Autonomous Collaborative Authentication with Privacy Preservation in 6G: From Homogeneity to Heterogeneity

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

***Abstract*—The emerging collaborative authentication schemes are capable of outperforming the conventional isolated methods as a benefit of their multi-dimensional data/information gleaned, but they face new challenges in the sixth generation (6G) wireless networks owing to their increased overhead, limited flexibility and autonomy. Moreover, they may also be vulnerable to the privacy leakage of individual entities. These challenges are mainly due to the complex heterogeneous network architecture, owing to the distributed nature of the devices and information involved as well as the diverse security requirements of the 6G-aided vertical systems. As a remedy, we introduce autonomous collaborative authentication for achieving security enhancement through the situation-aware cooperation of different security mechanisms, of heterogeneous security information/context, and of heterogeneous devices and networks. For this purpose, a federated learning-based collaborative authentication scheme capable of privacy-preservation is developed, where cooperative peers observe and locally analyze heterogeneous information of the authenticating device, and afterwards update their authentication models locally. By sharing their authentication models rather than directly sharing the observed authentication information, privacy preservation can be achieved based on the proposed scheme. Moreover, given the time-varying heterogeneous network environment and the wide range of quality-of-service (QoS) requirements, the membership of the group collaborating in support of distributed authentication is updated based on the situation-dependent conditions. To further reduce the communication overhead, a locally collaborative learning process is further developed, where both the updated parameters and observed authentication information are stored and processed locally at the cooperative peers. Finally, a smart contract is designed for achieving collaborative security combined with privacy preservation and for providing accountable services.**

INTRODUCTION

Evolving from the trend in the fifth generation (5G), the sixth generation (6G) connections will drive beyond personal communications to the fully-fledged Internet-of-Things (IoT), interconnecting machines, vehicles, computing resources, industry/business processes, and even robotic agents [1]. The 6G systems are expected to further improve the reliability, capacity, power-efficiency and low latency trade-offs in support of challenging applications ranging from autonomous systems to extended reality [1]. New lightweight devices and wearables will emerge relying on distributed computing, intelligent computing surfaces, and storage enabled by the edge cloud [2]. Key emerging services in 6G include holographic teleportation, extended reality, unmanned aerial vehicle (UAV) services, autonomous services, Internet-of-Everything (IoE), and ambient connectivity [3].

Due to the critical roles of 6G networks and the enormous interconnection integrated in 6G-aided systems, any potential security risks as exemplified by eavesdropping, spoofing, forgery, interception, and denial-of-service attacks, could lead to catastrophic consequences. In this article, we focus on authentication mechanisms for confirming the identities of communicating entities, as well as their access to network, to the information available and to the resources associated with their identities within the system [4]. However, the heterogeneous architecture, diverse devices and data, as well as the complex environment and information uncertainties impose new challenges in terms of the reliable and efficient authentication of 6G networks. To be more specific, the heterogeneous nature of a 6G system makes it difficult to utilize global information for dynamic security provision through tight collaboration among different networks relying on different

The work of H. Fang and X. Wang was supported by the NSERC Discovery Grant Program RGPIN-2018-06254. The work of L. Hanzo was supported by 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, 215006, China, and was with the Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada. Email: fanghe@suda.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.

Z. Xiao is with the Department of Information and Communication Engineering, School of Informatics, Xiamen University, Xiamen 361005, China. Email: zlxiao@xmu.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.

protocols. The heterogeneous nature of devices and data dose not readily lend itself to convenient information fusion, leading to inefficient collaboration and potentially unsafe decisions. Hence, developing a reliable, efficient, and dynamic authentication method for achieving the maximum security in the heterogeneous 6G systems becomes a challenging task.

Challenges of Isolated Authentication Schemes

Existing security mechanisms rely on isolated network-specific designs, which are typically conceived for a particular network and application, as well as for a certain layer of the protocol stack. Such mechanisms typically involve two parties, namely as entity to be authenticated and another performing the authentication. These isolated authentication schemes validate the legality of devices without any cooperation with the different layers of the protocol stack, other devices or networks. For example, the classic Diffie-Hellman key agreement protocol is vulnerable to the man-in-the-middle attacks if two users involved in the protocol do not share any authenticated information about each other prior to the protocol execution, such as the public keys, certificates, passwords or shared keys [5]. The authentication scheme of [6] only utilizes the unique physical layer attributes, e.g. the communication links, devices, or physical environment-related features, to identify the transmitter. The method of [7] realizes physical layer authentication by embedding an authentication tag into a message signal. However, these non-collaborative authentication schemes face following challenges in 6G networks:

- **High security overhead/latency and low authentication reliability.** In the heterogeneous 6G network, using network- or layer-specific security methods will cause both extra latency and computation overhead as well as low-reliability of authentication. Specifically, conventional techniques impose higher computational overhead to increase the difficulties for attackers to crack the security keys. Purely relying on conventional cryptographic techniques cannot meet the diverse requirements in 6G communications, especially for those requiring extremely short end-to-end latency. Furthermore, physical layer authentication techniques may be ill-equipped for dealing with mutually observable attributes and for the communications involving heterogeneous networks, leading to low authentication reliability.
- **Limited authentication alternatives, knowledge and computational resources for guaranteed security provision.** Only exploring security credential or features of a simple layer of the protocol stack for authentication inevitably has limited security compared to comprehensive multi-dimensional observations of an extended search space. For instance, the authentication reliability of purely physical layer attributes is eroded by imperfect channel estimation in complex dynamic environments. Furthermore, if authentication purely relies on a single isolated device, its security remains more limited than that of collaborative authentication.
- **Inflexible and risk-agnostic security provision.** The existing non-collaborative authentication schemes tend to be risk-agnostic. To elaborate a little further, the conventional cryptographic techniques usually increase the security by escalating the difficulties for attackers to crack the security keys at the cost of a high computation complexity and long latency. Furthermore, the performance of physical-layer authentication strongly depends on the features used, which may become impaired in dynamic environments without risk-aware solutions.

