also shown in Fig. 6 that a smaller μ results in reduced authentication threshold ν, because the attacker is located closer to the legitimate user in these cases.

Fig. 7 characterizes the authentication threshold vs. the FA rate of the proposed scheme by using different numbers of cooperative peers. They estimate the RSSI of the user to be authenticated for verification. We can observe from Fig. 7 that the FA rate dramatically decreases upon increasing the authentication threshold ν. This is because that the FA rate of the proposed scheme depends on the learning accuracy of the proposed distributed learning-based solution (i.e. Algorithm 1) relying on the imperfect RSSI estimation. Moreover, harnessing more cooperating peers reduces the FA rate of the proposed scheme. Fig. 6 and Fig. 7 also demonstrate that there is a trade-off between the FA rate and MD rate of the proposed scheme. We can also observe from Fig. 5 and Fig. 7 that the performance of the proposed scheme utilizing 4 cooperative devices is very close to that of utilizing 5 devices. Hence, we can choose 4 devices to be cooperators to reduce the collaboration cost in this case.

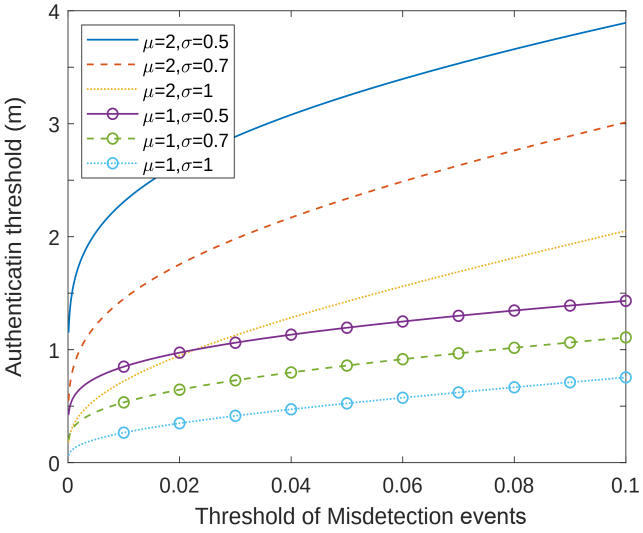


Fig. 6: Determined authentication threshold vs. threshold of MD rate of the proposed scheme in cases with different μ and σ values of Log-normal distribution in (21).

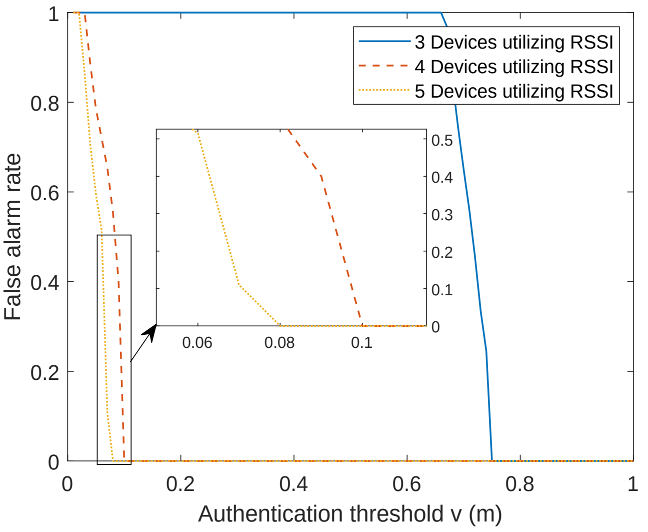


Fig. 7: Authentication threshold vs. FA rate of the proposed scheme with different numbers of cooperative peers.

B. Outdoor Communication Scenario

In this subsection, an outdoor communication scenario is simulated, where the legitimate user's position is [0,0] m and its velocity is 10km/h, the identity attacker's position is [0,10] m. Fig. 8 characterizes the learning processes of cooperative peers and the convergence of the proposed scheme. It can be observed from this figure that the learning processes converge to [0.1,0.35] m, which is close to the user, i.e. [0,0] m. The detection error value in this case is 0.364 m, which is the distance between the convergence result of Algorithm 1 and the real position of the user. Given the authentication threshold ν by Theorem 1, the user to be authenticated will be identified as a legitimate user.

