A Survey on Cross-Layer Authentication in Wireless Communication Networks

Xin Liu[1], Jianing Wang[1], Shichang Guo[1], and Haiyang Wang[1]
[1]School of Computer Science and Technology, Xidian University, Xi'an, 710126, China

In current wireless networks, Physical Layer Authentication (PLA) and cryptography-based authentication have been recognized as the two dominant methods that can be trusted for user authentication and device identification. PLA methods are intensively studied in the field of network security as a strong complement to upper layer authentication. However, using only two existing authentication mechanisms cannot meet the security requirements and service demands of future wireless network development. Cross-layer authentication was created in response to the future explosion of Internet of Things (IoT) devices for secure authentication and broader service requirements. This paper presents a survey on current research status of cross-layer authentication schemes in wireless networks. We divide current cross-layer authentication approaches into two categories: cross-layer device authentication and cross-layer user-device authentication, introduce the state-of-the-art works in each category and finally discuss the challenges and future research directions.

***Index Terms*—Cross-layer authentication, physical layer authentication, cryptography-based authentication.**

I. Introduction

WIRELESS communication networks are growing at a rapid pace over the past few decades. The types of devices and services being accessed are growing at an explosive rate. With the development of computer industry, the deepening of network globalization and the increasing popularity of smart devices, wireless communication networks, which refers to a new technology formed by the organic combination of wireless communication and Internet of Things (IoT) technology, have become the world's fastest-growing industry with the largest market potential and the most attractive prospects [1]. As of summer of 2020, and according to recent research (as of 2021) there are around 8 billion mobile subscriptions in the world, with 5.5 billion being smartphone subscriptions [2]. These numbers are expected to soar in upcoming years as technologies such as 5G/6G networks and more IoT devices are deployed around the world [3]. In the past, we have seen applications of wireless communication networks in areas such as environmental monitoring, transportation, entertainment, security, and healthcare [4]. Meanwhile, advances in communications and networking technologies are rapidly making ubiquitous network connectivity a reality. Wireless networks are also essential to support this anytime, anywhere access [5].

Due to the broadcast nature of wireless networks, information can be easily eavesdropped or intercepted during propagation through the wireless medium. Malicious attackers can use these vulnerabilities to tamper with messages or impersonate the sender's identity. These vulnerabilities in wireless networks could undermine the authenticity, confidentiality, integrity, and availability if they are not carefully addressed. As wireless communication networks are widely used in military, transportation and other fields, their security and confidentiality become particularly important. In the military field, the confidentiality of information is required to be very high, and the security of transmission processes becomes very important, while in the transportation field, the leakage of information may lead to the danger of human life. The inherent physical structure and electromagnetic transmission method of wireless communication networks make the attacks against it very stealthy, and we have summarised three typical attack methods. They are brute force attacks, spoofing attacks and denial of service attack (DoS). The brute force attack is that attackers use their superior arithmetic power to brute-force decrypt a user's wireless network packets, thereby tampering with or stealing data transmitted over wireless communication networks. A spoofing attack is where an attacker masquerades as a legitimate node to spoof a user or other legitimate node, thereby hijacking its legitimate session to enable eavesdropping, data collection, or data manipulation of the attacked. DoS attacks interfere with the normal operation of the network by attacking the physical and MAC layers, making the network unable to provide services. These attacks need to be resisted by effective authentication to build a secure wireless communication environment. As hundreds of millions of smart mobile devices flood into the Internet, the security of these devices, and the privacy of their users need to be effectively safeguarded. Authentication is considered the best solution to these problems. From the point of view of the authentication object, authentication is divided into user identity authentication and device authentication. The former is based on the authenticity of the user's identity for authentication, while the latter is based on device-specific identification. From another point of view, authentication methods are categorized into cryptography-based authentication and Physical Layer Authentication (PLA).

Manuscript received January 1, 2024; revised April 18, 2024. Corresponding author: Jia'ning Wang (email:jianingwang@stu.xidian.edu.cn).

This work was supported in part by the National Key Research and Development Program of China (Grant No. 2022YFB2902202), the Shaanxi Province Key R&D Program (Grant No. 2024GX-YBXM-073), the National Natural Science Foundation of China (Grant No. 62202354, 62202355) and Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi (Grant No. QCYRCXM-2022-144).

A. Cryptography-based Authentication

Cryptography-based authentication methods have made great progress so far. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [6]. Cryptographic goals are confidentiality, authentication, data integrity and non-repudiation. Cryptographic techniques are typically divided into two generic types: symmetric and asymmetric encryption. Literature [7] lists the cryptographic primitives considered and the relationships between them.

B. Physical Layer Authentication

At the same time, there has been a proliferation of studies on PLA. It utilizes the randomness of wireless channels and/or unique hardware features to achieve confidentiality and security authentication of devices [8]. PLA can be divided into passive and active schemes [9]. The basic concept of the passive scheme is that the receiver achieves authentication of the transmitter based on the physical layer characteristics of the received signal. And the basic concept of active authentication is that the sender generates a tag based on a key and embeds it in the source message, and the receiver authenticates the sender by checking for the presence of the tag in the incoming signal. Passive schemes are mainly divided into device-based authentication [10], [11], [12], and channel-based authentication. Device-based authentication is also known as Radio-frequency Fingerprinting (RFF), which achieves device identification based on the inherent Radio-frequency (RF) features caused by hardware defects [10], [11], [12]. The uniqueness and ubiquity of these hardware defects caused by the manufacturing process and the fact that they are difficult to fake or tamper with paves the way for identification using this technique. RF features, although small and do not affect normal communication functions, can serve as unique device identifiers [13], [14]. RFF features mainly include transient features such as transient amplitude, transient power spectral density, and phase noise, as well as steady-state features such as Carrier Frequency Offset (CFO), power amplifier defects, clock offset, I/Q imbalance, and physically unclonable functions, etc. Compared to transient features, steady-state features benefit from the fact that they are less difficult to extract.