In 6G networks, the authentication has to be harmonized with the physical-target innovations and the applications by close cooperation between the most appropriate combination of network segments, devices, and communication features, as detailed in this article.

Existing Collaborative Authentication Frameworks and Their Challenges

Collaborative authentication frameworks have already been proposed for solving many practical security problems, such as spoofing attacks, intrusion detection, and denial of service attacks [8]. A set of collaborative authentication frameworks are summarized in Figure 1. Diamant *et al.* [9] proposed a cooperative authentication scheme (see Figure 1 (a)) for underwater acoustic sensor networks utilizing physical-layer features. This scheme employs multiple trusted nodes for independently helping the sink to evaluate each incoming packet's belief and then reach an authentication decision. The security frameworks of Figure 1 (a)-(c) are studied by Heng *et al.* [10] for authentication by utilizing Global Positioning System (GPS) signals for detecting spoofing attacks. The security framework of Figure 1 (d) is widely studied in cooperative communications [11]. Moreover, the blockchain technology has been studied for both distributed key management and authentication [12]. The benefits of collaborative authentication include, but are not limited to:

- **Reliable and efficient security provision.** In collaborative authentication schemes, the devices/users are expected to share security-related information for improving their performance,

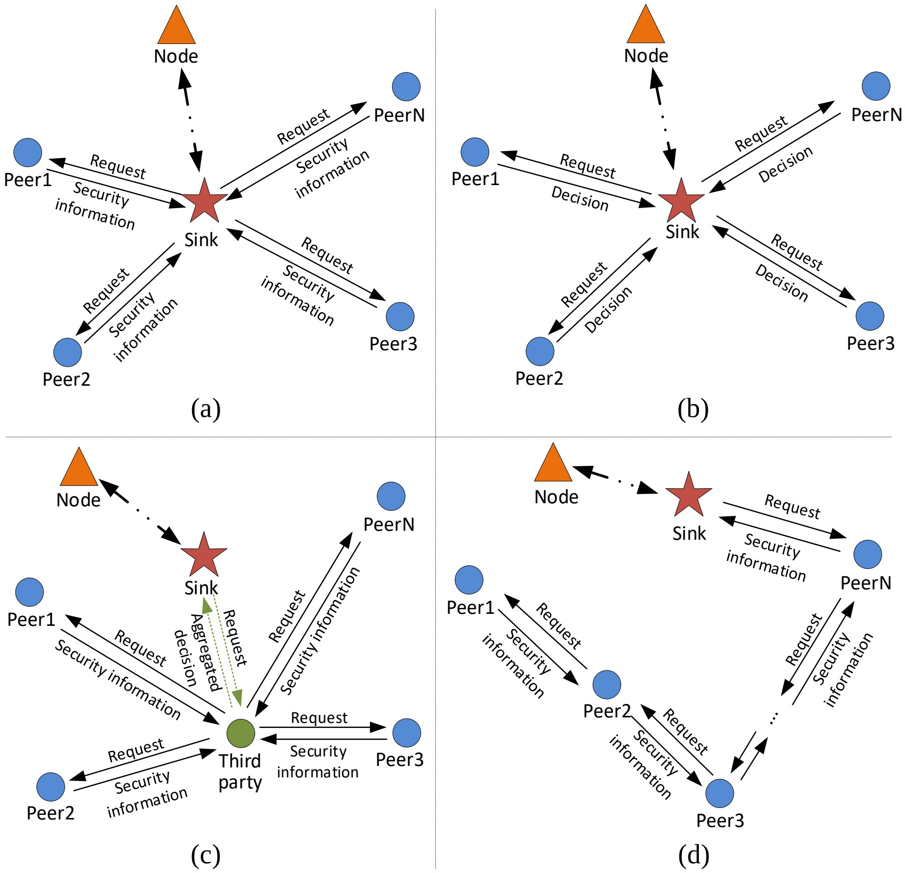


Fig. 1: Existing collaborative authentication frameworks.

which will compensate for uncertainties and imperfect observations.

- **Robustness improvement in dynamic or untrusted environment.** The use of multi-dimensional data/information gleaned from cooperative peers will improve the robustness to perturbations, hence resulting in improved security.
- **Increased difficulty in attacking collaborative systems by adversaries.** Relying on multiple devices or different security mechanisms in collaborative systems increases difficulty for the adversaries to successfully imitate legitimate devices and compromise them.