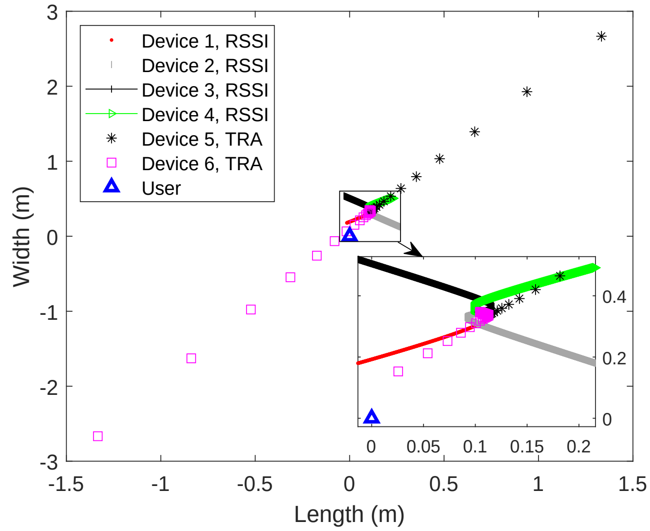


Fig. 8: Learning processes at cooperative peers and the convergence of the proposed scheme in an outdoor communication scenario, where Devices 1-4 choose the RSSI and Devices 5-6 utilize TRA.

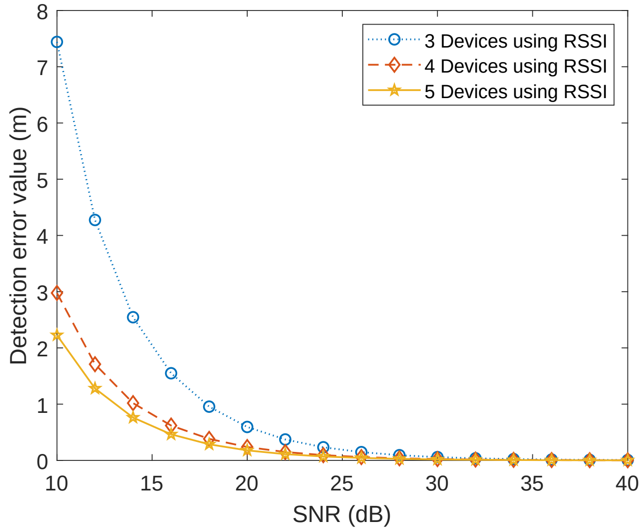


Fig. 9: SNR vs. detection error value of the proposed scheme in the cases that different numbers of cooperative peers are utilized, i.e. 5, 4, and 3.

Fig. 9 characterizes the signal-to-noise ratio (SNR) vs. the authentication accuracy of the proposed scheme. The cooperative peers' positions are [-16,12] m, [-22,-20] m, [28,16] m, [24,-18] m, and [12,14] m. We can observe from Fig. 9 that the detection error value decreases dramatically with the increase of SNR value, because the estimation errors of RSSI are lower. The performance of the case that 5 devices using RSSI is the best. The reason is that more cooperative peers utilized in the proposed scheme can collect more RSSI information for collaborative authentication, and for compensating the estimation errors of RSSI to achieve better performance.

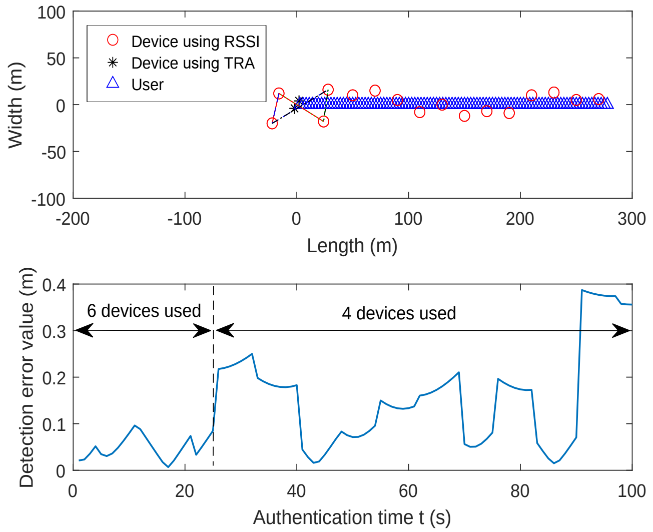


Fig. 10: Autonomous collaborative authentication process of the proposed scheme, where the SNR is 30dB.