Channel-based PLA is based on the principle that the receiver can estimate the channel vectors from the received frames of the sender, and identify and authenticate the legitimacy of the sender by means of hypothesis-testing. Channel-based features reflect channel information between legitimate transmitters and receivers, such as Received Signal Strength (RSS)[5] and Channel State Information (CSI) [15]. Using the reciprocity of the wireless channel transmission process, the channel features observed by a transmission pair are highly correlated. Such features can be used to generate a pair of symmetric keys, so it can also be called the channel key method. The key of PLA is to recognize the identities of wireless terminals on physical layer as soon as possible [16].

Although traditional cryptography techniques can prevent identity-based attacks in wireless networks, current network environments are rich and diverse, and in some scenarios cryptography-based authentication methods can appear inefficient or insufficiently secure [5], e.g., IoT, Internet of Vehicles (IoV), Smart Grids (SG) networks, Unmanned Aerial Vehicles (UAVs), and Wireless Sensor Networks (WSNs). For some small devices in IoT, such as devices with low power consumption, low storage, and low processing capability in IIoT, they cannot satisfy the processing data capability required for cryptographic authentication, nor can they satisfy the storage capability of ultra-long passwords, so cryptographic authentication methods cannot be applied in the authentication of these devices. Cryptographic authentication relies heavily on its complex calculations, making it impossible for attackers to decipher their private keys, and with the development of quantum computing [17], this advantage is likely to become smaller and smaller in the future, putting the security of devices and users connected to the network at risk. Overall, for the current diversity of authentication scenarios, authentication based on traditional cryptography is increasingly recognized by research as having huge overhead, computationally intensive, inefficient and time-consuming and even security is low [18], [19], [20], [21].

Most of the existing PLA mechanisms are designed for static communication, and their accuracy decreases significantly in dynamic scenarios where the network environment and wireless channel change frequently [22]. For example, the channel key method just mentioned above, which utilizes the randomness of the channel, making it possible to generate a sufficient number of randomly distributed keys per unit of time, thus making it very difficult for an attacker to predict the corresponding key. However, in the process of wireless communication, the movement of terminals or people and objects in the surrounding environment may cause changes in reflection, refraction, and scattering paths of the wireless channel, which will cause the channel to change over time, and these movements are unpredictable or difficult to predict, so that channel changes are random, which will bring a great deal of impact to the security and feasibility of the PLA. For some high-speed mobile devices, such as drones, automobiles, etc., in the process of extracting RF fingerprint features, the environment will have a great impact on the feature extraction, factors such as temperature, humidity, and obstructions can affect the quality and stability of the signal. This makes it very difficult to extract the complete signal and impossible to extract device features from such an incomplete and unstable signal as an authenticated RF fingerprint, so in the authentication of high-speed mobile devices, PLA appears to be incompetent. Although PLA has been widely recognized as the most powerful complement to cryptographic authentication owing to its advantages of lighter weight, low computational volume, low overhead, its security compared to cryptographic methods still have shortcomings, especially in the authentication of mobile devices.

As 5G technology continues to evolve, the future is more dedicated to the interconnection of everything in network scenarios such as Industry 4.0, SG, VANETs, UVAs, and

WSNs, which are increasingly demanding in terms of cybersecurity. Traditional cryptographic authentication or PLA methods alone cannot meet the security requirements of large-scale access, fast-moving devices, and diverse service demands in complex network environments. In scenarios with large-scale access, the overall computation and storage resource required for cryptographic authentication will be a huge burden for a central authentication entity, especially those with constrained resources, for example, a roadside unit in charge of the network access of a large number of vehicles. Thus, traditional cryptographic authentication alone cannot meet the security requirements in such scenarios. In high-speed mobile scenarios, the long latency of cryptographic methods cannot meet the high-precision and lightweight requirements of authentication, while physical layer methods are difficult to extract the required hardware features, and the channel environment is even worse, makes it difficult to extract a complete and stable signal, resulting in the inability to authenticate or the error of authentication is too large to meet the requirements. Neither of the traditional authentication methods alone can satisfy either of these scenarios, so combining their strengths may be a solution. More and more scholars have noticed this problem, and began to seek for cross-layer security authentication that is more lightweight, satisfies diverse services, and has higher security level. As early as 2007, Tin-Yu Wu et al. [23] proposed user authentication, key generation, and data encryption in heterogeneous networks for higher multimedia loads and faster transmission rates in the fourth-generation mobile communication systems, utilizing the design of security protocols across different network layers to achieve enhanced cryptography-based cross-layer security authentication, which is the first understanding of cross-layer authentication.

Subsequently in 2009, Wei Wang et al. [24] pointed out for the first time that traditional encryption and authentication techniques cannot be directly applied to WSNs, and their results provide a quality-driven security design and resource allocation framework for WSNs, which fills the interdisciplinary research gap between high-level multimedia signal processing and low-layer computer networks, and such a cross-layer framework realizes objective energy-efficiency, quality, and security gains by jointly involving multimedia-selective encryption at the application layer, stream authentication, and resource allocation at the low layer.