Despite these compelling benefits, the existing collaborative authentication schemes also face numerous challenges in heterogeneous 6G networks as detailed below:

- **Homogeneous nature.** Most of the existing collaborative authentication schemes only explore cooperation with their homogeneous counterparts, but ignore cooperation with different security methods and other protocol layers. Given the rapidly growing number of heterogeneous devices and their data collected for supporting intelligent services, homogeneous schemes remain inefficient in 6G networks. They are particularly inefficient in dealing with handover authentication in heterogeneous networks, when the devices move from one cell to another. Hence, upgrading homogeneity to heterogeneity is extremely helpful for reliable collaborative authentication in 6G.
- **Limited flexibility and automation.** The data collection and aggregation models of the existing collaborative security schemes [9], [10] tend to be time-invariant. Moreover, they are deficient in modeling heterogeneous data, thus tend to fail in capturing the critical aspects of the practical environment and devices. More importantly, the lack of adaptive data collection and aggregation as well as the autonomous exploitation of heterogeneous security information and cooperation with other devices will result in low authentication reliability in 6G communications requiring agile situation-aware services and flexible processes.
- **Privacy erosion:** For collaborative authentication, the collection and correlation of multi-dimensional data are required. However, the significantly increased level of interconnectivity in

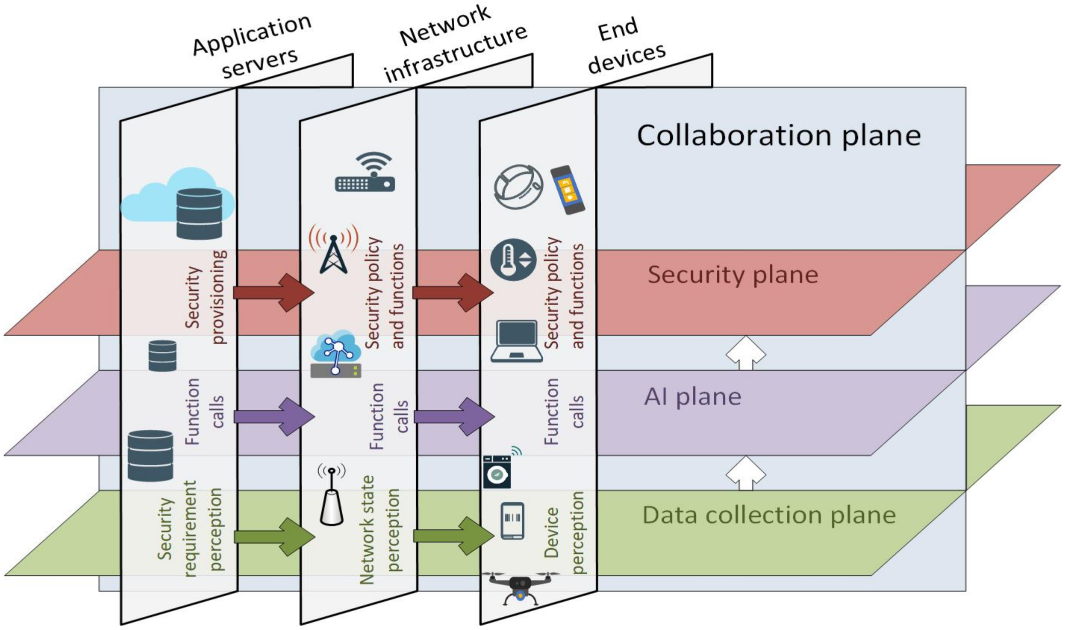


Fig. 2: Conceptual architecture of a 6G network using autonomous collaborative security.

6G leads to increased probability of privacy erosion. To be more specific, combining the multi-dimensional data gleaned from different layers, devices and applications will enhance the security, but it will also increase the risk of leaking sensitive data of individual peers.

- **Lack of accountability.** Most of the existing collaborative authentication schemes assume that the cooperative peers are fully trusted. However, the cooperative peers could be inquisitive, malicious or hostile, who may provide misleading authentication decision or information, leading to the failure of collaborative authentication. Hence, all the cooperative peers should be accountable for their behaviors to promote participation fairness and to increase the overall system stability.

In a nutshell, an autonomous collaboration plane relying on distributed agents and heterogeneity is required for authentication intrinsically coupled with privacy preservation. A potential conceptual architecture suitable for 6G networks relying on autonomous collaborative security is portrayed in Figure 2, which is constituted by the application servers, network infrastructure, and end devices. These heterogeneous devices access the network through different access points, and reach different application servers. In this architecture, three horizontal planes are introduced for autonomous collaborative security provision, including the data collection plane, AI plane, and security plane. The data collection plane collects and stores the data arriving from the intelligent network elements, which can be accessed by the AI plane for autonomous collaborative authentication.

Contributions of This Article

To overcome the above challenges, collaborative authentication with privacy preservation relying on edge intelligence is conceived, where multiple heterogeneous cooperative peers assist the service provider in authenticating its users with the aid of heterogeneous observations. The contributions of this article are summarized as follows:

- A federated learning-based collaborative authentication scheme is proposed. It employs a distributed training process, where the learning models are updated locally at the cooperative peers and then the model parameters are forwarded to the service provider for model update. Privacy preservation is achieved during the security provision process, since the observation themselves are not uploaded to the service provider.
- A situation-aware secure group update strategy is designed for adaptively updating the cooperations of different security mechanisms, heterogeneous security information/context, and heterogeneous devices. We also develop an autonomous approach for the handover authentication of heterogeneous networks, when the user is moving from one cell to another.
- In order to reduce communication overhead of the proposed federated learning-based collaborative authentication, a locally collaborative process is

developed, where both the model parameters and the information observed for authentication are processed locally only at the cooperative peers.