Fig. 10 characterizes the simulated system topology relying on our autonomous collaborative authentication process, where 6 cooperative edge devices collected the observations of the user at beginning. During the movement of the user, the proposed scheme autonomously updates the cooperative devices. In this simulation, the other edge devices are located at [50,10] m, [70,15] m, [90,5] m, [110,-8] m, [130,0] m, [150,-12] m [170,-7] m, [190,-9] m, [210,10] m, [230,13] m, [250,5] m, and [270,6] m, which are shown as red circles in Fig. 10. In order to reduce the collaboration cost, the proposed scheme utilizes 4 cooperative edge devices for collaborative authentication based on situation awareness after the 25th authentication episodes. It can be observed from Fig. 10 that more devices autonomously join the collaborative authentication process utilizing the RSSI, and the proposed scheme continues operating during the user's movement. The results of Fig. 10 verify the authentication robustness of the proposed scheme in the noisy communication environment considered.

Fig. 11 characterizes the attacker localization process based on Algorithm 3. In this simulation, 4 cooperative peers are utilized for collaborative authentication relying on the RSSI. It is observed from this figure that the learning processes converge to [0.1,9.96] m, which is close to the real position of the attacker, i.e. [0,10] m. The detection error value in this case is 0.1045 m. Hence, the location of the identity spoofer can be determined by the proposed scheme.

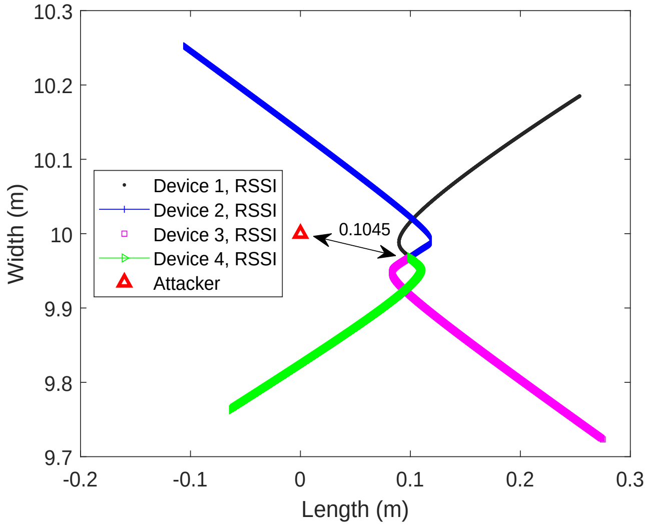


Fig. 11: Attacker localization based on the proposed scheme.

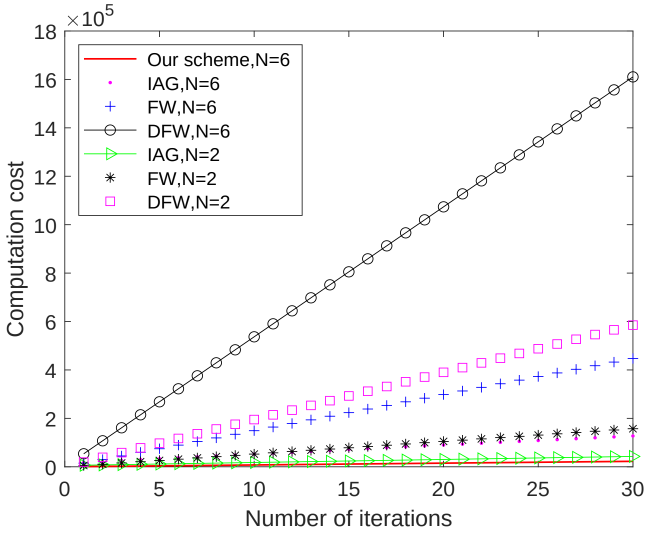


Fig. 12: Comparison results of the proposed distributed learning-based scheme and the centralized scheme of [29].