To facilitate the subsequent research on cross-layer authentication, this paper aims to provide a survey on the state-of-the-art cross-layer authentication approaches in wireless networks. Surveys on PLA and cryptographic authentication alone have been provided in [25] and [26], while there has not been a systematic survey on cross-layer authentication. To the best of our knowledge, this is the first to fill the gap. For the first time, we categorize cross-layer authentication into cross-layer device authentication and cross-layer user-device authentication from the perspective of the research object, and we separate these two authentication methods into separate presentations from the perspective of authentication scenarios. For cross-layer device authentication, we introduce the related work from two scenarios: industrial IoT and SG, and for cross-layer user-device authentication, we further introduce the work from three aspects: VANETs, UAVs and WSNs. Our work makes a systematic categorization of cross-layer authentication for different scenarios on the advantages of cross-layer authentication over the use of PLA and cryptographic authentication alone, which is expected to inspire more research in the field of cross-layer authentication.

The remainder of this paper is organized as follows. In Section II, we provide an overview of cross-layer authentication schemes targeting devices for two authentication scenarios: industrial IoT and SG. In Section III, we provide an overview of cross-layer authentication schemes for user-devices with respect to three authentication scenarios, namely, VANETs, UAVs, and WSNs. In Section IV, we present the challenges and future research directions for cross-layer authentication, including fast and seamless switching authentication and future ultra-long-range user authentication. Finally, Section V concludes the paper.

C. Research Methodology

Before starting the research, we identified several keywords as cross-layer authentication, converged authentication, cryptographic authentication, physical layer authentication, RF fingerprinting, etc., and searched for the above keywords on Google Scholar, IEEE Internet of Things Journal, IEEE Wireless Communications, and so on. After sifting through more than a hundred relevant literatures, I skimmed the overviews and introductions of the literatures, and then sifted through them again, selecting the ones that were highly relevant to my needs of cross-layer authentication, cryptographic authentication, and PLA.

After screening the articles we have to take the next step of categorization, we have classified cross-layer authentication into two broad categories, cross-layer device authentication and cross-layer users-device authentication, this is for the classification of authentication objects, which can be accomplished through the accuracy literature. After this categorization, we further categorized these two parts of the literature for authentication environments to arrive at the classification of this paper, which categorizes cross-layer device authentication into two categories, IIoT and SG, and categorizes cross-layer users-device authentication into three scenarios, namely VAENTs, UAVs, and WSNs. This was followed by a breakdown of the literature, which also included a number of review articles, articles on cryptographic authentication and PLA, all of which were managed in separate categories for my ease of reading. These are the activities I have undertaken and my research and categorization methods in completing this review.

II. Cross-Layer Device Authentication

The aim of cross-layer device authentication is to verify the authenticity of devices by combining cryptographic approaches and PLA approaches, where the former checks the digital certificates of the devices and the latter checks the devices' RFF features. This section describes the cross-layer authentication of devices for machine-like communication in the following two scenarios.

A. Cross-Layer Device Authentication in the Industrial Internet

The Industrial Internet of Things (IIoT) technology is a key enabler for the next industrial revolution, know as Industry 4.0 [27], [28]. The excesses from the third industrial revolution to Industry 4.0 have raised a new set of security issues [29], [30], [31]. Traditional industrial communication systems, designed to operate reliably in noisy factory environments, primarily use hard-wired proprietary communication technologies to connect sensors, actuators and controllers, as well as other industrial components, such as supervisory and data acquisition systems and manufacturing execution systems. With the advent of IIoT, however, the factory of the future will increasingly rely on a variety of communication technologies, including wireless standards, to ensure connectivity, interoperability, and remote operation and control of production processes over the Internet [32].

Authors in the literature [33], [34], [35] present security challenges in Industry 4.0 and point out that IIoT practices increase security and privacy risks. Device authentication and privacy protection in the IIoT are key issues for a secure Industry 4.0, and failures in these areas will facilitate attackers to wreak havoc with IIoT applications in a multitude of environments [36]. The IIoT is often different from the IoT in that the former requires higher levels of security and privacy [37]. IIoT is a very resource-constrained communication network that contains a large number of lightweight devices, so it is important to design lightweight authentication mechanisms with high security, high privacy, and low overhead in terms of computation time and transmission size [34].

The authors in Literature [38] summarize some of the main typical challenges faced in wireless industrial communications, including the openness of the wireless broadcast channel, large-scale network access, and the large interaction overhead on the physical layer. Scarce memory resources limit the use of resource-demanding cryptographic primitives, which makes traditional upper-layer protection mechanisms insufficient to secure such IoT systems, such as lightweight encryption [39] and privacy guarantees [40]. Another representative approach [41], [42] is the channel-based PLA method, however, research has shown that this method is not very sensitive to real communication scenarios due to the randomness of the wireless channel and other hardware-level errors in the intrinsic characteristics [43]. In order to compensate for the authentication defects of upper-layer authentication and PLA in this scenario, some scholars have begun to study the cross-layer authentication scheme combining PLA and cryptographic authentication techniques. Dan Shan et al. proposed a novel Physical Layer Challenge Response Authentication Mechanism (PHY-CRAM) for wireless communication networks, where unencrypted shared keys are exchanged between the two communicating parties, which are masked by random numbers and channel fading, preventing the leakage of CSI, and thus realizing the secure transmission of information [44]. Hoorin Park et al. proposed a lightweight authentication mechanism, Tagora, in Literature [45]. Unlike traditional authentication protocols that consider collisions as interference, Tagora utilizes unpredictable conflicts for authentication at both the physical and application layers, and the authentication consists of a collision-recovery algorithm with a randomized offset scheme and phase encryption at the physical layer, and an authentication process based on the challenge-response mechanism at the application layer, and experiments have demonstrated the ability of their method to effectively deal with traceability problems and replay attacks. An EPS-AKA protocol for applying PLA to large-scale IoT systems is proposed in Literature [46], which uses a distributed authentication architecture to reduce the overhead and delay associated with the authentication of massive IoT devices.