- A smart contract is designed for expressing the requirements and implementing the proposed schemes, as well as for ensuring that they will be appropriately executed. Autonomous collaborative authentication is achieved by intelligently combining the heterogeneous authentication information, the assistance of cooperative peers, and the awareness of different situations by harnessing the intelligent distributed processing capability of 6G systems.

FEDERATED LEARNING-BASED COLLABORATIVE AUTHENTICATION

Firstly, a collaborative authentication with privacy preservation scheme is proposed based on the federated learning technique [13]. Again, the observations of security information/context used for authentication are retained locally by the heterogeneous peers, and only the model parameters are aggregated and forwarded to the service provider. As a benefit, the private information of the cooperative peers can be preserved.

As shown in Figure 3, a service provider has to authenticate its users for secure communications relying on the multiple cooperative peers. To elaborate, the cooperative peers help to collect the user's security information/context, such as the identity/password, hardware token, biometric features, screen touches, barometer, mobility, trajectory, communication link-related features, device-specific features and location-related features. If the observations of the service provider are the same as those of the cooperative peers, the user will be authenticated as legitimate. Otherwise, the user will be classified as an attacker. However, directly uploading these security-related pieces of information observed by the cooperative peers to the service provider may result in potential erosion of both user's and cooperative peers' privacy. Hence, collaborative authentication combined with intrinsic privacy protection is extremely helpful for efficient security provision.

We propose a federated learning-based scheme for performing collaborative authentication without leaking the private information observed by cooperative peers to the service provider, which is shown in Figure 3. To achieve collaborative authentication, firstly, the service provider should designate several peers (can be heterogeneous) to participate in the authentication. Then, the different users' authentication features can be observed by the specific peers, and a collaborative authentication model can be constructed based on the features adopted, denoted as $\mathscr{F}(\boldsymbol{w})$. The cooperative peers update the authentication model parameters $\boldsymbol{w} = (w_1, w_2, ..., w_M)^{\mathrm{T}}$ in parallel, purely based on their local knowledge. The goal of this collaborative authentication scheme is to minimize the combination of objective functions $\mathscr{F}_n(\boldsymbol{w})$ uploaded by all the cooperative peers. The detailed collaborative authentication process is summarized in Algorithm 1, which corresponds to Steps 1-5 of Figure 3.

Algorithm 1 Federated learning-based collaborative authentication with privacy preservation

```
Service provider executes (Step 1):
designate cooperative peers;
build authentication model based on selected feature(s);
initialize model parameters $\boldsymbol{w}_0$;
for each round $t = 1, 2, ...$ do
    service provider broadcasts global model $\mathscr{F}(\boldsymbol{w})$
    to its cooperative peers (Step 2);
    for each peer $n$ in parallel do
        update parameters $\boldsymbol{w}_{n,t-1}$ with local observed
        features (Step 3);
        upload new parameters $\boldsymbol{w}_{n,t}$ to service
        provider (Step 4);
    end for
    service provider aggregates model parameters
    from all peers and updates global model (Step 5);
end for
```

We can observe from the collaborative authentication process of Algorithm 1 and Figure 3 that the observations of the user's security information/context are stored and processed locally by the cooperative peers, and only the model parameters extracted are sent to the service provider for global authentication model updates and secure aggregation. Hence, privacy preservation can be achieved by the proposed federated learning-based collaborative authentication scheme. Moreover, in the proposed schemes, we focus our attention on the collaboration mechanisms used for authentication. The potential attacks encountered by the federated learning process, such as backdoor attacks and inference attacks, are not considered in this paper. They will be tackled in our future research.

SITUATION-AWARE COLLABORATIVE AUTHENTICATION

The proposed federated learning-based collaborative authentication of Algorithm 1 is a static framework, since it does not consider the cooperative peers' resources/conditions and exploits fixed authentication information. Let us assume that a cooperative device is harnessed in the collaborative authentication, but its battery is exhausted or its communication channel is of low signal-to-noise ratio during the model parameters'