Fig. 12 characterizes the performance of the proposed scheme compared to the centralized schemes of [29], including an incremental aggregated gradient (IAG)-based scheme, Frank-Wolfe (FW)-based scheme, and distributed Frank-Wolfe (dFW)-based scheme. In [29], the authors proposed a centralized physical layer authentication framework relying on the help of 6 landmarks to collect the channel estimates of the user to be authenticated. We can observe from Fig. 12 that the computation cost of our scheme is much lower than that of all schemes of [29], because our scheme relies on the training models and collaborative processes at the network edge. The cooperative peers do not have to transmit the collected information and training models to the service provider for every iteration. More importantly, the problem is modeled as a convex problem, which is convenient to solve. Extra 6 landmarks are used for security purpose in [29], while the cooperative peers in this paper could be the existing edge devices and edge servers/access points of the network. Hence, our scheme can be widely used in 5G/6G networks.

V. Conclusion

This paper proposed a new collaborative authentication scheme, which relies on multiple edge devices by distributively sharing authentication information among them. The edge nodes help the service provider to authenticate its users based on local information collection and processing. Hence, the authentication accuracy can be improved by relying on security provision at the network edge, by harnessing multiple cooperating devices, and by utilizing multiple authentication features. A situation-aware secure group update algorithm was developed for updating the cooperative group of edge nodes and their associated authentication features autonomously. To localize the identity spoofer once it is authenticated, an attacker localization algorithm was proposed. Our results characterized the proposed scheme in both indoor and outdoor communication scenarios. The results demonstrated that the proposed scheme outperforms the existing centralized authentication schemes.

In our future work, we will focus on further improving the authentication accuracy of the proposed collaborative authentication scheme in the noisy communication systems operating at low SNRs. We will also explore the employment of more features for collaborative authentication, which are robust in dynamic communication environments. The benefits of edge intelligence will be studied for autonomous security provision in our future work, which will move the security framework from the center to the network edge, so that the response time and network load of the security provision will be reduced.

VI. Appendix

A. Appendix 1: Proof of Theorem 1

Given μ_a and σ_a^2, the MD rate of the proposed collaborative authentication scheme can be rewritten according to (5) and (22), which is formulated as

$$\begin{aligned} F_{\mathrm{MD}} &= \int_0^{\nu} \frac{1}{\sigma_a x\sqrt{2\pi}} e^{-\frac{(\ln x-\mu_a)^2}{2\sigma_a^2}} dx \\ &= \frac{1}{2}(1+erf(\frac{(\ln \nu-\mu_a)}{\sqrt{2}\sigma_a})). \end{aligned} \tag{29}$$

Since there is a trade-off between the MD rate and FA rate of the system, the minimum of F_{FA} can be achieved when $F_{\mathrm{MD}} = \epsilon$. Hence, the threshold determination process can be formulated as

$$\frac{1}{2}(1+erf(\frac{(\ln \nu-\mu_a)}{\sqrt{2}\sigma_a})) = \epsilon. \tag{30}$$

Then, ν_{opt} satisfies (25) and the result of (24) can be obtained.

B. Appendix 2: Proof of Theorem 2

Given the collaboration cost constraint τ, we have

$$\varphi \leq \tau \Rightarrow N \leq [\sqrt{\frac{\tau}{K+1}+\frac{1}{4}}+\frac{1}{2}]. \tag{31}$$

Since the cooperative peers are trusted, collaborative authentication can be performed based on the observation of the user's position by comparing it to the reported position, i.e. to $\boldsymbol{a}$. We need no less than 3 observations of the location-related features by different devices to determine the position of a user. Moreover, upon denoting the maximum number of devices that are available for helping the service provider at time t by $N_0[t]$, the optimal number of cooperative peers is chosen to be as high as possible to achieve the best authentication performance. Hence, the result of (27) can be readily derived.

References

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55-61, 2020.

[2] H. Fang, L. Xu, and X. Wang, "Coordinated multiple relays based physical layer security improvement: a single leader-multiple followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197-209, 2018.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

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

[5] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384-2428, 2021.