B. Cross-Layer Device Authentication in SG

A SG is a fully automated power transmission network that monitors and controls each user and grid node, ensuring a two-way flow of information and power between all nodes throughout the transmission and distribution process from the power plant to the end user. SG is typically Machine-to-Machine (M2M) communications. M2M is a type of application and service based on intelligent interaction and networking between machine terminals, which has also been made Machine-type Communications (MTC) in the Third Generation Partnership Project (3GPP) [47]. MTC is defined as M2M with no human intervention at all, and this type of technology is considered a key enabler for the next generation of the emerging networked society [48]. As mentioned above, SG is a typical MTC, and the components of SG include a large number of automation devices, and the integration of these devices makes M2M communication form a large-scale heterogeneous network, and the authentication of a large number of M2M nodes becomes a challenging new problem [49].

SG security includes the protection of the communication network and the power grid, which are systems that ensure that the SG can properly verify the authentication, integrity and confidentiality of the system before providing services. To cope with attacks in the SG, including interruption, interception, modification, and forgery, determining that messages are coming from legitimate entities, authentication must be taken to counter these attacks that may be present. The traditional digital signature-based approach is computationally intensive and impractical for resource-limited smart meters, while the use of PLA at the expense of security levels cannot meet the security requirements of SG systems. The authors in Literature [49] proposed a two-tier based M2M authentication framework for SG with global authentication through PKI and local authentication through channel signatures, using digital and channel signatures to combine the advantages of the two different authentication schemes. Exploiting the unpredictability of the signature channel for local layer channel signatures, this scheme is suitable for smart meters with limited resources. In literature [50], the authors have calculated the trust assessment by simple mathematical calculations considering the wireless device characteristics and limitations. The proposed work provides routing decisions using cross-layer parameters of physical, Medium Access Control (MAC) and network layers, which improves the reliability of SG communication systems.

The above two scenarios, are completely without human intervention, there is no user involved in the pure device cross-layer authentication, and one of the characteristics of this authentication is that all the devices involved in the authentication process are assumed to be static and fixed in position, and once a randomly moving user joins the environment, and its behavior is difficult to predict. In Table I, we make a simple comparison of the cross-layer authentication methods in these two scenarios. But in many scenarios, it is not completely static, this assumption is difficult to meet, so these cross-layer device authentication can not meet the real-life authentication scenarios, then a new cross-layer authentication method based on the user's device should be born.

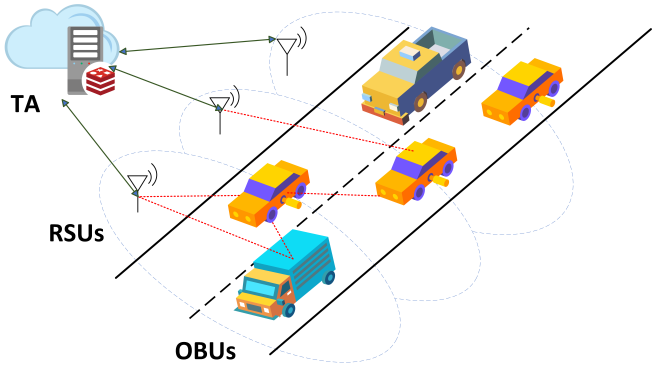

Fig. 1. Vehicle communications architecture.

III. Cross-Layer Users-Device Authentication

In order to cope with the above challenges, some scholars have begun to study systems that bind devices and users one by one, such as large-scale vehicular communication, mobile self-organizing networks and wireless sensor networks, etc. These authentication scenarios join the user's authentication and require higher requirements for smooth and seamless communication, which requires higher security level and lighter cross-layer authentication to meet the demand. We refer to this type of authentication mechanism as cross-layer users-device authentication, and this subsection will categorize the authentication mechanism from three representative scenarios, namely, large-scale vehicular communication, drone networks, and wireless sensor networks.

A. Cross-Layer Users-Device Authentication in VANETs

A VANET has human-vehicle connectivity, which can connect vehicles to a network through wireless communication technology, and then effectively utilize all vehicle dynamic information on the network information platform to provide different functional services for vehicles in operation. The main application scenarios are divided into driver assistance, automatic driving and intelligent transportation system. VANET, a subset of Mobile Ad hoc NETworks (MANETs), refer to a set of smart vehicles used on the road. These vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies [51]. Since VANETs messages are distributed in exposed environments, the security of VANETs is necessary to protect road safety, vehicle security, and driver privacy protection.

VANETs provide communication between vehicles and roadside devices as well as vehicles communicate with each other [52], [53], in this network scenario vehicles are communication nodes and they belong to the same self-organizing network, so there is no need to know about each other's existence beforehand [54]. As shown in Fig. 1, the system contains three types of nodes: On-Board Units (OBUs), Trusted Authority (TA) and Road Side Units (RSUs). OBUs are unlimited electrical devices mounted on mobile vehicles, while RSUs are placed along the road to form the network infrastructure. RSUs act as routers between vehicles. Using Dedicated Short Range Communication (DSRC) radios, OBUs can connect vehicles to RSUs [55]. The trusted authority is connected with RSUs using a wired channel. It acts as an administrator and manages the entire network. Also, TA is responsible for generating, broadcasting, and periodically updating the system parameters in the network. Moreover, it authenticates vehicles and removes them if they are involved in malicious activity or transmitting fraud messages. Hence, TA is having huge storage capacity and high computation power as compared to OBUs and RSUs [56]. VANETs face a number of attacks [57], [58], [59], [60]. Authentication is very important to maintain the security of VANETs, and authentication is required to be fast and smooth, but also need to be able to meet the needs of mass access, high-speed mobility.