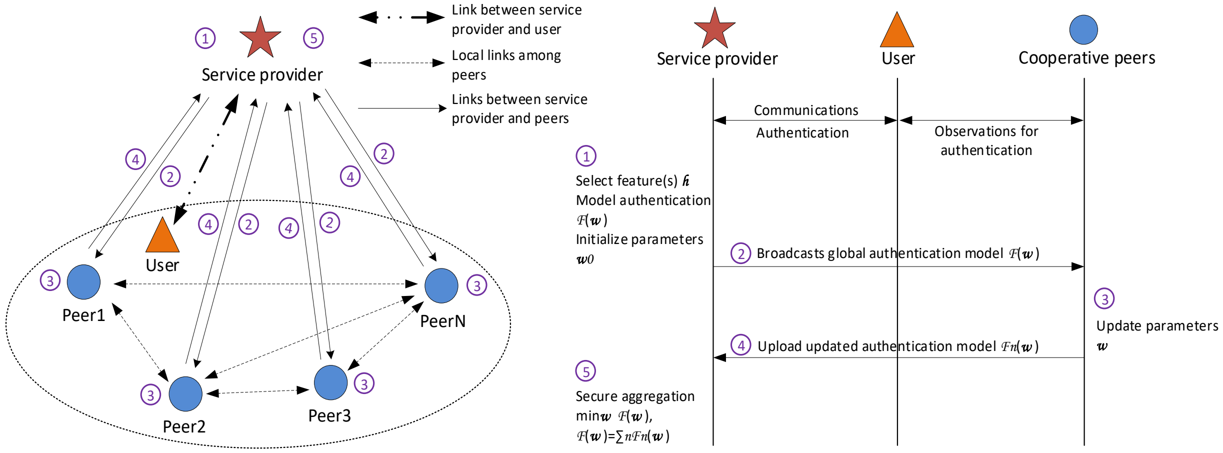

1
5
Service provider
Link between service provider and user
Local links among peers
Links between service provider and peers
4
2
2
4
User
4
2
4
2
3
Peer1
3
PeerN
3
Peer2
Peer3
3
Service provider
User
Cooperative peers
Communications
Authentication
Observations for authentication
1
Select feature(s) h
Model authentication $F(w)$
Initialize parameters $w0$
2 Broadcasts global authentication model $F(w)$
3
Update parameters w
4 Upload updated authentication model $Fn(w)$
5
Secure aggregation
$\min_w F(w)$,
$F(w)=\sum nFn(w)$

Fig. 3: The proposed federated learning-based collaborative authentication scheme.

update. Such undesired situations will obviously degrade the convergence of Algorithm 1 and thus erode the authentication performance. Hence, the specific situations of both the cooperative peers and their authentication features should be taken into account in the proposed federated learning-based scheme for achieving intelligent automation.

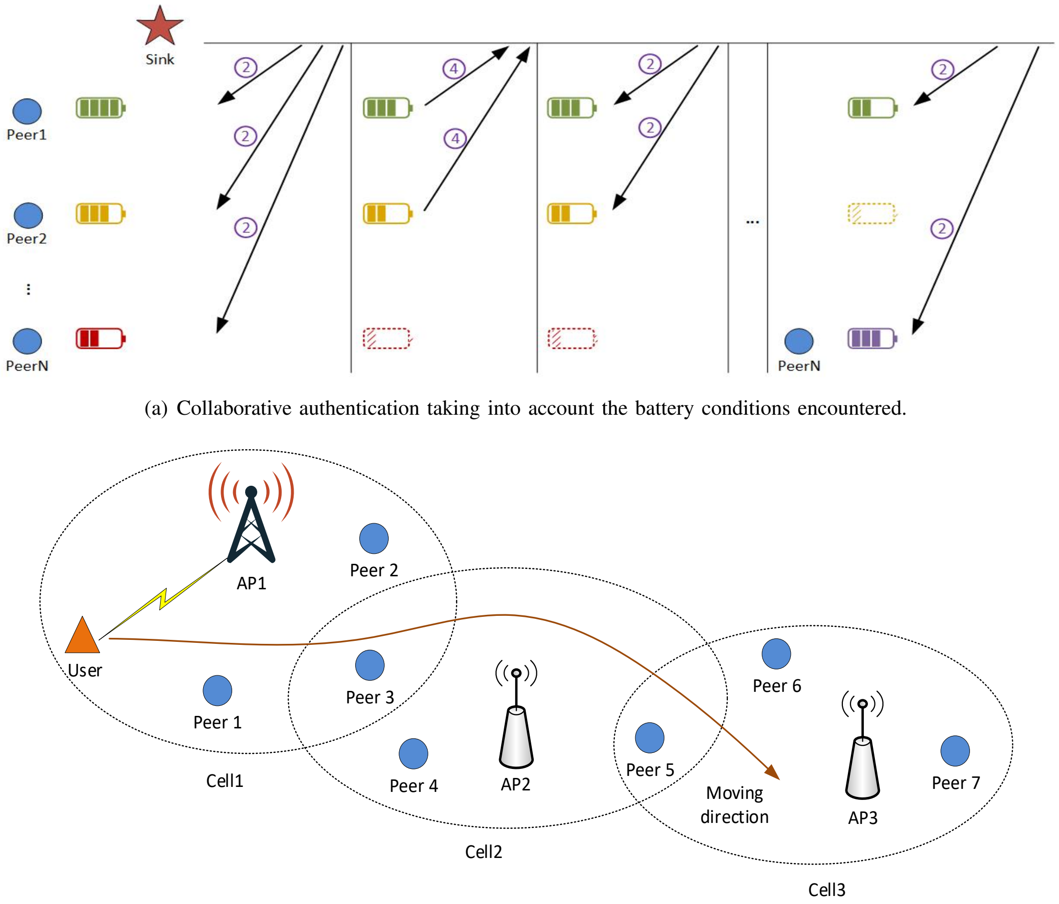
In situation-aware collaborative authentication, specific cooperative peers can be removed or added according to their particular conditions based on predesigned thresholds. Consider Figure 4 (a) as an example. If the battery charge of a peer is lower than a given threshold, it will be asked to exit from the collaboration, i.e. the service provider will not send the updated global authentication model to this device (namely Step 2 of Figure 3) and this device will not upload any updated local authentication model to the service provider (namely Step 4 of Figure 3). Consequently, its role will be replaced by a new device having much better conditions, e.g. higher battery charge. Furthermore, the time-varying features of the user, e.g. location information, network connection, and power/battery information, could be observed by densely located heterogeneous devices for meeting the stringent demands. In the situation-aware authentication process, the information can be adaptively updated by utilizing reliable features under the specific conditions of the user and cooperative peers.

As the user moves from one cell to another, the peers involved may leave the collaborative authentication due to their small coverage areas, while new devices may join. Therefore, the system's flexibility and robustness should also be considered in conceiving efficient handover authentication. Figure 4 (b) provides an autonomous handover authentication example for heterogeneous networks, where the user accesses the services via different networks, e.g. WiFi, ZigBee, and 5G/6G. The user may frequently move out of one cell and enter another one, e.g. from cell 1 to 2 and 3. The proposed situation-ware collaborative authentication will achieve prompt and reliable handover authentication based on the results gleaned from the previous cell and from smooth autonomous cooperative peer update. To be more specific, when a user moves to cell 2, the service provider may authenticate the user based on the result of cell 1 and also based on the seamless results gleaned from Peer 3. Then, the collaborative authentication will be updated and enhanced with the aid of all the three peers (i.e. Peers 3-5).

It is plausible that exploiting more features and cooperative peers is capable of improving the authentication performance, but naturally at the cost of higher computational and communications overhead imposed by aggregating the locally updated parameters [6], [14], [15]. The authors of [14] took the associated time requirement into consideration, and proposed a time-efficient asynchronous federated learning protocol. In contrast to [14], we study the trade-off between the authentication performance and communication performance in collaborative authentication. To achieve a guaranteed security level in different situations, both the security risk and the authentication latency should be evaluated. Then, both the number of features and that of cooperative peers can be adjusted based on the proposed situation-aware collaborative authentication by maximizing the communication performance under the specific security constraints.

LOCALLY COLLABORATIVE LEARNING FOR EFFICIENT AUTHENTICATION

The 6G networks are expected to provide substantially higher data rate than the 5G networks, while



(a) Collaborative authentication taking into account the battery conditions encountered.

(b) Autonomous handover authentication in the heterogeneous network considering different network connections.

Fig. 4: Situation-aware collaborative authentication.

having an end-to-end latency below 1msec. The federated learning process typically requires hundreds of rounds for their model updates. Thereby, the communication overhead between the cooperative peers and service provider should be carefully taken into account, especially when the number of cooperative peers is not small. To overcome this challenge, we develop a locally collaborative learning scheme to reduce the communication overhead for achieving efficient collaborative authentication.

As shown in Figure 3, the service provider is usually located far from both the user and from the cooperative peers, while most of the cooperative peers are much closer to the user, hence they are capable of gleaning direct observations of the user. If we rely on collaboration among the peers themselves instead of uploading their model parameters to the service provider, the communication overhead of the collaborative authentication process will be substantially reduced. As seen in Algorithm 2, both the parameter updates and the authentication information observed are stored and processed locally by the cooperative peers. Compared to uploading the model parameters to the service provider (i.e. Algorithm 1), the communication overhead of the proposed locally collaborative authentication (i.e. Algorithm 2) is dramatically reduced.

Furthermore, this paper is focused on collaborative authentication mechanisms based on situation-aware cooperation, i.e. on the cooperation of different security mechanisms, of heterogeneous security information/context, and of diverse devices and networks. When the cooperative peers achieve consensus with the service provider, the user will be authenticated as being legitimate. Otherwise, the user will be identified as an attacker. As a benefit of having multiple cooperative peers and numerous features involved in the authentication as well as owing to the intrinsic situation awareness designed, the proposed locally collaborative authentication scheme achieves unforgeability and substantial security enhancements.

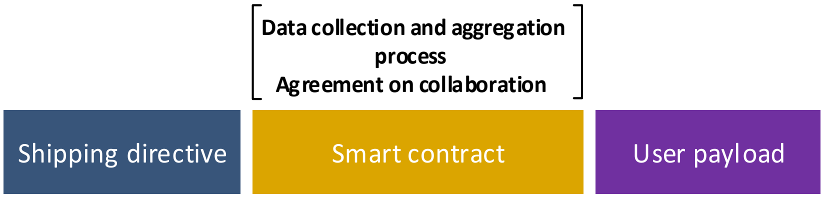

Data collection and aggregation process
Agreement on collaboration
Shipping directive
Smart contract
User payload

Fig. 5: Smart contract design in new IP evolution of 6G for accountable collaboration.

Algorithm 2 Locally collaborative authentication with privacy preservation

```
Service provider executes:
designate cooperative peers;
build authentication model based on selected feature(s);
initialize model parameters $\boldsymbol{w}_0$;
broadcast global authentication model to its cooperative peers;
for each round $t = 1, 2, ...$ do
    for each peer $n$ in parallel do
        observe authentication features and share their observations with each other;
        update parameters $\boldsymbol{w}_{n,t-1}$ with local observed features;
    end for
end for
every peer replies its authentication decision to the service provider.
```

ACCOUNTABLE COLLABORATIVE AUTHENTICATION

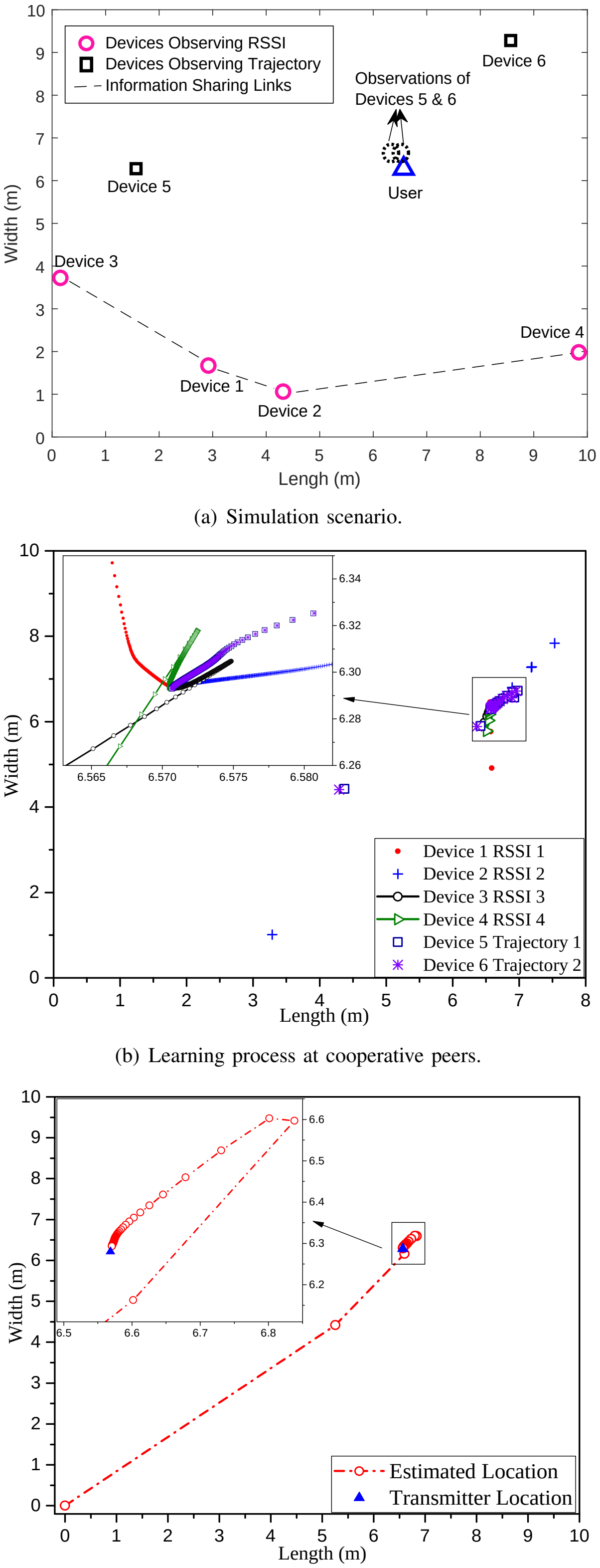
In the aforementioned collaborative authentication schemes, some of the cooperative peers could be malicious, since the 6G network is expected to have dense connections and diverse devices. If a cooperative peer is malicious, it may enter fraudulent model parameters into the learning process and thus inflict convergence failure upon the proposed learning process. Therefore, each cooperative peer should be accountable for its actions within the collaborative authentication. A smart contract can then be developed to record the data collection and aggregation processes of the cooperative peers, where a bespoke detection algorithm may be conceived for identifying rogue peers.

The operational Internet Protocol (IP) was designed as an emulation of postal letters and has a header (envelope) and a user payload (sheet of text or contents) [13]. The 6G concept has extended traditional postal services by attaching "a contract" to the courier package. The new IP will extend the existing IP in a similar way by attaching a "contract" (as shown in Figure 5) to the traditional IP packet. In this article, a smart contract is designed for collaborative authentication with privacy preservation and for ensuring that the agreement will be executed, which is characterized in Figure 5. The trigger functions are contained in the smart contract for initiating the collaborative authentication process as well as for securing group updates and agreement on collaboration. Moreover, the model parameters of the learning process and authentication decisions of every peer are recorded in the smart contract, so that cooperator misconduct can be tracked. Hence, the designed smart contract guarantees accountability under autonomous collaborative authentication.

PERFORMANCE ANALYSIS AND EVALUATION

For evaluating the proposed federated learning-based collaborative authentication scheme, a simulation example is provided using MATLAB by exploiting the received signal strength indicator (RSSI) and movement trajectory for authentication. In the simulation, 6 devices are placed randomly in an indoor office as cooperative peers, and the reference user to be authenticated is also located in the same office, as shown Figure 6 (a) with location [6.57m, 6.28m]. To be more specific, Devices 1-4 use the RSSI and Devices 5-6 utilize the motion trajectory measured by laser radar for authentication, respectively. The RSSI estimates are shared only between neighbouring devices. The observations of Devices 5 and 6 are given as [6.56m, 6.64m] and [6.44m, 6.62m], respectively, which indicate the imperfect observations (of Devices 5 and 6) for collaborative authentication. The service provider is located outside this office. The privacy of devices in this office, i.e. their location, motion trajectory, and wireless channel information, should be concealed from the service provider, while Devices 1-6 assist in authenticating the user.

Figure 6 (b) characterizes the convergence process of the authentication models at the cooperative peers' sides. All the estimates of Devices 1-6 converge to the real position of the user based on their local information, i.e. RSSI and motion trajectory of the user observed by Devices 1-6. More importantly, Figure 6 (c) shows the convergence process of the global authentication model at the service provider's side.



(a) Simulation scenario.

(b) Learning process at cooperative peers.

(c) Global learning process at service provider.

Fig. 6: The collaborative authentication process combined with privacy preservation.

Observe in this figure that the estimates of the user's position converge to its real position. If the convergence results of both the cooperative peers and service provider are close enough, the user is authenticated as the legitimate node, otherwise, deemed to be a spoofer. Note that the cooperative peers only upload the parameters of the authentication models to the service provider, thus the location privacy of Devices 1-6 is protected.

CONCLUSION AND FUTURE PERSPECTIVES

The challenges faced by non-collaborative authentication schemes and the benefits of collaborative security provision were investigated. To achieve robust, scalable, and privacy-preserving collaboration among devices, federated learning-aided authentication was proposed. An adaptive strategy was designed for updating the cooperative peers and their authentication features based on situation-awareness. Then, a distributed learning algorithm was developed for efficient collaborative authentication. Finally, a smart contract was designed for ensuring that the proposed schemes and processes will indeed be executed. Autonomous authentication was achieved by intelligently exploiting the heterogenous information gleaned from the cooperative peers in different situations.

In 6G networks, there are also many other research directions for achieving collaborative security provision, where distributed learning improves the quality of service. We summarize a range of future research ideas on intelligent security services as follows.

Federated learning methods play a critical role in supporting privacy-sensitive applications where distributed training data may be collected from the network's edge. This has the potential of supporting predictive features on smart phones without diminishing the user experience or leaking private information. It may also be utilized for other 6G applications, such as cloud/fog computing. One of the challenges of federated learning is how to handle a massive number of devices. Moreover, due to the heterogeneity of 6G systems, federated learning algorithms must be compatible with heterogeneous hardware and should be capable of dropping devices during the communication process. Given that federated learning may suffer from the backdoor attacks and inference attacks, more secure learning techniques will be conceived in our future research.

The blockchain technique may be utilized for distributed collaborative security provision, which relies on a growing list of blocks that record data based on distributed consensus mechanisms. Due to its advantages, including its decentralized nature, traceability, and robustness to data tampering, blockchain constitutes a promising framework for distributed security provision. Collaborative intrusion detection can also be achieved with the aid of blockchain, where multiple devices are capable of spotting suspicious files in a distributed way. Furthermore, trust among different devices/users can be established based on blockchain-aided techniques, where the behaviors of devices/users including their conducive and malicious acts will be stored in the blocks for efficient trust management and prediction.

In 6G systems, the efficiency of the collaboration negotiation process is one of the open issues, especially in delay-sensitive communications. The negotiation processes usually require multiple rounds of communications for reaching an agreement. When the number of devices is higher, the efficiency of negotiation process is much reduced since it needs more rounds of communications among the devices. Hence, how to efficiently arrive at an agreement of the negotiation process in collaborative security provision is one of our future targets.

REFERENCES

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, 2019.

[2] Z. Xiao, H. Fang, and X. Wang, "Distributed nonlinear polynomial graph filter and its output graph spectrum: Filter analysis and design," *IEEE Trans. Signal Process.*, doi: 10.1109/TSP.2021.3054523, 2021.

[3] E. Yaacoub and M.-S. Alouini, "A key 6G challenge and opportunity-connecting the base of the pyramid: A survey on rural connectivity," *Proc. IEEE*, vol. 108, no. 4, pp. 533-582, 2020.

[4] 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.

[5] 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.

[6] 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.

[7] Z. Gu, H. Chen, P. Xu, Y. Li, and B. Vucetic, "Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3722-3733, 2020.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy , M. Daneshmand, and A. H. Gandomi, "Authentication and key management in distributed IoT using Blockchain technology," *IEEE Internet of Things J.*, vol. 8, no. 16, pp. 12947-12954, 2021.

[13] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, “Federated learning for Internet of Things: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, doi: 10.1109/COMST.2021.3075439, 2021.

[14] C. Zhou, H. Tian, H. Zhang, J. Zhang, M. Dong, and J. Jia, “TEA-fed: Time-efficient asynchronous federated learning for edge computing,” *18th ACM International Conference on Computing Frontiers (CF 2021)*, Catania, Italy, May 11-13, 2021.

[15] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, “A joint learning and communications framework for federated learning over wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 269-283, 2021.

BIOGRAPHIES

HE FANG [S’17, M’21] (fanghe@suda.edu.cn) is a professor with the School of Electronic and Information Engineering, Soochow University, China. She received her Ph.D. degree in Electrical and Computer Engineering, Western University, Canada. Her research interests include intelligent security provision, trust management, machine learning, distributed optimization and collaboration techniques.

XIANBIN WANG [S’98, M’99, SM’06, F’17] (xianbin.wang@uwo.ca) is a professor and Tier 1 Canada Research Chair in 5G and Wireless IoT Communications at Western University. He has over 500 publications, in addition to 30 patents. He is a Fellow of IEEE, CAE and EIC. He has served as Editor-in-Chief/Associate Editor/Guest Editor for more than 10 journals. He was the Chair of the ComSoc SPCC Technical Committee and is serving as the Chair of IEEE London Section.

ZHENLONG XIAO [S’14, M’17] (zlxiao@xmu.edu.cn) is an Associate Professor with the Department of Informatics and Communication Engineering, School of Informatics, Xiamen University, Xiamen, China. His research interests focus on nonlinear signal processing, graph signal processing, and collaborative signal processing.

LAJOS HANZO [F’04] (lh@ecs.soton.ac.uk) (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) is a Fellow of the Royal Academy of Engineering, FIEEE, FIET, Fellow of EURASIP and a Foreign Member of the Hungarian Academy of Sciences. He coauthored 2000+ contributions at IEEE Xplore and 19 Wiley-IEEE Press monographs. He was bestowed upon the Eric Sumner Field Award.