[6] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406-138446, 2020.

[7] F. Shu, L. Yang, X. Jiang, W. Cai, W. Shi, M. Huang, J. Wang, and X. You, "Beamforming and transmit power design for intelligent reconfigurable surface-aided secure spatial modulation," *IEEE J. Sel. Top. Sign. Proces.*, vol. 16, no. 5, pp. 933-949, 2022.

[8] H. Fang, X. Wang, Z. Xiao, and L. Hanzo, "Autonomous collaborative authentication with privacy preservation in 6G: From homogeneity to heterogeneity," *IEEE Network*, vol. 36, no. 6, pp. 28-36, 2022.

[9] R. Khan, P. Kumar, D. Nalin, K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196-248, 2020.

[10] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384-2428, 2021.

[11] Q. Yan and D. Tuninetti, "Key superposition simultaneously achieves security and privacy in cache-aided linear function retrieval," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5250-5263, 2021.

[12] J.-N. Liu, X. Luo, J. Weng, A. Yang, X. A. Wang, M. Li, and X. Lin, "Enabling efficient, secure and privacy-preserving mobile cloud storage," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1518-1531, 2022.

[13] D. Dłaz-Snchez, A. Marłn-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. Simon Sherratt, "TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3502-3531, 2019.

[14] P. Szalachowski, "Password-authenticated decentralized identities," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4801-4810, 2021.

[15] K.-A. Shim, "BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1545-1554, 2017.

[16] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proc. IEEE*, vol. 94, no. 2, pp. 467-478, 2006.

[17] M. Zorgui, Z. Rezki, B. Alomair, and M.-S. Alouini, "The diversity-multiplexing tradeoff of secret-key agreement over multiple antenna channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1562-1574, 2015.

[18] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517-1530, 2016.

[19] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. Li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030-1034, 2021.

[20] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574-583, 2015.

[21] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18-33, 2019.

[22] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692-2705, 2020.

[23] N. Xie, Z. Li, and H. Tan, "A survey of physical layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282-310, 2021.

[24] H. Fang, A. Qi, and X. Wang, "Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement," *IEEE Network*, vol. 34, no. 3, pp. 24-29, 2020.

[25] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3068-3079, 2020.

[26] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, "A collaborative security framework for software-defined wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2602-2615, 2020.

[27] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 954-968, 2019.

[28] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1794-1805, 2015.

[29] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676-1687, 2018.

[30] C. Huang, G. Chen, and K.-K. Wong, "Multi-agent reinforcement learning-based buffer-aided relay selection in IRS-assisted secure cooperative networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4101-4112, 2021.

[31] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1284-1298, 2022.

[32] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge artificial intelligence for 6G: Vision, enabling technologies, and applications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 5-36, 2022.

[33] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4221-4232, 2020.

[34] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5G and beyond perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2191-2217, 2021.

[35] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009-2030, 2020.

[36] K. Yang, T. Jiang, Y. Shi, and Z. Ding, "Federated learning via over-the-air computation," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2022-2035, 2020.

[37] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions, " *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50-60, 2020.

[38] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621-634, 2019.

[39] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 4, pp. 1065-1079, 2018.

[40] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4221-4232, 2020.

[41] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616-629, 2021.

[42] P. Ky. ti et al., WINNER II Channel Models, Standard IST-4-027756 WINNER II, D1.1.2 V1.2, 2007.

[43] T. J. Karr, “Atmospheric phase error in coherent laser radar,” *IEEE Trans. Antennas Propag.*, vol. 55, no. 4, pp. 1122-1133, 2007.

[44] H. Zhao, C. Wang, Y. Lin, F. Guillemard, S. Geronimi, and F. Aioun, “On-road vehicle trajectory collection and scene-based lane change analysis: Part I,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 1, pp. 192-205, 2017.

[45] A. Zanella, “Best practice in RSS measurements and ranging,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2662-2686, 2016.

[46] M. Barbi, C. Garcia-Pardo, A. Nevrez, V. P. Beltrn, and N. Cardona, “UWB RSS-based localization for capsule endoscopy using a multilayer phantom and in Vivo measurements,” *IEEE Trans. Antennas Propag.*, vol. 67, no. 8, pp. 5035-5043, 2019.