We analogize the OBUs module on the vehicle to the ID card in a cell phone, and consider this type of authentication object as a device bound to the user one by one, and for this type of authentication we call it cross-layer user-device authentication. A large number of scholars have started research on cross-layer authentication on VANETs. Subir Biswas et al. proposed an improved Elliptic Curve Digital Signature Algorithm (ECDSA) combined with identity-based signatures for vehicle message authentication and a funny prioritization verification strategy for periodic road safety messages in 2013 [61]. They treat the vehicle's current location information as the vehicle ID, which is used as the corresponding identity parameter for anonymous signature generation and verification.In the same year Jia-Lun Tsai proposed in the literature [62] that Biswas et al.'s scheme is vulnerable to private key disclosure attacks, where any malicious receiving vehicle that receives a valid signature from a legitimate signing vehicle can obtain the signing vehicle's private key from the learned valid signature, and they proposed an improved authentication scheme that overcomes this weakness. The scheme is based on ECDSA and supports authentication and non-repudiation, and it is also shown that the scheme can support identity revocation and tracking, which greatly saves authentication overhead.

Khaled Rabieh et al. point out that RSUs need access to the number of vehicles in the vicinity [63], and an attacker may masquerade as more than one vehicle traveling at the same time to launch a Sybil attack, and if the RSUs is unable to identify a Sybil vehicle, this can lead to a series of security problems such as traffic paralysis as the RSUs reports the

TABLE I
ANALYSIS OF CROSS-LAYER AUTHENTICATION ADVANTAGES AND DISADVANTAGES IN IIOT AND SG SCENARIOS.

Authors	Advantages	Disadvantages	Security	Overhead
Dan Shan et al.[44]	Immune to many types of active and passive attacks.	Efficiency is greatly reduced in long distance communication.	high	middle
Park et al.[45]	Effective response to traceability issues and replay attacks.	Side-channel attacks have a high impact on the programme.	very high	high
Lee et al.[46]	Reduces the overhead and latency of mass authentication.	Authentication security is not guaranteed.	middle	very low
Chin et al.[49]	Combines both digital and channel signature schemes.	More affected by the channel environment.	middle	very low
Velusamy et al.[50]	Consider the limitations of wireless devices.	Not yet implemented in a dynamic environment.	very high	low

wrong number of vehicles to the traffic management center. They proposed a cross-layer authentication to cope with this problem by composing a challenge packet at the MAC layer and directing the PHY layer to send it to a specific location, utilizing hash functions and public key cryptography to secure the challenge-response packet. Mahmound A. Shawky et al. [64] used upper layer authentication to determine the legitimacy of the corresponding terminal in the first time slot, and re-authenticated the corresponding terminal in conjunction with the short-term reciprocal nature of the wireless channel, reducing the overall complexity and computational and communication overhead.

B. Cross-Layer Users-Device Authentication in UAVs

UAVs, commonly known as drones or unmanned aircraft, are unmanned aircraft that are operated using radio remote control equipment and self-contained programmed controls, or are operated autonomously, either fully or intermittently, by on-board computers. UAVs have become ubiquitous in recent years in both the civilian and military sectors thanks to their operational flexibility and high mobility, as well as their ability to avoid the risk of personal injury. And missions are usually carried out with multiple drones forming a drone swarm [65]. The UAVs fleet has the characteristics of high dynamic and high speed, the activities of the whole fleet are led by the cluster head (CH), in the face of different tasks, there may be the case of switching the CH, which will have the risk of the attacker to become the new CH, which will lead to the leakage of the sensitive information to the whole fleet, and the harm brought about by it is difficult to bear. One of the traditional authentication techniques for drone swarms has been cryptography, such as the Advanced Encryption Standard (AES) [66], however, with the rapid development of computing power, the potential to decipher cryptographic algorithms is increasing, making it easier for attackers to impersonate legitimate drones and become the new CH [67]. Another mainstream approach is to utilize RF fingerprinting, which has been widely used in intrusion detection, access control, clone detection, and fault detection, to authenticate UAV swarms come using its unique channel-based attributes [42], [10]. However, this approach is affected by the time-varying and imperfect estimation of physical layer attributes in realistic scenarios [68], [69], and PLA is not applicable to authentication in dynamic scenarios. Some scholars have attempted to utilize cross-layer approaches to achieve more stable and lightweight authentication. In Zhang et al. [22] the physical layer is used as a fast authentication process and the upper layer attributes are used for supervision, although this improves the stability of the authentication, it is not a cross-layer approach that fuses the physical layer and upper layer authentication. Hao et al. [70] proposed using two independent decisions, RSSI and PER, and then fusing the final decision based on multivariate decision making, but the environment where UAV swarms are located changes rapidly, and the RSSI attribute carries much less information in open-air environments than in indoor environments, so it is still not applicable to authentication in real scenarios. A novel edge-intelligence based CH security mechanism has been proposed in the literature [71] that utilizes a Linear Discriminant Analysis (LDA) algorithm to accurately fuse authentication decisions by retaining only the necessary attributes and projecting the high-dimensional estimation into a low-dimensional space for maximum separability. Situation-aware cross-layer attribute selection algorithms are developed to select the minimum number of attributes, resulting in the shortest time required for attribute estimation, thus reducing the overhead and time delay required for authentication.

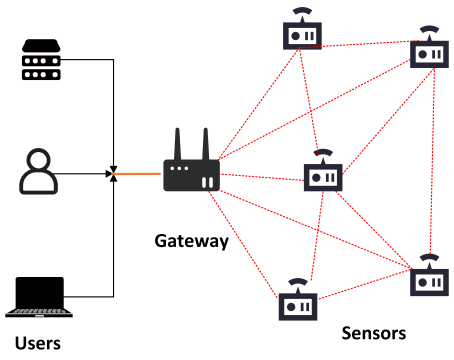

Fig. 2. Architecture of WSNs.

C. Cross-Layer Device Authentication in WSNs

A WSN is a distributed sensor network whose endpoints are sensors that can sense and inspect the external world. Sensors in a WSN communicate wirelessly, so the network setup is flexible, the location of the devices can be changed

TABLE II
ANALYSIS OF CROSS-LAYER AUTHENTICATION ADVANTAGES AND DISADVANTAGES IN VANETS, UAVS AND WSNS SCENARIOS

Authors	Advantages	Disadvantages	Security	Overhead
Rabieh et al.[63]	Detecting fake nodes without RSU support.	Requires vehicles to be equipped with directional antennas.	high	middle
Shawky et al.[64]	Significant reduction in certification time.	Performance in real wireless channels at different speeds is unknown.	high	middle
Hao et al.[70]	Better ability to detect spoofing attacks.	Not suitable for outdoor real-life applications.	high	middle
Wang et al.[71]	Reduced computational complexity.	Authentication for real scenarios has not yet been realised.	high	low
Zhang et al.[22]	High real-time performance.	Higher time consumption.	very high	high
Haenel et al.[72]	Save certification time and resources.	The level of accuracy is not comparable to purely cryptographic methods.	middle	low

at any time, and it can be connected to the Internet in a wired or wireless way. A multi-hop self-organizing network is formed through wireless communication. Consider a WSNs as shown in Fig. 2, which have three main components: sensors, gateways and users. Nodes in WSNs, often referred to as sensor nodes, have the ability to perform assembly and process sensitive data as well as communicate with other neighboring nodes [73]. WSNs have gained a lot of attention globally, and in [74] advances in WSNs technology, communications, and digital electronics have led to the development of small, multifunctional, and energy-efficient sensors to provide communication over specific ranges. WSNs have applications in a variety of fields, such as environmental monitoring, defense surveillance, and healthcare. WSNs are characterized by low power consumption for data transmission, limited battery energy, and low prices. WSNs are a typical self-organizing network consisting of randomly distributed sensor nodes with communication and data processing modules that have the ability to implement sensing, acquire information about the surrounding environment, lightweight computing, and wireless communication. The information sensed by the sensor is passed to the user through the gateway. However, public WSNs are susceptible to malicious active and passive high attacks, which pose security and privacy concerns [75]. There are many two-factor based authentication and key agrement (AKA) protocols have been proposed to address these issues.

Under the public key cryptosystem, in order to secure data and protect user's privacy, authentication is generally realized through signatures or Message Authentication Codes (MACs), while the security key is realized through the Diffie-Hellman key exchange protocol. The physical layer is identified by means of RF fingerprint authentication. Zhang et al. propose an authentication scheme that crosses the physical and upper layers in literature [22]. They first extracted physical layer features, such as received signal strength, angle of arrival, etc., and used these features to generate a normalized feature vector, which distinguishes whether the PHY features are the same as the reference features according to the preset thresholds in the hypothesis testing, and subsequently introduces a pre-existing upper layer authentication scheme at a reasonable time node to guide the adjustment of the PLA parameters.

The scheme proposed by Arie Haenel et al. [72] is similar to Zhang's authentication scheme, out of two constraints in that scenario: low cost and low power consumption. Their proposed hybrid cross-layer authentication protocol utilizes known RFF techniques and known lightweight cryptographic authentication algorithms to reduce the energy consumption of low-resource devices, using the two approaches as complements to each other. Restricted RFF authentication is used and when this method fails, a challenge response mechanism based on hash algorithm is used, and after authentication is completed whether it is successful or unsuccessful, the corresponding RFF feature is extracted and the corresponding RFF is stored against that ID.

Currently, some other scholars have proposed that a combination of biometric and cryptographic authentication can be utilized to achieve mutual authentication of users and sensors. Saru Kumari, Km. Renuka et al. proposed a user anonymous authentication scheme that relies on both biometrics and Elliptic Curve Cryptography (ECC) that has established the required security features such as forward and backward confidentiality [76]. But their scheme cannot maintain anonymity and cannot resist depersonalization attacks, replay attacks, and DoS attacks.Fan et al. proposed a biometric-based anonymous AKA scheme that meets the overlay security requirements of WSNs while proving to be secure under the three-party AKA security model [75]. In Table II, we make a brief comparison of the cross-layer authentication methods in these three scenarios.

IV. CHALLENGES AND FUTURE DIRECTIONS

Despite the current work and interest in the area of cross-layer authentication, there are still a number of issues that require further discussion. In this section, we discuss some of the problems and challenges that exist at this stage of cross-layer authentication, as well as the goals and perspectives for future research.

A. Problems at This Stage

As can be seen from the above description, many of the existing cross-layer authentication is actually the physical layer and the upper layer authentication added to the secondary authentication, there is a sequential order, more of the two complement each other rather than fully integrated into a whole authentication mechanism.

Vague definition of who is certified. In much of the literature, there is no clear indication of the type of object being authenticated, and it is not possible to distinguish whether it is authentication of a device or authentication of a user, but only a pronoun is used to refer to the object of authentication.

Although the research on cross-layer authentication has been partially successful in theory, in practice, cross-layer authentication needs more research to prove its high security, lighter weight, and low overhead, etc. This means that cross-layer authentication is still very much lacking in operability, and more research and experiments that are more in line with real-life scenarios are needed to prove its feasibility. We have listed some possible problems at this stage.

Interoperability: Interoperability requires cross-layer authentication schemes provide interchangeable services between several systems or users, thus enabling them to work together effectively. There has been no in-depth research on this aspect, and we believe that syntactic and semantic interoperability needs to be achieved first, and perhaps this will be the direction of our subsequent research.

Security: In view of the existing authentication methods, the upper layer authentication and PLA are not well combined, in the future, we may face the possibility of attackers to separate attacks on different levels, for example, the high-speed development of quantum computers may attack the upper layer authentication, resulting in the collapse of the entire authentication system, and at the same time for the physical layer of the attack is also the same. How to adequately combine the two to improve the safety of the programme is then also a question to be pondered.

Performance overhead: At this stage of the research is mainly aimed at being able to achieve cross-layer authentication, without putting the overhead on the primary solution to the problem, resulting in the existing scheme does not make a balance between security and overhead, it can only be a loss of one or the other, we believe that in the subsequent research, it will be possible to achieve a scheme with high security and low overhead.

Scalability challenge: In the rapid development of science and technology at the same time, the various aspects of the service demand for identity verification solutions is bound to become increasingly large, then how to make the existing identity verification solutions to quickly adapt to the future needs of the various aspects of the problem is also the need for in-depth thinking.

Cross-domain compatibility problem: Cross-layer authentication will definitely face the problem of different domain names, protocols or ports, as long as one of these three is different, it will prevent the user's operation, resulting in the authentication between different domains can not be carried on, which is also a follow-up research needs to be resolved.

Others: Existing cross-layer authentication application scenarios are mostly for large-scale, high-speed communication scenarios, which will inevitably lead to the high cost of its application, which is difficult to achieve for a single user's personal communication, and its civilian value is difficult to target the realisation of how to popularise the future, and how to reduce the cost of it will make a need to consider the issue.

B. Future Research Goals and Perspectives

1) Fast Switching Authentication

When the mobile terminal moves from the home domain to the target domain, it will be re-authenticated because of the switching network, and each switching will carry out a new authentication, which greatly reduces the continuity of the network service, while the wireless network bandwidth is restricted, the acceptance of the environment is complex, the error rate is high, and the mobile terminal computation and resource storage, power supply constraints. If the switching delay time is too long, it may lead to a series of problems such as information leakage, connection interruption, etc., which affects the network service and even generates a threat to the security of the network system. Key exchange-based authentication methods are limited by their complex computation process, which cannot achieve seamless switching, and the time delay will still be large. Then there is a need for a lighter weight, low computational complexity and adaptable to the resources of the first mobile terminal authentication algorithm, the purpose is to confirm whether the mobile terminal intends to access the network can securely access and use the network resources, and to realize the mobile terminal and the network to carry out a secure session in the unreliable wireless communication environment.

In the field of satellite authentication, due to the high degree of exposure of the airspace network, high-speed movement of the network nodes, limited computing resources and intermittent link connectivity, the dynamic transformation of the airspace network topology, the difficulty of accessing the base station to provide continuous service, and the frequent switching of the access terminals, which will lead to repetitive security access authentication, resulting in discontinuity or even interruption of the security service. Then how to switch securely and freely without repeated authentication, thus realizing the trusted maintenance of nodes is the focus of future research.

The cross-layer authentication can combine the characteristics of physical layer continuity authentication and high security level of upper layer authentication, which may be a breakthrough point to solve the seamless switching authentication.

2) Clarification of Authentication Targets

As we all know, the upper layer authentication is for the authentication of the authenticated user's identity, while the PLA is for the authentication of the authenticated user's device, the current cross-layer authentication does not have a separate study of the user's identity, so how to find a unified standard in the two authentication methods to achieve cross-layer authentication for the authentication of a user's identity, which is likely to be a very critical point for the future of the user's identity authentication of the ultra-long-distance range, but this is still an unexplored issue, which is expected to become a key direction of the research in the future.

V. CONCLUSION

This paper provides a comprehensive overview of cross-layer authentication schemes, describing existing cross-layer authentication in terms of cross-layer device authentication and cross-layer user-device authentication, respectively. We present cross-layer authentication schemes from five scenarios: Industrial Internet, SG, VANETs, UAVs networks and WSNs.

Finally, we present some problems and future directions of cross-layer authentication at this stage.

REFERENCES

[1] Z. Lv and H. Song, "Mobile internet of things under data physical fusion technology," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4616–4624, 2019.

[2] Perez, Alfredo J and Zeadally, Sherali, "Recent advances in wearable sensing technologies," *Sensors*, vol. 21, no. 20, p. 6828, 2021.

[3] A. J. Perez and S. Zeadally, "Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions," *Computer Science Review*, vol. 43, p. 100450, 2022.

[4] Perez, Alfredo J and Zeadally, Sherali, "Design and evaluation of a privacy architecture for crowdsensing applications," *ACM SIGAPP Applied Computing Review*, vol. 18, no. 1, pp. 7–18, 2018.

[5] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[6] D. May, H. L. Muller, and N. P. Smart, "Random register renaming to foil dpa," in *Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*. Springer, 2001, pp. 28–38.

[7] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[8] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[9] R. Dastres, M. Soori, and M. Asamel, "Radio frequency identification (rfid) based wireless manufacturing systems, a review," *Independent Journal of Management & Production*, vol. 13, no. 1, pp. 258–290, 2022.

[10] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1–29, 2012.

[11] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222–233, 2020.

[12] G. Shen, J. Zhang, A. Marshall, M. Valkama, and J. Cavallaro, "Towards length-versatile and noise-robust radio frequency fingerprint identification," *IEEE Transactions on Information Forensics and Security*, 2023.

[13] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for lora," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 774–787, 2022.

[14] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3974–3987, 2021.

[15] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[16] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[17] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, 2017.

[18] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.

[19] D. J. Bernstein, "Cryptographic competitions," *Cryptology ePrint Archive*, 2020.

[20] B. Schneier, "Risks of relying on cryptography," *Communications of the ACM*, vol. 42, no. 10, pp. 144–144, 1999.

[21] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, "Improving software quality in cryptography standardization projects," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2022, pp. 19–30.

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

[23] T.-Y. Wu, D. Chung, C.-Y. Chen, and H.-C. Chao, "Pave the way to future smart living space-cross-layer enhanced aaa for 4g core network," in *2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*. IEEE, 2007, pp. 325–330.

[24] W. Wang, "Quality-driven cross layer design for multimedia security over resource constrained wireless sensor networks," 2009.

[25] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2020.

[26] J. Clark and J. Jacob, "A survey of authentication protocol literature," 1997.

[27] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive internet of things for industrial applications: Addressing wireless iiot connectivity challenges and ecosystem fragmentation," *IEEE industrial electronics magazine*, vol. 11, no. 1, pp. 28–33, 2017.

[28] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[29] M. Waidner and M. Kasper, "Security in industrie 4.0-challenges and solutions for the fourth industrial revolution," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2016, pp. 1303–1308.

[30] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 6–16, 2017.

[31] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.

[32] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, "A lightweight authentication mechanism for m2m communications in industrial iot environment," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288–296, 2017.

[33] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, 2017.

[34] T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within industry 4.0 paradigm," *Procedia manufacturing*, vol. 13, pp. 1253–1260, 2017.

[35] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and F. A. Khan, "Securing critical infrastructures: deep-learning-based threat detection in iiot," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 76–82, 2021.

[36] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE transactions on industrial informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[37] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[38] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[39] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[40] J. Zhang and M. Wu, "Blockchain use in iot for privacy-preserving anti-pandemic home quarantine," *Electronics*, vol. 9, no. 10, p. 1746, 2020.

[41] Z. Gu, H. Chen, P. Xu, Y. Li, and B. Vucetic, "Physical layer authentication for non-coherent massive simo-enabled industrial iot communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3722–3733, 2020.

[42] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, and H. Zhang, "Physical-layer authentication for internet of things via wfrft-based gaussian tag embedding," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9001–9010, 2020.

[43] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE transactions on information forensics and security*, vol. 11, no. 9, pp. 2091–2106, 2016.

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

[45] H. Park, H. Roh, and W. Lee, "Tagora: A collision-exploitative rfid authentication protocol based on cross-layer approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3571–3585, 2020.

[46] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A novel cross-layer authentication protocol for the internet of things," *IEEE Access*, vol. 8, pp. 196 135–196 150, 2020.

[47] G. T. . V. 0.0, "System improvements for machine-type communications," 2012.

[48] C. Zhao, L. Huang, Y. Zhao, and X. Du, "Secure machine-type communications toward lte heterogeneous networks," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 82–87, 2017.

[49] W.-L. Chin, Y.-H. Lin, and H.-H. Chen, "A framework of machine-to-machine authentication in smart grid: a two-layer approach," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 102–107, 2016.

[50] D. Velusamy, G. Pugalendhi, and K. Ramasamy, "A cross-layer trust evaluation protocol for secured routing in communication network of smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 193–204, 2019.

[51] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[52] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[53] Y. Wang and F. Li, "Vehicular ad hoc networks," *Guide to wireless ad hoc networks*, pp. 503–525, 2009.

[54] V. Yadav, S. Misra, and M. Afaque, "Security of wireless and self-organising networks: Security in vehicular ad hoc networks," 2010.

[55] S. N. Pathak and U. Shrawankar, "Secured communication in real time vanet," in *2009 Second International Conference on Emerging Trends in Engineering & Technology*. IEEE, 2009, pp. 1151–1155.

[56] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in vanets," *Computer Science Review*, vol. 41, p. 100411, 2021.

[57] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[58] S. Jat, R. S. Tomar, and M. S. P. Sharma, "Traffic analysis for accidents reduction in vanet's," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 2019, pp. 115–118.

[59] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, and D. Gaiti, "Denial of service (dos) attacks detection in manets using bayesian classifiers," in *2014 IEEE 21st Symposium on communications and vehicular technology in the Benelux (SCVT)*. IEEE, 2014, pp. 7–12.

[60] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET communications*, vol. 4, no. 7, pp. 894–903, 2010.

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

[62] J.-L. Tsai, "An improved cross-layer privacy-preserving authentication in wave-enabled vanets," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1931–1934, 2014.

[63] K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in vanets," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7298–7303.

[64] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, 2023.

[65] M. A. Khan, I. Ullah, N. Kumar, O. S. Oubbati, I. M. Qureshi, F. Noor, and F. U. Khanzada, "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4839–4851, 2021.

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

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

[68] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2018.

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

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

[71] H. Wang, H. Fang, and X. Wang, "Safeguarding cluster heads in uav swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1298–1309, 2021.

[72] A. Haenel, Y. Haddad, M. Laurent, and Z. Zhang, "Practical cross-layer radio frequency-based authentication scheme for internet of things," *Sensors*, vol. 21, no. 12, p. 4034, 2021.

[73] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "Puf-based authentication and key agreement protocols for iot, wsns, and smart grids: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205–8228, 2022.

[74] D. K. Sah and T. Amgoth, "Parametric survey on cross-layer designs for wireless sensor networks," *Computer Science Review*, vol. 27, pp. 112–134, 2018.

[75] Q. Fan, J. Chen, F. Xu, L. Li, and M. Luo, "A biometrics-based anonymous authentication and key agreement scheme for wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 16, p. e6178, 2022.

[76] S. Kumari and K. Renuka, "A provably secure biometrics and ecc-based authentication and key agreement scheme for wsns," *International Journal of Communication Systems*, vol. 33, no. 3, p. e4194, 2020.