[47] F. Zafari, A. Gkelias, and K. K. Leung, “A survey of indoor localization systems and technologies,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2568-2599, 2019.

[48] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, “Distributed optimization and statistical learning via the alternating direction method of multipliers,” *Found. Trends Machine Learning*, vol. 3, no. 1 pp. 1-122, 2010.

[49] D. Gabay and B. Mercier, “A dual algorithm for the solution of nonlinear variational problems via finite element approximations,” *Computers and Mathematics with Applications*, vol. 2, pp. 17C40, 1976.

[50] S. Boyd and L. Vandenberghe, “Convex optimization,” Cambridge University Press, 2004.

He Fang (Member, IEEE) is a full professor with the School of Electronic and Information Engineering, Soochow University, China. She received her Ph.D. degree in Electrical and Computer Engineering from Western University, Canada, in 2020. Her research interests include intelligent security provision, trust management, machine learning, distributed optimization and collaboration techniques. She currently serves as a Guest Editor and Topical Advisory Panel Member for several journals, including IEEE Wireless Communications. She was involved in many IEEE conferences including IEEE GLOBECOM, VTC, and ICCC, in different roles such as Session Chair and TPC member. She also served as the Vice-Chair of Communication/Broadcasting Chapter, IEEE London Section, Canada, from Sep. 2019 to Aug. 2021.

Zhenlong Xiao (Member, IEEE) received the B.S. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2008, the M.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011, and the Ph.D. degree from the Hong Kong Polytechnic University, Hong Kong, in 2015. He is currently an Associate Professor with the Department of Informatics and Communication Engineering, School of Informatics, Xiamen University, Xiamen, China. His research interests include the nonlinear signal processing, graph signal processing, and collaborative signal processing.

Xianbin Wang (Fellow, IEEE) is a Professor and Tier-1 Canada Research Chair at Western University, Canada. He received his Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

Prior to joining Western, he was with Communications Research Centre Canada as a Research Scientist/Senior Research Scientist between July 2002 and Dec. 2007. From Jan. 2001 to July 2002, he was a system designer at STMicroelectronics. His current research interests include 5G/6G technologies, Internet-of-Things, communications security, machine learning and intelligent communications. Dr. Wang has over 500 highly cited journal and conference papers, in addition to 30 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of Canadian Academy of Engineering, a Fellow of Engineering Institute of Canada, a Fellow of IEEE and an IEEE Distinguished Lecturer. He has received many prestigious awards and recognitions, including IEEE Canada R.A. Fessenden Award, Canada Research Chair, Engineering Research Excellence Award at Western University, Canadian Federal Government Public Service Award, Ontario Early Researcher Award and six IEEE Best Paper Awards. He currently serves/has served as an Editor-in-Chief, Associate Editor-in-Chief, Editor/Associate Editor for over 10 journals. He was involved in many IEEE conferences including GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE and CWIT, in different roles such as general chair, symposium chair, tutorial instructor, track chair, session chair, TPC co-chair and keynote speaker. He has been nominated as an IEEE Distinguished Lecturer several times during the last ten years. Dr. Wang was the Chair of IEEE ComSoc Signal Processing and Computing for Communications (SPCC) Technical Committee and is currently serving as the Central Area Chair of IEEE Canada.

Li Xu (Member, IEEE) is a Professor with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou. He received the Ph.D. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004. He currently is the Dean of the College of Computer and Cyber Security and the Director of Fujian Key Laboratory of Network Security and cryptography. His research interests include network and information security, wireless networks and communication, Big data and intelligent information in complex networks. He has authored or coauthored more than 180 papers in international journals and conferences, including IEEE Transactions on Information Forensics and Security, IEEE Transactions on Computer, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Parallel and Distributed Systems.

Lajos Hanzo (FIEEE’04) received the Honorary Doctorates degree from the Technical University of Budapest and Edinburgh University. He is a Foreign Member of the Hungarian Science-Academy and a fellow of the Royal Academy of Engineering (FREng), IET, and EURASIP. He was a recipient of the IEEE Eric Sumner Technical Field Award. For more information, see (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo).