Received 18 August 2024; accepted 26 September 2024. Date of publication 4 October 2024; date of current version 24 October 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3474290

State-of-the-Art Security Schemes for the Internet of Underwater Things: A Holistic Survey

NADIR ADAM[1], MANSOOR ALI[1], FAISAL NAEEM[2], ABDALLAH S. GHAZY[1], AND GEORGES KADDOUM[1,3] (Senior Member, IEEE)

[1]Electrical Engineering Department, École de technologie supérieure, Montreal, QC H3C 1K3, Canada
[2]School of Computing, University of the Fraser Valley, Abbotsford, BC V2S 7M7, Canada
[3]Artificial Intelligence and Cyber Systems Research Center, Lebanese American University, Beirut 03797751, Lebanon

CORRESPONDING AUTHOR: N. ADAM (e-mail: nadir.adam@etsmtl.ca)

This work was supported in by the ULTRA TCS Research Chair on Intelligent Tactical Wireless Networks for Challenging Environments, and in part by the National Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant CRDPJ 538896-19.

ABSTRACT With the growing interest that is being shown in marine resources, the concept of the Internet of Things (IoT) has been extended to underwater scenarios, which has given rise to the Internet of Underwater Things (IoUT). The IoUT encompasses a network of interconnected intelligent underwater devices that can be used to monitor underwater environments and support various applications, such as underwater exploration, disaster prevention, and environmental monitoring. Advances in underwater wireless communication and sensor technologies have propelled the IoUT concept forward. However, the IoUT faces significant challenges. The harsh and vast underwater environment makes information sensing particularly difficult and leads to insufficient or inaccurate data being collected. Additionally, underwater conditions like pressure variation, hydrological characteristics, temperature changes, water currents, and topography hinder conventional communication models and make data transmission difficult and inefficient. Security in IoUT networks is a critical concern due to hardware limitations and seawater channel imperfections. Constrained sensor nodes and spatial-temporal uncertainty introduced by node mobility further complicate security provisioning. This survey paper addresses these challenges by offering a comprehensive overview of IoUT security. The investigation thoroughly examines both traditional and classic machine learning techniques and focuses on deploying advanced technologies such as federated learning and digital twin. The study effectively addresses integration challenges and open issues and provides a roadmap for future directions to play a pivotal role in formulating robust security mechanisms for IoUT networks.

INDEX TERMS Internet of Underwater Things (IoUT), federated learning, digital twin, trust management, privacy-preserving, security.

I. INTRODUCTION

THE INTERNET of Underwater Things (IoUT) is a relatively new concept that combines marine technology and network connectivity to extend the reach of the digital age into the depths of oceans. Like its terrestrial counterpart, the Internet of Things (IoT), the IoUT encompasses a network of interconnected sensors, devices, and systems that are deployed underwater. IoUT systems facilitate the collection, transmission, and analysis of data from oceanic environments to support a wide array of applications, including confidential applications such as self-defense, border security, surveillance, and monitoring. Confidential applications require secure IoUT systems to ensure confidentiality, integrity, and availability. Secure IoUT has been an important topic in research and development in the underwater communication field. Its significance has heightened these days due to modern attacking techniques being proposed for underwater communications [1], [2].

Figure 1 illustrates the general architecture of an IoUT network. The sensors and sink nodes collaborate to gather

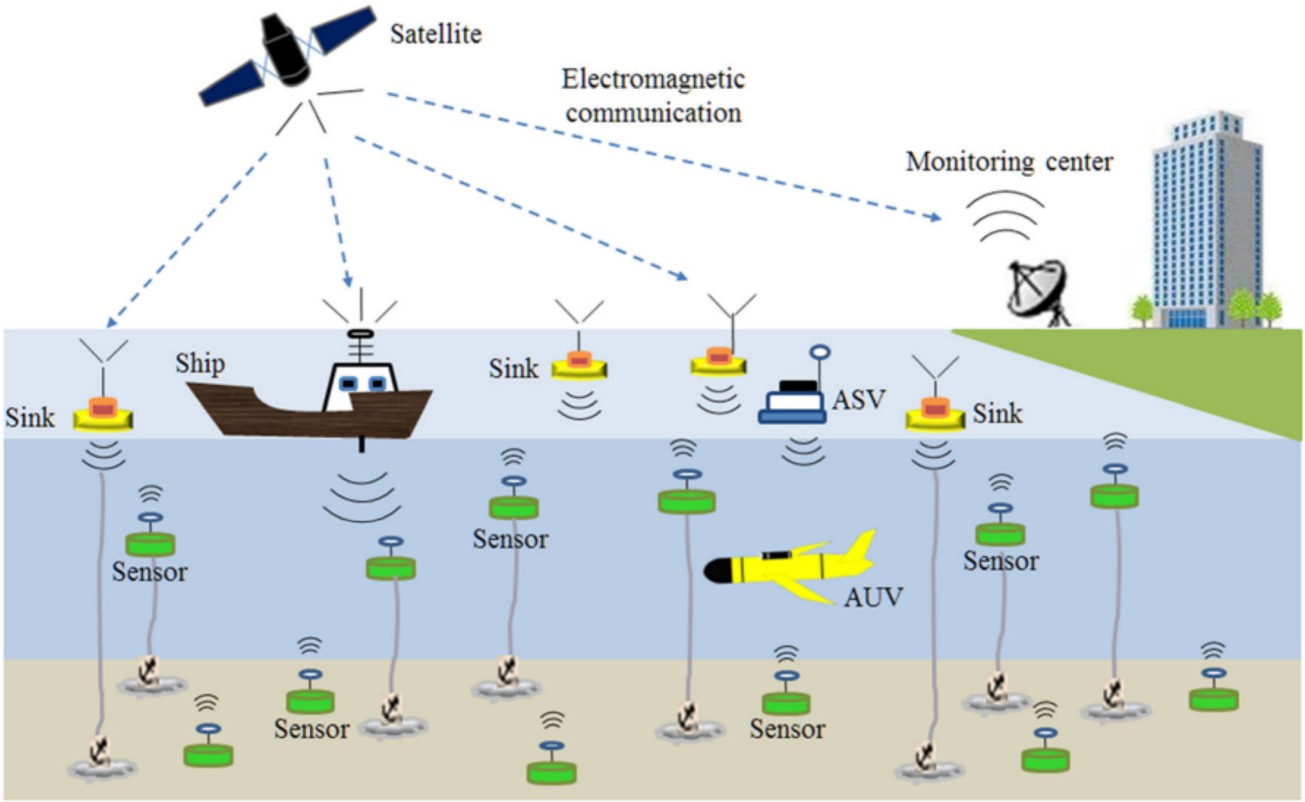

FIGURE 1. General Network Architecture of the Internet of Underwater Things (IoUTs) [3].

seawater data and transmit it to an onshore monitoring center. Sensors can function as either fixed nodes or mobile nodes, such as autonomous vehicles navigating through seawater. These components utilize acoustic communication systems for low-speed, long-range applications and optical communication systems for high-speed, short-range applications. They collect data from seawater and relay transmissions to sink nodes. The sink nodes then forward this data to a satellite using radio frequency (RF) signals. The satellite relays the data to the IoUT center for processing and analysis [4], [5], [6], [7], [8], [9].

The unique underwater environment, characterized by harsh conditions where IoUT networks are deployed, makes securing these networks challenging. For instance, communication underwater often relies on broadcasting, which can lead to the signal strength being higher at the eavesdroppers than at the legitimate nodes. Moreover, line-of-sight communication is not always possible due to the dynamic nature of seawater. Spatial uncertainty induced by currents and waves may direct links to eavesdropper nodes rather than legitimate ones. In addition, underwater channels suffer from severe limitations like attenuation, scattering, and dispersion. The underwater environment, which is influenced by factors such as pressure, temperature, water currents, and marine structures, is highly non-uniform. The complexity of marine settings, including their topography, structures, and natural elements, adds further complexity to signal transmission and reception. Multipath fading, beam bending, and Doppler shift may lead to the channel capacity at the legitimate nodes being lower than that at the eavesdropper ones. Moreover, hardware and physical limitations (e.g., size, weight, battery capacity, memory, digital signal processor) also contribute to these challenges [10], [11], [12].

II. IOUT COMMUNICATION TECHNOLOGIES, LIMITATIONS, AND CHANNEL MODELS

IoUT encompasses a diverse range of communication technologies, each with unique advantages and challenges. Hence, this section explores the key differences between acoustic, RF, and optical communication technologies in underwater environments, delves into the specific challenges they face, and reviews the relevant channel models essential for effective underwater communication.

A. IOUT COMMUNICATION TECHNOLOGIES

Unlike IoT, IoUT nodes predominantly use acoustic signals for communication due to their long-range capabilities and relatively low hardware costs, making them the most established technology for underwater environments. However, acoustic communication presents several challenges. The propagation speed of acoustic waves is much slower than that of RF and optical waves, which reduces the data

TABLE 1. List of main acronyms.

Acronym	Definitions
AIS	Automatic Identification System
AMSVs	Autonomous maritime surface vessels
AoA	Angle of Arrival
ASW	Anti-submarine warfare
AUG	Autonomous Underwater Glider
AUV	Autonomous underwater vehicle
BER	Bit error rate
BS	Base station
CFD	Computational fluid dynamics
CIR	Channel impulse response
CNN	Convolutional neural network
CDMA	Code Division Multiple Access
DDoS	Distributed denial of service
DL	Deep learning
DRL	Deep reinforcement learning
DSSS	Direct sequence Spread spectrum
DT	Digital twin
FEA	Finite element analysis
FHSS	Frequency hopping Spread spectrum
FL	Federated learning
GA	Genetic Algorithm
GMM	Gaussian Mixture Model
HDSPJ	Half-duplex self-protection jamming
IIoT	Industrial internet of things
IMU	Inertial measurement unit
IT	Information technology
IoT	Internet of Things
IoUT	Internet of Underwater Things
IRSs	Intelligent reflecting surfaces
LDPC	Low Density Parity Check
LiDARs	Laser imaging, detection and ranging
LSTM	Long Short-Term Memory
MADDPG	Multi-agent deep deterministic policy gradient
MCN	Maritime communication
MCSS	Multi-carrier spread spectrum
MEMS	Micro-Electrical mechanical systems
ML	Machine learning
MTRRS	Maximum time-reversal resonating strength
NOMA	Non-orthogonal multiple access
OFDM	Orthogonal frequency division multiplexing
OT	Operational technology
PFL	Part-Federated Learning
PLA	Physical layer Authentication
PoQ	Proof of quality
RFL	Remaining fatigue life
RFS	Random finite set
RL	Reinforcement learning
RRMS	Relative root mean square
SINR	Signal-to-interference-plus-noise ratio
SNR	Signal-to-noise ratio
SS	Spread spectrum
SVM	Support Vector Machine
TR	Time-reversal
UASN	Underwater acoustic sensor network
UAV	Unmanned aerial vehicle
USVs	Unmanned surface vehicles
UUV	Unmanned underwater vehicle
UW	Underwater
UW-A	Underwater acoustic
UWSN	Under wireless sensor networks

rate and increases the bit error rate. Additionally, acoustic signals have much lower bandwidth. Moreover, multipath interference and high latency further complicate underwater acoustic communication. On the other hand, while acoustic waves are less susceptible to interference and errors at short ranges with low energy levels, they still face significant issues. The open nature of the underwater acoustic channel makes it easier for attackers to intercept or block communications [3].

RF communication offers advantages over acoustic waves in terms of higher bandwidth and faster transmission speeds. RF waves can operate over a range of frequencies, with extremely low frequency (ELF) waves used for long-distance military communication and higher frequencies for shorter distances. However, RF communication in seawater suffers from high attenuation and requires large antennas and high transmission power. In addition, the absorption loss in seawater limits the practical use of RF waves, making them more suitable for buoyant RF systems that link underwater to terrestrial stations. In contrast, RF communication in freshwater is more effective but still requires large antennas and high power to overcome high antenna losses. Despite these challenges, RF communication can achieve higher data rates using advanced techniques such as multiple input multiple output (MIMO) schemes and adaptive algorithms [13].

Lastly, underwater optical wireless communication (UOWC) provides the highest data rates and can support high-speed transmission over moderate distances. Optical communication is capable of achieving Gbps speeds, but it faces severe challenges related to water absorption and

TABLE 2. Performance metrics and characteristics of underwater communication technologies [3], [9], [13], [14], [15], [16].

Criteria	Acoustic	RF	Optical
Range	Long distance (in Km)	$\leq$ 10 m	$\sim$ Hundreds of meters
Data Rate	Low (in Kbps)	Medium (in Mbps)	High (in Gbps)
Speed	1500 m/s	$2.26 * 10^8$ m/s	$2.25 * 10^8$ m/s
Frequency Band	10-15KHz	30-300 Hz	10^{12} - 10^{15} Hz
Bandwidth	Distance dependent 1000 Km $\leq$ 1 KHz 1-10Km $\approx$ 10KHz $\leq$ 100 m $\approx$ 100 KH z	MHz	10-150 MHz
Attenuation	$\leq$ 100 dB/m	3.5-5 dB/m	$\leq$ 15 dB/m
Latency	High	Moderate	Low
Loss	0.1-4 dB/km	3.5-5 dB/m	0.39-11 dB/m
Energy Efficiency	Low ($\approx$ 100 bits/J for several Km)	$\approx$ 10000 bits/J for 10 m range	$\approx$ 30,000 bits/J at 100 m
Benefits	Long range, proven technology	Immune to noise, water-terrestrial transmission	High speed, low cost, ultra-high bandwidth
Key Factors	Temperature, salinity, pressure	Underwater Conductivity and permittivity	Absorption and scattering
Disadvantages	High delay, low bandwidth	EM interference, low frequency propagation, large antennae size	Short range, strict LoS requirement, affected by environment, requires alignment, prone to turbidity
Best Application	Deep sea transmission	Water-terrestrial transmission	Short range, high data rate transmission

scattering. UOWC requires a line-of-sight (LoS) to avoid significant signal degradation, and the hardware involved is costly. While optical communication is advantageous for its high data rates, it is less practical in environments where LoS cannot be maintained. UOWC technology is also limited by the need for precise alignment and the high costs associated with advanced optical hardware. Therefore, it is often necessary to use a combination of technologies to address challenges like signal attenuation [14].

Table 2 provides a comparison between the aforementioned communication technologies for IoUT.

B. IOUT CHANNEL MODELING

The behavior of the underwater physical layer varies significantly under different channel models and propagation modes, making it challenging to design a universally applicable channel model [3]. Signal attenuation, for instance, differs among electromagnetic, acoustic, and optical carriers, and wired and wireless channels also exhibit distinct behaviors.

In the context of underwater acoustic channels (UWA), key features include slow propagation speed, with acoustic waves traveling at approximately 1450-1550 m/s, much slower than terrestrial radio signals. This slow propagation, combined with multipath scattering from reflections off the sea surface and bottom, contributes to long channel delay spreads [17]. Hence, an appropriate channel model is essential for gaining insights into underwater data transmission, predicting system performance, optimizing node placement, and reducing energy consumption before deployment [14]. In [18], a thorough discussion of underwater acoustic channel modeling is provided, covering both propagation models and statistical characterization.

On the other hand, the optical characteristics of underwater environments are influenced by various factors such as temperature, pressure, salinity, water quality, and air bubbles. These parameters affect the refractive index and attenuation coefficients, impacting light intensity and signal transmission [19]. Recent studies have focused on these effects through both theoretical and experimental research. For instance, a single layer of oceanic turbulence over the entire transmission range has been considered. However, experimental results reveal ocean stratification, where temperature gradient and salinity are depth-dependent, typically varying between a few meters to tens of meters. This stratification results in multiple non-mixing layers with different oceanic turbulence characteristics. Therefore, considering multiple oceanic layers for vertical transmissions may provide a more realistic performance assessment for UOWC systems [20], [21], [22]. Despite these advancements, more comprehensive experimental research in real marine environments is needed to fully understand the impact of actual channels on UWOC performance.

Table 3 provides a comparison between underwater and terrestrial channel modeling characteristics.

C. IOUT SECURITY CHALLENGES

The unique characteristics of the underwater channel limit the ability to adapt existing IoT techniques to underwater communications. Hence, innovative security methodologies for IoUT networks are essential to address these challenges. One example is implementing security schemes that have traditionally been implemented in higher layers (such as

TABLE 3. Comparison of underwater vs. terrestrial channel modeling.

Aspect	Underwater	Terrestrial
Communication Technologies	Acoustic, Optical, RF	RF, microwave, optical
Signal Attenuation Factors	High (varies with medium properties)	Lower (affected by obstacles, weather)
Acoustic Modeling	Complex, influenced by water properties and topography	Simplified, less common
Optical Modeling	High data rates, affected by scattering, absorption	High data rates, more stable, less attenuation
Electromagnetic Modeling	Limited due to high attenuation	Widely used, efficient for long distances
Environmental Impact	Significant (plants, reefs, seabed topography)	Moderate (buildings, terrain)
Channel Modeling Complexity	High (multi-layer, variable properties)	Moderate (uniform medium, simpler models)
Energy Concerns	High, lack of energy harvesting techniques	Moderate, better energy management options

application and transport layers) into lower layers (including network, media access control, and physical layers). This reduces the hardware requirements for implementing sensor nodes. Even when sensor nodes are compact, high-layer security schemes are insufficient, as attacking nodes can exploit associated anti-security measures. Moreover, advancements in supercomputing technology have revealed promising security schemes to address hacking and eavesdropping risks. Embedding security schemes in the physical layer is a promising option, as hacking systems cannot intercept information recovery or processing signals. Security schemes that are implemented in the physical layer leverage the randomness of the communication channel and modern machine learning (ML) algorithms to achieve perfectly secure communications. ML-based physical layer security schemes have been extensively explored in the literature.

In this survey, we comprehensively explore the current state of security methodologies for IoUT networks. Our examination encompasses traditional security schemes and delves into ML-based approaches, with a specific focus on federated learning (FL) and digital twin (DT) technologies. Our emphasis on these advanced technologies distinguishes our survey from existing works and ensures that the use of these technologies in IoUT security and privacy-preserving applications is thoroughly explored.

The remainder of this paper is organized as follows. Section III summarizes the existing surveys on underwater communication security and emphasizes our contributions to the body of knowledge. Section IV introduces the underwater threats and security mechanisms at different levels. In Section V, non-learning-based security schemes are introduced. Section VI explores using ML to enhance security. The applications and challenges of deploying FL underwater are discussed in Sections VII and VIII, respectively. Section IX pertains to DT technology and its relevance to IoUT security. Section X outlines obstacles to implementing DT underwater. Finally, Section XI concludes this paper with a summary of our key findings and potential future research directions.

III. SUMMARY OF PREVIOUS SURVEYS AND OUR CONTRIBUTIONS

In this section, we summarize the existing surveys on underwater communication security, and detail our contributions to the body of knowledge [2], [5], [6], [10], [11], [12], [23], [24].

The authors of [2] provide an overview of recent research investigating trends, applications, technical challenges, privacy issues, security attacks, and potential security solutions for the IoUT. The authors conclude that further research should focus on developing hybrid communication technology that supports fast, reliable, and low-power communication in IoUT networks. Additionally, privacy and security issues can be addressed by developing standard security models and architectures for the IoUT. The fundamentals of network security, as well as the main security threats facing the IoUT and countermeasures for them, are discussed in [5], while [6] provides an extensive overview of various underwater communication technologies, air-to-water communication technologies, the fundamental properties of security requirements, and solutions designed for IoUT.

Yisa et al. [10] discuss IoUT characteristics, security attacks, and attack mitigation techniques. They conclude that a comprehensive security framework and light and energy-efficient protocols for IoUT are still needed. Yang et al. [11] present a more complete survey of the particularities of IoUTs, their current security schemes, and the challenges, attacks, and constraints that affect them. They identified the following types of threats at each network level.

- *Physical layer:* Jamming attacks and eavesdropping attacks.
- *Data link layer:* Unfairness, denial-of-sleep attacks, exhaustion attacks, collision attacks, and jamming attacks.
- *Network layer:* Homing attacks, hello flooding attacks, Sybil attacks, wormhole attacks, sinkhole attacks, black hole/gray hole attacks, misdirection attacks, neglect and greed attacks, selective forwarding attacks, and replay attacks.
- *Transport layer:* Synchronization flooding attacks and desynchronization attacks.

In [12], the authors discussed the challenges, threats, and security issues prevalent in underwater wireless sensor networks. They conclude that an excess of security measures due to applications having varying security requirements can significantly increase energy consumption. Therefore, it is crucial to consider these factors when designing security

TABLE 4. Summary of related surveys on IoUT security.

Ref.	Year	Contribution	Limitations
[2]	2021	The paper addresses four key inquiries concerning IoUT systems: What are the current trends in the IoUT system? What are the challenges faced by the current IoUT system? What methods can be employed to overcome these challenges, including addressing security attacks and privacy issues? What are the findings and future directions?	The paper does not primarily focus on security concerns, it provides comprehensive coverage of various other critical aspects essential for understanding IoUT systems. These encompass discussions on applications, communication technologies, and challenges associated with underwater channels.
[5]	2018	The paper covers the fundamentals of network security, main security threats, and their respective countermeasures.	It does not delve into denial of service (DoS) attacks and feasible countermeasures in each layer in detail.
[6]	2023	The paper provides a comprehensive and up-to-date review of underwater and air-water wireless communications, with a primary focus on the security aspect of these communication systems.	It briefly touches upon the utilization of ML techniques to enhance the security of IoUT.
[10]	2021	The paper provide discussion on the current security challenges in IoUT and UWSNs.	The paper lacks in-depth discussion on the current security challenges in IoUT and UWSNs, potential attacks on UWSNs, and methods available to overcome these challenges and defend against possible attacks. This lack of detailed analysis on threat attacks and defense mechanisms significantly limits the paper's contribution to addressing critical security concerns in underwater communication networks.
[11]	2018	The paper offers an in-depth survey of the current security schemes, challenges, attacks, constraints, and particularities of IoUTs.	It restricts future research topics solely to the reconfiguration of the security system periodically.
[12]	2019	The paper discusses six specific attacks and identifies seven attack surfaces for autonomous ships. These attack surfaces include remote operation systems, vessel-to-land communications, intra-vessel networks, voyage data recorders, firmware, sensors, and positioning systems. The six possible attacks outlined in the paper encompass link disruption, signal jamming, Automatic Identification System (AIS) spoofing, GPS spoofing, tampering, and code injection.	The paper limits the security scope on the threat attaches associated to autonomous vehicles.
[23]	2011	The paper presents a comprehensive overview of IoUTs' security, including possible attacks and countermeasures.	It only considers a limited number of security threats and classic defense techniques.
[24]	2018	The paper examines the challenges, threats, and security issues prevalent in UWSNs. The authors highlight the diverse security requirements across different applications, emphasizing that an excess of security measures can substantially increase energy consumption. Hence, they stress the importance of carefully considering these factors when designing security schemes for underwater communications.	The paper considers few security threats and classic defence techniques. As well, it does not present research topics for future works.

schemes for underwater communications. Moreover, [23] presents a thorough overview of IoUT security, attack types that may be encountered, and attack countermeasures.

Silverajan et al. [24], discussed six specific attacks and seven attack surfaces for autonomous ships. The ships' remote operation systems, vessel-to-land communications, intra-vessel networks, voyage data recorders, firmware, sensors, and positioning systems are identified as potential attack surfaces. The six possible types of attacks are link disruption, signal jamming, automatic identification system (AIS) spoofing, global positioning system (GPS) spoofing, tampering, and code injection.

The existing literature lacks sufficient coverage of current IoUT security concerns, which highlights the critical need for our survey paper. Our work sets itself apart by thoroughly examining and addressing the unique security challenges that are inherent in the IoUT. Importantly, our paper traces the evolution from non-learning-based methods and ML-based approaches to the latest advancements, which are represented by FL and DT. This incorporation of FL and DT underscores the need for a comprehensive and thorough review. The detailed discussion that is provided in our paper is intended to provide insights and recommendations for enhancing the security posture of IoUT systems.

IV. UNDERWATER THREATS AND SECURITY MECHANISMS

Threats and security in the IoUT present a comprehensive challenge, requiring unique metrics and techniques to ensure a robust network. This section focuses on threats at various levels within IoUT systems, providing a clear picture of the security landscape and highlighting specific vulnerabilities and attack vectors. Additionally, we detail security techniques, examine vulnerabilities, and discuss attacks specific to IoUT, emphasizing the importance of targeted security measures to strengthen the overall resilience of IoUT systems.

A. DEVICE-LEVEL THREATS AND SECURITY TECHNIQUES

Device-level threats primarily involve physical tampering and unauthorized access to IoUT devices. Since these devices are often deployed in remote and harsh underwater environments, they are susceptible to physical damage, theft, and tampering. Malicious actors could physically access the devices to extract sensitive information, disrupt operations, or implant malicious firmware. Tamper-resistant enclosures and anti-tamper mechanisms are crucial to protect these devices [25], [26], [27]. Another significant threat is the compromise of the hardware itself, such as through the insertion of malicious components during manufacturing or supply chain attacks, which can undermine the entire security infrastructure of the IoUT network [28]. Device security is paramount in IoUT as the devices are often deployed in harsh and inaccessible environments. Metrics for device security include tamper resistance, which measures the ability of a device to withstand physical tampering, and intrusion detection, which gauges the effectiveness of mechanisms designed to detect unauthorized access [29]. Techniques to enhance device security involve the use of ruggedized and tamper-proof casings to protect the devices physically. Additionally, Hardware Security Modules (HSMs) are employed to perform cryptographic operations securely, safeguarding sensitive data and cryptographic keys. Anti-tamper mechanisms, such as sensors and alarms, can be integrated to detect and respond to tampering attempts, providing an additional layer of security to the physical devices [30].

B. PHYSICAL LAYER SECURITY AND THREATS

Physical layer threats in the IoUT involve the vulnerabilities associated with the communication medium itself. Given the underwater environment, the physical layer primarily deals with acoustic, optical, or electromagnetic communication. Threats at this layer include jamming, where attackers intentionally emit signals to interfere with legitimate communication, causing disruptions and loss of connectivity [31]. Eavesdropping at the physical layer can occur when attackers use specialized equipment to capture signals, leading to data breaches. Signal attenuation and multipath fading are natural phenomena that can degrade the quality and reliability of communication in underwater environments [32].

Physical layer security and covert communication are specialized techniques critical for securing data communication in underwater environments. Physical layer security exploits the characteristics of the communication medium to enhance security [33]. Metrics such as Signal-to-Noise Ratio (SNR), which measures the quality of the signal against background noise, and Bit Error Rate (BER), which indicates the number of errors in the transmitted data, are used to evaluate physical layer security [34]. Techniques like spread spectrum, which spreads the signal over a wide bandwidth to make interception harder [35], beamforming, which directs the signal towards the intended receiver to reduce eavesdropping [36], and channel coding, which adds redundancy to correct transmission errors, are employed to secure data at the physical layer [37].

Covert communication involves hiding the presence of communication to avoid detection, with metrics like detection probability and covert rate used to evaluate its effectiveness. Techniques such as steganography, which hides messages within non-suspicious data [38], frequency hopping, which changes the transmission frequency to avoid detection [39], and underwater acoustic modulation, which blends signals with ambient noise [40], are used to achieve covert communication, ensuring that sensitive data remains undetected and secure during transmission.

C. DATA-LEVEL SECURITY AND THREATS

Data-level threats encompass unauthorized access, data breaches, and data integrity attacks. Unauthorized access to sensitive data can lead to information leakage, where confidential data such as environmental readings or military communication logs are exposed to unauthorized parties [41]. Data breaches can occur through various means, including interception during transmission, accessing unprotected storage, or exploiting software vulnerabilities [42]. Data integrity threats involve the alteration or corruption of data, either accidentally or maliciously, which can lead to erroneous decision-making based on inaccurate information [43]. Data security ensures that the data collected, transmitted, and stored by IoUT devices remains secure from unauthorized access and alterations. Key metrics for data security include data confidentiality, data integrity, and data availability [44]. Data confidentiality is typically achieved through encryption methods such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA), which secure the data by making it accessible only to authorized entities [45]. Data integrity is maintained using hash functions like Secure Hash Algorithm 256-bit (SHA-256), ensuring that the data remains unaltered during transmission and storage [46]. To ensure data availability, redundancy techniques are employed, wherein data is stored in multiple locations, thus preventing data loss due to failures or attacks on a single point of storage. Encryption, access controls, and data validation mechanisms are essential to protect against these

threats, ensuring that data remains confidential and unaltered throughout its lifecycle [47], [48].

D. NETWORK-LEVEL SECURITY AND THREATS

Common network-level threats include eavesdropping, where attackers intercept and listen to the communication between IoUT devices, leading to data breaches and loss of confidentiality [49]. Denial of Service (DoS) attacks are another major concern, where malicious actors flood the network with excessive traffic, rendering it unusable for legitimate communication and severely disrupting operations [50]. Man-in-the-middle (MitM) attacks, where the attacker intercepts and potentially alters the communication between two parties, are particularly dangerous in the IoUT as they can go undetected in the noisy underwater environment [51]. Network security is crucial for protecting the communication channels and infrastructure from unauthorized access, attacks, and disruptions. Metrics for network security include latency, throughput, and packet loss rate [52]. Latency measures the time taken for data to travel from the source to the destination, while throughput assesses the amount of data transmitted over the network within a given time. The packet loss rate indicates the percentage of packets lost during transmission, which can impact the reliability of data communication [53]. To secure the network, firewalls are used to filter incoming and outgoing traffic based on predefined security rules. Virtual Private Networks (VPNs) create secure tunnels for data transmission, ensuring that data remains confidential and intact during transfer [54]. Intrusion Detection Systems (IDS) monitor network traffic for suspicious activities, enabling the detection and mitigation of potential threats in real-time [55]. Implementing strong encryption, network segmentation, and anomaly detection systems is critical to mitigating these threats.

E. APPLICATION-LEVEL SECURITY AND THREATS

Application-level threats involve vulnerabilities in the software applications that control and manage IoUT devices and data. These threats include malware and ransomware attacks, where malicious software is introduced into the system to steal data, corrupt files, or lock access until a ransom is paid [56]. Application-level attacks can also exploit software vulnerabilities, such as buffer overflows, injection attacks, and insecure coding practices, to gain unauthorized access or control over the system [57]. Application security involves securing these software applications. Metrics for application security include code quality, vulnerability density, and patch management efficienc2y [58]. Ensuring regular software updates, employing secure coding practices, and implementing robust application security measures like intrusion detection systems and firewalls can help protect against threats at the application level [59].

F. AUTHENTICATION AND AUTHORIZATION SECURITY AND THREATS

Authentication and authorization threats are critical as they ensure that only legitimate users and devices can access the IoUT network and its resources. Threats at this level include credential theft, where attackers steal login credentials to gain unauthorized access to the network. Phishing attacks, where attackers trick users into revealing their credentials through deceptive emails or websites, are a common method for credential theft [60]. Weak or reused passwords also pose a significant risk, as they can be easily guessed or cracked using brute force attacks [61]. Insufficient authorization controls can lead to privilege escalation, where a user gains access to higher-level functions or data than intended [62]. Authentication and authorization are critical to ensure that only authorized entities can access the IoUT network and its resources. Metrics such as authentication time, which measures the time taken to verify an entity's identity, and authorization accuracy, which ensures that access controls are correctly applied, are used to evaluate these processes. Public Key Infrastructure (PKI) is commonly used for authentication, relying on digital certificates to verify identities [63], [64]. Biometric authentication, which uses unique biological traits such as fingerprints and retinal scans, provides a highly secure method of verifying identities [65]. Role-Based Access Control (RBAC) is employed to grant access based on predefined roles, ensuring that users can only access resources necessary for their specific roles, thereby minimizing the risk of unauthorized access [66].

G. SOFTWARE AND FIRMWARE UPDATES SECURITY AND THREATS

Threats related to software and firmware updates include the risk of installing malicious updates, either through compromised update servers or through man-in-the-middle attacks during the update process [67]. Ensuring the authenticity and integrity of updates using cryptographic signatures and secure update protocols is crucial to mitigate these threats [68]. Software and firmware updates are essential for maintaining the security and functionality of IoUT devices. Regular updates help fix vulnerabilities and enhance performance. Metrics such as update frequency, which indicates how often updates are released, and update success rate, which measures the percentage of devices successfully updated, are crucial for evaluating the effectiveness of update mechanisms [69]. Over-the-air (OTA) updates enable wireless updating of software and firmware, making it easier to deploy updates to devices located in remote underwater environments [70]. Cryptographic signatures are used to ensure the authenticity and integrity of updates, preventing the installation of malicious or corrupted updates. Rollback mechanisms allow devices to revert to previous versions if an update fails or introduces issues, ensuring the continuity and reliability of the IoUT network [71].

Table 5 provides a concise summary of various underwater threats and the corresponding security countermeasures designed to mitigate them.

In the next section, we discuss various non-learning-based security approaches. We dissect these strategies to provide a thorough understanding of non-learning-based security

TABLE 5. Summary of underwater threats and security countermeasures.

Security Level	Threats	Security Techniques	Metrics
Device-Level	Physical tampering, unauthorized access, hardware compromise, supply chain attacks	Tamper-resistant enclosures, anti-tamper mechanisms, HSMs	Tamper resistance, intrusion detection
Physical Layer	Jamming, eavesdropping, signal attenuation, multipath fading	Spread spectrum, frequency hopping, beamforming, channel coding and modulation	SNR, BER, detection probability, covert rate
Data-Level	Unauthorized access, data breaches, data integrity attacks	Encryption, hash functions, redundancy techniques	Data confidentiality, data integrity, data availability
Network-Level	Eavesdropping, DoS, MitM attacks	Firewalls, VPNs, IDSs	Latency, throughput, packet loss rate
Application-Level	Malware, ransomware, software vulnerabilities (buffer overflows, injection attacks)	Secure coding practices, regular software updates, intrusion detection systems	Code quality, vulnerability density, patch management efficiency
Authentication and Authorization	Credential theft, phishing, weak/reused passwords, privilege escalation	PKI, biometric authentication, RBAC	Authentication time, authorization accuracy
Software and Firmware Updates	Malicious updates, man-in-the-middle attacks during updates	Cryptographic signatures, secure update protocols, OTA updates, rollback mechanisms	Update frequency, update success rate

measures and enhance the depth of the insights presented in our survey paper.

V. NON-LEARNING-BASED IOUT SECURITY

In what follows, we discuss different non-learning-based security approaches that provide a variety of effective mechanisms for enhancing the confidentiality, integrity, and availability of data in IoUT networks. These approaches provide a strong defense against potential security threats and unauthorized access to ensure the secure operation of IoUT systems.

A. SPATIAL APPROACHES

A typical source transmits power in watts, while a node detects signals in microwatts. The rest of the power is generally lost to the environment in different ways, which creates security threats where eavesdroppers are located. Modern techniques, such as directive antennas, beamforming techniques, and IRSs, are proposed to overcome that problem and increase a system's level of secrecy. Directive antennas and beamforming customize the beams before they are emitted by the sources, while IRSs reconfigure the beams before they reach the receivers. These techniques require knowing a receiver's general location. Therefore, we discuss them in more detail below and explain their respective functionalities and applications.

1) DIRECTIVE ANTENNAS AND BEAMFORMING TECHNIQUES

Optical sources, such as laser diodes, are highly directive and can be pointed toward the target without increasing the complexity of a system. Acoustic sources can be aligned too. However, aligning an acoustic source increases the complexity of the system and the cost of implementation. For instance, a novel acoustic source that is based on a parametric acoustic array is proposed for underwater communications [72]. Not only is the parametric array light and compact, but it is highly directive and has a narrow beam with no side lobes. The narrow beam width secures the data from a spatial point of view.

In mobile scenarios like those involving autonomous underwater vehicles (AUVs), a more flexible solution could be provided by adapting the radiation pattern using beamforming techniques rather than generating fixed radiation patterns using directive antennas. Beamforming could be implemented using multiple input multiple output technology, single input multiple output technology, multiple input single output technology, relays, cooperative multipoint systems, or distributed antenna systems, among other options. Beamforming involves the transmitter adapting and optimizing its transmission parameters based on the channel characteristics of the legitimate receiver in order to improve secrecy performance and prevent eavesdroppers from successfully decoding the data. The transmitter can use digital beamforming, precoding (zero forcing, minimum mean square error, etc.), full/partial pre-equalization, adaptive power allocation, transmit antenna selection, interference alignment, cooperation, or relay selection, among other methods, to achieve this.

2) INTELLIGENT REFLECTING SURFACES

Using reflecting surfaces for beam reconfiguration has been a well-established method for decades. However, the latest IRS technology offers distinct advantages. Unlike traditional reflecting surfaces that have fixed coefficients, IRSs are able to dynamically reconfigure their coefficients in real time due to developments in micro-electrical mechanical systems (MEMSs) and composite materials [73]. Unlike active relay methods, which require additional energy, IRSs passively

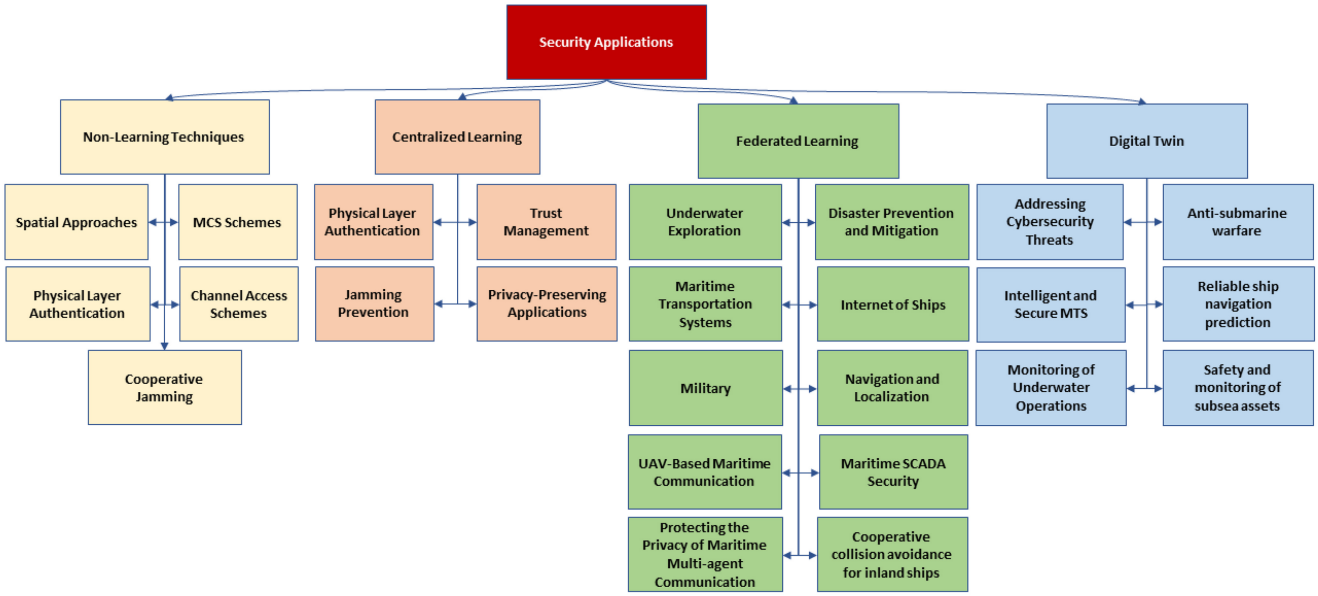

FIGURE 2. Key Techniques and Applications for Underwater Security.

reflect incident signals and are, therefore, energy-efficient and green technology.

Unlike backscatter communication, which is often constrained to using a limited number of antennas due to complexity and cost considerations [74], IRS technology stands out for its ability to integrate numerous reflecting elements. Moreover, IRSs simply facilitate signal transmission between designated transmitter-receiver pairs without transmitting their own information, while the same cannot be said for backscatter communication [75]. In the context of underwater communication, where acoustic signaling is preferred due to challenges with electromagnetic and optical methods [3], IRSs are a potential solution.

IRS deployment can be stationary, attached to AUVs, or floating. Stationary deployment is simpler but requires robust optimization for large distances. AUVs function as mobile relays and enhance the signal propagation of their integrated IRSs. Floating IRSs that are tethered with a cable pose a design challenge, as they require elements to reflect signals omnidirectionally [3].

The significant advantages of IRS technology have led to proposals to create programmable wireless environments for physical layer security. IRSs can adjust the reflecting coefficients to control incident wave attenuation and scattering and, in turn, ensure the desired propagation and create dead zones for eavesdroppers [75]. For instance, the authors of [76] focused on improving secrecy in a combined dual-hop system by integrating IRS-assisted RF and UOWC. Their mathematical analyses show that having more reflecting elements enhances secrecy performance by increasing the signal-to-noise ratio (SNR) gain. Moreover, communication security is ensured when there are sufficient reflecting elements to meet the minimum required by both the user and the eavesdropper. The study also looked into the impact that fading parameters, scale parameters, air bubble levels, temperature gradients, and water salinity have on secrecy performance.

On the other hand, the authors of [77] proposed the implementation of IRSs between buoyed nodes and AUVs. The buoyed-to-IRS-to-AUV (BIA) link facilitates secure and reliable communications by dynamically adjusting its beam widths and IRS depth in response to variations in wind and tide speeds. Their numerical results demonstrated the effectiveness of this approach, with the BIA link achieving a 300% increase in the secrecy rate compared to the direct buoyed-AUV link.

To summarize, while spatial security approaches offer significant advantages when it comes to enhancing the security of IoUT networks, they also come with challenges related to complexity, cost, hardware constraints, and the need for precise calibration. Careful consideration of these factors is essential for designing robust and effective security mechanisms for IoUT systems.

B. MODULATION AND CODING SCHEMES (MCSS)

1) MODULATION SCHEMES

Spread spectrum (SS) modulation achieves secure and reliable transmission since it ensures a low probability of interception (LPI) and suppresses jamming. SS schemes are implemented in the time domain in the form of direct-sequence SS (DSSS) modulation and in the frequency domain in the form of frequency-hopping SS (FHSS) modulation. SS modulation techniques produce noise-like streams and spread the information power over a wide frequency spectrum. Hence, attackers do not know exactly where the information they are seeking is located in the time or spectrum domains. FHSS schemes require relatively wider communication bandwidths than DSSS schemes do

to make sure information cannot be jammed or overheard. In multi-user networks, the DSSS scheme is known as the code-division multiple access (CDMA) scheme and involves each user being associated with unknown orthogonal codes.

CDMA schemes have long been used to ensure covert communications in multi-user networks. For instance, a multi-carrier spread spectrum (MCSS) modulation has been proposed as a means to render covert underwater acoustic (UW-A) communication at low SNRs [78], [79]. Moreover, a multiband orthogonal frequency-division multiplexing (OFDM) transmitter and receiver were proposed for secure UW-A communication in a low SNR regime to avoid interception [80]. Moreover, the authors of [81] proposed a noise-resistant UOWC system based on spectrum spread and encrypted OFDM (SSE-OFDM) modulation. Their experimental system demonstrates significant security enhancements, including suppressing the SNR of the eavesdropper and improving the SNR of the authorized user.

However, recent works have shown that SS schemes can become vulnerable to attacks since they can blindly identify the spreading code used by the legitimate user when neither the channel state information nor the training sequence is available. While SS schemes improve channel secrecy, they are not robust enough to reliably ensure secure communications.

2) CHANNEL CODING SCHEMES

On the other hand, channel coding schemes enhance underwater security by introducing redundancy for error detection and correction, improved reliability, and eavesdropping resistance. Some channel coding schemes inherit security from their architectures, which enable them to simultaneously encrypt and encode exchanged information. Jointing the encryption/encoding and decryption/decoding processes in the transmitter and receiver, respectively, yields faster processing and easier implementation.

Advanced coding schemes, such as low-density parity-check (LDPC) codes, not only provide error correction but also add complexity to make interception and decoding more challenging for potential eavesdroppers. For instance, an underwater Gaussian wiretap channel, which is a practical coding scheme that is based on LDPC codes, can be combined with existing cryptographic schemes to improve data security by taking advantage of the statistical nature of communication channels [33].

Some LDPC code design techniques have been assessed for security gaps when applied to an additive white Gaussian noise (AWGN) wiretap channel. The authors have studied applying a special type of LDPC code that is based on serially concatenated low-density generator matrix codes to the Gaussian wiretap channel. In [82], the equivocation rate of Eve's channel is considered an optimization criterion when designing an algorithm in the finite codeword length regime. The proposed algorithm makes it possible to construct irregular LDPC codes with shorter codeword lengths that are able to approach the ultimate performance limits.

C. CHANNEL ACCESS SCHEMES

An efficient channel access model that utilizes cross-layer design is suggested in [83], [84] to alleviate reactive jammers. The proposed model simultaneously optimizes the cooperative hopping and channel accessibility probabilities of authenticated sensor devices. Experimental results indicate that the proposed model outperforms current state-of-the-art models in terms of successful packet transmission.

D. COOPERATIVE JAMMING

Cooperative jamming proves beneficial in scenarios where the adversary's channel quality is better than that of the legitimate link, which makes it difficult to achieve perfect secrecy with zero information leakage during source-destination message exchanges, as discussed in [85].

The authors addressed this by proposing a secure physical layer scheme that employs cooperative friendly jamming by means of CDMA-based physical-layer network coding (PNC) to facilitate the confidential transmission of secure messages in the presence of eavesdropping attacks. The cooperative friendly jammer uses the same spreading code as the legitimate sender-receiver. The problem of optimally selecting the friendly jammer from a number of jammers and optimally allocating energy to the sender and the friendly jammer was formulated, so as to minimize the signal-to-interference-plus-noise ratio (SINR) at the eavesdropper while ensuring a minimum SINR at the legitimate receiver. The proposed scheme was validated using simulations and underwater testbed experiments.

The work in [86] involves randomly choosing a jammer from a set of sensor nodes to transmit a jamming signal in order to degrade the received SINR at the eavesdropper. The authors of [86] also adopted a coordinated multipoint (CoMP) signal alignment technique to facilitate signal reception at the legitimate receiver. The authors of [87] proposed a system that utilized cooperative jamming and artificial noise to maximize the secrecy rate. Those same authors later extended their work in [88], [89], [90], where they propose a secure transmission scheme that is based on energy-efficient cooperative jamming. Their proposed scheme involves three stages. First, the transmitter's communication range is divided into regions, and one assisting node in each region is selected as a friendly jammer. Next, the jamming power of the assisting nodes is optimized in accordance with a genetic algorithm (GA). Finally, the assisting nodes are re-clustered based on their energy threshold to prolong the lifetime of the underwater sensor network. Their proposed scheme was implemented in lake and sea environments and performed better in terms of secrecy rate than the half-duplex self-protection jamming (HDSPJ) approach, which is dependent on the legitimate receiver itself to transmit jamming signals [91].

E. PHYSICAL LAYER AUTHENTICATION

In [92], a cooperative method for authenticating messages in underwater acoustic networks is introduced. It involves

trusted nodes and a sink node cooperating to determine whether a received message is legitimate or from an attacker. The method exploits the spatial dependency and time invariance of underwater acoustic channel features to calculate a decision index for authentication. Trusted nodes carry out the calculation in a distributed manner, while the sink node combines their opinions and makes the final decision without needing to provide feedback to the trusted nodes. The approach's effectiveness is confirmed in extensive numerical simulations and sea experiments.

An authentication scheme that considers the angle of arrival (AoA) for stationary and line-of-sight underwater acoustic sensor networks (UASNs) is proposed in [93]. The authentication process involves comparing the measured AoA with the sink's estimated AoA database using the nodes' Mahalanobis distances. The legitimate and malicious nodes are modeled using a finite Gaussian mixture model (GMM) in order to estimate their Mahalanobis distances. The authors extended their work in [94], [95], where they propose a physical layer authentication (PLA) scheme for node authentication in an underwater time-varying multipath environment. Their proposed scheme uses the time-reversal (TR) process and considers the channel impulse response (CIR) to be a key location-specific feature. This is achieved by convolving a probe signal's estimated CIR with the node's CIR database, and then calculating the maximum time-reversal resonating strength (MTRRS) to make an authentication decision. A similar TR and CIR-based authentication scheme was also proposed in [96]. On the other hand, a novel two-step method for impersonation detection in an AWGN-limited, LoS underwater acoustic channel was proposed in [97]. Initially, a proximity-based binary hypothesis test where the sink node uses the distance estimate of the sender node to ascertain if it falls within a predefined trusted zone was employed. Subsequently, assuming knowledge of the AoA and thereby the transmitter's position, they utilize these estimates along with distance as unique identifiers of the transmitter. These parameters undergo a maximum likelihood test and subsequent binary hypothesis test, with their individual outcomes fused together to generate the final decision on impersonation.

Moreover, the authors of [98] propose a PLA scheme to address challenges that are posed by harsh underwater environments with temporal and spatial variation. The proposed scheme introduces a dynamic CIR database to enable robust authentication by fully tracking and exploiting time-varying acoustic links. The proposed scheme's ability to adapt to dynamic underwater environments and high authentication accuracy is validated by simulations and sea trials. Moreover, since relying on a static CIR database may limit prompt adaptation to dynamic underwater transmissions, a modified PLA scheme that relies on a dynamic database concept is proposed and is better able to detect malicious attackers is also proposed. The study emphasizes the need for further investigation into data augmentation algorithms to reduce authentication overhead in IoUT networks.

In addition, a PLA approach that utilizes a Kalman filter to track the power-weighted average delay of significant channel taps from a genuine transmitter was proposed in [99]. Their approach is able to determine whether a transmitter is legitimate or an impersonator by examining the Kalman filter's measure of innovation. This approach inherently considers mobility. Simulation results indicate that the proposed method remains effective even when an attacker can track and locate the genuine transmitter with different levels of accuracy and manipulate receiver-side impulse responses.

Moreover, in [100], [101], a PLA mechanism was proposed that utilizes transmitter node positions for authentication. The authors employed time of arrival (ToA) estimation to estimate transmitter positions using signals received at fixed reference nodes within a predefined underwater region. They analyzed the uncertainty associated with these position estimates and subsequently used binary hypothesis testing on these estimates to ascertain the legitimacy of transmitter nodes. Closed-form expressions were provided for false alarm and missed detection rates. Finally, simulation-based validation demonstrated robust performance across varying link qualities, placements of malicious nodes, and receiver operating characteristic (ROC) curves. Comparative analysis underscored its advantages over existing fingerprint mechanisms for PLA in underwater acoustic networks, such as AoA [93], CIR [95], and distance [97].

The limitations of the deterministic methods that are employed by non-learning-based technologies to address IoUT system requirements underscore the need for a paradigm shift. Hence, the next section provides an overview of state-of-the-art ML-based security schemes with a focus on key areas such as PLA, trust management, and jamming prevention.

VI. MACHINE LEARNING-BASED IOUT SECURITY

In what follows, we describe in detail some ML-based security schemes and privacy-preserving applications for IoUT networks.

A. PHYSICAL LAYER AUTHENTICATION

ML-based PLA in IoUT networks takes a data-driven approach to authentication and helps systems learn and adapt to underwater communication signals to increase network security in challenging underwater environments.

Recent research has explored using advanced ML techniques to strengthen underwater security. For example, the authors of [102], [103] propose a two-stage ML technique to identify a single impersonating attacker based on four features, i.e., number of channel taps, average tap power, relative root mean square (RRMS) delay, and smoothed received power. In the first stage, the trusted nodes train a neural network (NN), which results in a soft decision about the sender's authenticity. In the second stage, all the trusted nodes' NN outputs are fused to arrive at a hard decision

TABLE 6. Summary of non-learning-based techniques advantages and drawbacks.

Ref.	Approach	Description	Advantages	Drawbacks
[72], [76], [77]	Spatial approaches	Utilizes directive antennas, beamforming techniques, and IRSs to enhance signal directionality, mitigate interference, and customize signal beams to enhance data security by preventing eavesdropping	(1) Enables targeted communication towards specific receivers (2) Enhanced security against eavesdropping (3) Flexibility in shaping and directing beams (4) Energy efficiency with IRS technology	(1) Requires precise knowledge of underwater channel conditions (2) Limited effectiveness in dynamic environments (3) Implementation complexity and hardware constraints
[78], [79], [81], [80], [33], [82]	Modulation and Coding Schemes	Uses sophisticated modulation techniques and error-correcting codes to improve reliability and security of data transmission. For instance, SS modulation techniques spread data over wide spectra, making interception difficult. Channel Coding schemes like LDPC codes add redundancy for error correction and enhance security in multi-user networks	(1) Provides robustness against noise and interference with a LPI due to noise-like signal spreading (2) Supports high data rates over longer distances with improved reliability and error correction capabilities using advanced coding schemes	(1) FHSS requires wider communication bandwidth (2) Vulnerable to specific types of attacks
[83], [84]	Channel Access Schemes	Controls how devices access the communication channel to manage interference, ensure fair access, and optimize channel accessibility to combat reactive jammers and improve successful packet transmission rates	Effective in mitigating the effects of reactive jammers	(1) Implementation Complexity (2) Dependent on accurate synchronization and cooperation among devices
[85], [86], [87], [88], [89], [90], [91]	Cooperative Jamming	Utilizes friendly jammers to degrade eavesdropper channel quality. Techniques include PNC and CoMP signal alignment to maximize secrecy rates	(1) Enhances security by creating noise-like interference and effectively enhances secrecy through cooperative interference techniques (2) Dynamic defense against eavesdropping attacks (3) Improves confidentiality of transmitted data	(1) Requires optimal selection and synchronization of friendly jammers (2) Increased complexity in managing energy allocation and interference patterns
[92], [94], [93], [95], [96], [97], [98], [99], [100], [101]	Physical Layer Authentication	Verifies the authenticity of transmitters/receivers based on physical layer characteristics (e.g., signal strength, timing) before data transmission. Techniques include AoA comparisons, TR processes, and dynamic CIR databases to ensure robust authentication in dynamic underwater environments	(1) Provides robust authentication without relying on higher layers (2) Robust against impersonation and spoofing attacks due to spatial and temporal dependency features (3) Distributed authentication without direct feedback to trusted nodes	(1) Computational overhead in managing authentication processes (2) Limited adaptation to rapidly changing underwater channel conditions

about the authenticity of the received packet. The authors validate their scheme using simulations and data from the Mediterranean Sea. Furthermore, extending their research in [104], the authors utilized a sensor array for extracting and monitoring channel features. This enabled continuous tracking of these features over time without needing explicit

knowledge of the transmitter's movements, which is crucial for adapting to the dynamic channel conditions in underwater acoustic networks with mobile devices. The proposed strategy integrates an LSTM-based approach, where sensors predict future feature values based on learned models, thereby enhancing the robust authentication of transmitted data. This methodological advancement addresses challenges posed by mobile receivers and transmitters that alter channel characteristics with their movements, ensuring dependable authentication even in scenarios involving complex mimicry attacks.

On the other hand, the authors of [105] propose a PLA framework to detect spoofing attacks in underwater sensor networks. Their proposed scheme utilizes the acoustic channels' power delay profiles (PDPs) to distinguish legitimate and spoofed sensors. Moreover, the framework employs reinforcement learning (RL) to automatically select the authentication parameter without prior knowledge of the network or the spoofing model. Furthermore, the authors propose a deep reinforcement learning (DRL)-based authentication scheme that employs a convolutional neural network (CNN) to compress the state space observed by the sink and thus improve the sink's authentication accuracy.

Finally, the authors of [106] propose a PLA strategy that leverages the spatial dependency of CIRs. Their strategy utilizes two database-correlative features to characterize CIR patterns and enhances nodes' authentication accuracy while accounting for bandwidth and energy constraints. Furthermore, the authors introduce a training set construction method that does not require adversary data, making it possible to use support vector machine (SVM) for distributed spoofing attacker identification. The results of simulations performed with sea trial CIR data validate the proposed scheme's efficacy and showcase its high authentication accuracy, low overhead, and reduced energy consumption.

B. TRUST MANAGEMENT

Trust management systems, which are essential for assessing node reliability in IoUT networks amid adverse attacks, have experienced a significant upswing in dedicated research. This surge underscores the pivotal role these systems play in enhancing the IoUT security. For instance, the authors of [107] propose a synergetic SVM-based trust model that divides the network into clusters using the K-means algorithm. In addition, they implement a double cluster head approach to extend the network's lifetime and enhance network security. Finally, they apply SVM algorithms to generate a trust evaluation model.

Similarly, an SVM and Dempster-Shafer (SVM-DS) fusion-based trust management mechanism for UASNs is proposed in [108]. The scheme utilizes three types of trust evidence, namely packet-based, data-based, and energy-based evidence, to evaluate the trustworthiness of nodes. A node's degree of trustworthiness is determined by a trained SVM model, and the trust classification results for the three types of evidence are fused using the DS evidence theory to obtain an overall trust classification. The mechanism also incorporates a trust redemption process that takes into account historical performance and environmental factors to correct the trustworthiness classification of nodes. Lastly, the trust evaluation results of neighboring nodes are fused to update the target node's trust value.

Furthermore, the authors of [109] addressed the problem of effective trust updating in the face of unstable underwater environment fluctuations and attack mode switching by proposing a trust update mechanism. Firstly, they designed an environment model to quantify the impact underwater fluctuations have on sensor data to facilitate updating the trust scores. Secondly, they introduced the concept of key degree, which determines the relative priority of sensor nodes for trust score updating. Nodes with higher key degree values are more sensitive to malicious attacks and, thus, must be better protected. Lastly, the authors introduce an RL-based trust update mechanism to efficiently update the trust score despite attack mode changes.

Han et al. [112] propose a novel trust model to defend against sudden network faults and malicious attacks. Their proposed model is divided into three phases. First, a quantified environment model is developed to reflect the underwater environment's impact on trust evaluation. Then, an RL-based trust update model is constructed to mitigate hybrid attacks. Finally, a trust redemption model is developed to reinstate low-trust sensor nodes in order to improve the network's resource utilization. Experimental results prove that the proposed trust model can achieve highly efficient trust updating in the face of attack mode changes.

In addition, the authors of [113] propose an LSTM network-based adaptive trust model for UASNs that they call LTrust. The LSTM network is trained to build an adaptive trust model with explicit memory properties that are then used to calculate trust values for anomalous node detection. Simulation results show that the LTrust model is highly effective at defending against both hybrid and single-mode attacks.

To screen out unreliable recommendations and dishonest nodes in the network and avoid potential danger, Zhang et al. [114] propose a recommendation management trust mechanism that is built on collaborative filtering and variable weight fuzzy algorithms. First, three types of trust evidence—communication-based, data-based, and energy-based evidence—are used as indicators. Next, the variable weight fuzzy comprehensive evaluation algorithm is applied to calculate a node's direct trust value. Afterwards, the node's degree of honesty is defined to quantify its ability to be honest. Then, the proposed collaborative filtering algorithm is used to determine the node's overall recommended trust value. Simulation results show that the proposed mechanism can filter out unreliable recommendations and improve the trust model's recognition rate and stability in typical attack scenarios.

TABLE 7. Summary of ML-based techniques for physical layer authentication.

Ref.	Objective	ML Method	Contribution	Results
[102] [103]	Physical Layer Authentication	Unsupervised Learning	Utilized neural networks to distinguish between legitimate and fake transmissions in the absence of a reliable statistical model.	
[104]		LSTM	Proposed an LSTM-based feature extraction strategy using a sensor array, enabling continuous tracking of channel features without requiring explicit knowledge of transmitter movements	The proposed protocol is capable of detecting both naive attacks and more advanced attacks
[105]		RL	Proposed an RL-based authentication scheme for spoofing detection, and extended it with a deep Q-network-based authentication scheme to enhance accuracy for sinks supporting deep learning	Their scheme enhanced spoofing detection accuracy and network utility when compared to the Q-learning-based approach in [110], [111].
[106]		SVM	Proposed a PLA strategy that utilizes spatial dependency in CIRs and employs two database-correlative features to characterize CIR patterns	Enhanced enhancing node authentication accuracy while considering bandwidth and energy constraint.

It is important to note that while traditional trust models are beneficial, they face scalability challenges in the context of mobile underwater devices, heterogeneous network environments, and variable attack patterns [117].

C. JAMMING PREVENTION

The authors of [118] propose an RL-based anti-jamming power control method for dynamic underwater environments that enables each sensor to choose its transmit power without knowing the jammer's channel gain. However, this method performed worse in terms of learning speed, SINR, BER, and overall utility than the deep Q-network-based scheme that is proposed in [119]. Moreover, Xiao et al. [120] propose an RL-based anti-jamming relay scheme that optimizes relay mobility and power allocation without requiring knowledge of the underwater channel model or the jamming model. They also propose a DRL-based relay scheme that further enhances the relay performance of nodes that support deep-learning (DL) computations. In [121], the authors approach the interference communication problem as an ordinal potential game model. To solve the game, they propose a DRL-based optimal anti-interference transmission strategy that is learned from historical information using the deep deterministic policy gradient algorithm. Simulation results demonstrate that the proposed algorithm can significantly reduce network interference while meeting node bandwidth requirements. The authors of [122] introduce an RL-based unmanned aerial vehicle (UAV)-aided scheme to optimize both the relay power and trajectory of UAVs. Optimization relies on factors such as the BER of maritime messages, the received power, and the UAV's location. The scheme is designed for ship-to-ship anti-jamming communication in complex and dynamic maritime environments. Simulation results show the proposed scheme can increase communication utility, save energy, and reduce the BER more than the benchmark Q-learning-based relay (QLR) scheme.

D. PRIVACY-PRESERVING LOCALIZATION

The authors of [124] investigate a privacy-preserving localization challenge in UASNs and propose to address it by employing DRL. Their study considers unsupervised, supervised, and semi-supervised scenarios. For each scenario, the authors devise localization estimators using DRL techniques to precisely obtain the locations of sensor nodes.

E. OPEN ISSUES FOR INTEGRATING ML-BASED TECHNIQUES IN IOUT SECURITY

The aforementioned ML-based techniques evidently address some of the main concerns regarding information sensing and processing, latency, reliability, fault tolerance, and efficiency [125]. However, some challenges hinder the broad employment of ML algorithms in IoUT networks. These include:

- *Data quality:* Network issues may result in losing a substantial volume of data. Moreover, external noise could get added to the data and reduce the quality of the data that is needed to train the ML algorithms.
- *Data handling:* IoUT sensors/devices quickly generate massive amounts of data. It is very challenging to label and handle said data in real time.
- *Latency:* The training of classic ML algorithms involves aggregating data from all the sensors/devices in the central cloud, which increases latency and introduces considerable communication costs.
- *Privacy preservation:* The sensitive information collected from many types of autonomous vehicles, like submarines, needs to be kept private to avoid serious consequences. The classic ML approach involves transferring collected data to a central cloud for further processing. Malicious users can take advantage of this situation and try to acquire sensitive information during the transmission or storage phases.

Given the above challenges, FL has emerged as a transformative force for securing communication and

TABLE 8. Summary of ML-based techniques for trust management.

Ref.	Objective	ML Method	Contribution	Results
[107]	Trust Management	SVM	Incorporated multiple trust factors, including Communication Trust, Packet Trust, and Energy Trust	Superior performance in a sparse deployment environment, particularly in terms of detecting malicious nodes, ensuring a high success rate of communication, and extending network lifetime compared to Group-based, multidimensional trust metrics, and cloud-based trust models
[108]		SVM	Proposed a trust redemption process based on historical performance and environmental influence	Achieves superior performance in malicious detection and reduces the possibility of misjudgment of normal nodes compared to [107]
[109], [112]		RL	Introduces a three-phase model that include quantified environment model, an RL-based trust update model, and trust redemption model to reinstate low trust sensor nodes and improve network resource utilization.	Achieves highly efficient trust updating in the presence of changing attack modes
[113]		LSTM	Designed a defective recommendation filtering method to enhance trust recommendation accuracy among nodes, and implemented an adaptive trust model based on LSTM network to identify anomalous nodes and evaluate their trust value.	Demonstrated the effectiveness of the LTrust model under both hybrid attack and single-mode attack scenarios, and Outperformed other approaches in terms of trust value, accuracy, and error rate. Highlighting the significance of considering the relative importance of different nodes within the network topology for more accurate trust evaluation.
[114]		SVM	Proposed a trust mechanism that utilized three trust indicators (communication-based, data-based, and energy-based evidence) to enhance assessment. Applied a variable weight fuzzy comprehensive evaluation algorithm for calculating direct trust, considering multiple indicators. Introduced honesty degree to quantify nodes' honesty ability.	The proposed model effectively filtered out unreliable recommendations, improving the recognition rate and stability of the trust model under typical attack scenarios in UASNs.
[115]		SVM	Introduced a compressive sensing-based homomorphism encryption and trust scheme. Leveraged SVM to train a trust model, enabling nodes to identify malicious attacks.	Security analysis demonstrated that the proposed model effectively ensures data confidentiality and identifies malicious nodes, enhancing overall network security.
[116]		SVM	Proposed a trust-based malicious identification scheme that quantifies the impact of the underwater environment on communication trust. Leveraged communication traffic to identify abnormal packet transmission or reception behaviors, focusing on mitigating DOS attacks. Employed SVM and K-means++ algorithms to train a prediction model for malicious node identification.	The model effectively identifies malicious nodes in complex underwater environments, outperforming three other identification schemes, with performance improvement particularly noticeable in scenarios with higher rates of malicious nodes.
[116]		SVM	Proposed a trust-based malicious identification scheme that quantifies the impact of the underwater environment on communication trust. Leveraged communication traffic to identify abnormal packet transmission or reception behaviors, focusing on mitigating DOS attacks. Employed SVM and K-means++ algorithms to train a prediction model for malicious node identification.	The model effectively identifies malicious nodes in complex underwater environments, outperforming three other identification schemes, with performance improvement particularly noticeable in scenarios with higher rates of malicious nodes.

decision-making processes in various and critical underwater scenarios, which we discuss in the next section.

VII. FL FOR IOUT SECURITY

FL is a secure, collaborative, and decentralized ML framework that has great potential for realizing a secure and efficient IoUT framework. In an FL-based IoUT framework, all the nodes in the network train their subsequent sub-models independently. Moreover, all the nodes interact only with the encrypted sub-model parameters alongside the fusion node to achieve an integrated global ML model [126]. In an FL-based IoUT framework, communication overhead is reduced and optimal security is ensured by effectively mining large-scale datasets. The fundamental rule of FL, offloading

TABLE 9. Summary of ML-based techniques for anti-jamming and privacy-preserving localization.

Ref.	Objective	ML Tool	Contribution	Results
[118]	Anti-Jamming	RL	Formulated the interactions between an underwater sensor network and a reactive jammer as two jamming games. The Nash Equilibrium was derived for the one-shot jamming scenarios with known channel gains and transmission costs.	Simulations have shown the efficacy of the proposed anti-jamming power control strategy.
[119]		Deep Q-Network	Proposed an anti-jamming underwater transmission framework that applies RL to control the transmit power and use the transducer mobility to address jamming in underwater acoustic networks.	Experimental results show that the proposed scheme can reduce the bit error rate of the underwater transmission against reactive jamming compared with the Q-learning-based scheme.
[120]		DRL	Proposed an DRL-based relay scheme to help a UWSN resist jamming, which optimized the relay mobility and power allocation without being aware of the underwater channel model and the jamming model.	The experimental results have shown that the proposed relay scheme can reduce the BER, save energy consumption, and increase the utility compared to a benchmark scheme QLR. The deep-RL-based relay scheme further improved the relay performance with an increased computation overhead.
[121]		DRL	The paper has studied the interference communication problem as an ordinal potential game model. To solve the problem, the paper has proposed a DRL-based anti-interference transmission strategy, specifically, an optimal anti-interference transmission strategy learned from historical information using the deep deterministic policy gradient algorithm.	The simulation results have demonstrated that the proposed algorithm can significantly reduce network interference while meeting node bandwidth requirements. The training time of the method is also analyzed for different network sizes, and the results have shown that the proposed method can be adapted to networks of different sizes and does not increase the additional training time.
[122]		DQR	Introduces an RL-based UAV-aided scheme to optimize both the UAV relay power and trajectory. The scheme is designed for ship-to-ship anti-jamming communication within complex and dynamic maritime environments. Additionally, the paper offers performance bounds based on the Nash Equilibrium of the anti-jamming game and addresses computational complexity.	The simulation results have verified that the efficacy of the proposed schemes can increase utility, save energy, and reduce BER compared with the benchmark QLR scheme.
[123]	Privacy-Preserving Localization	DRL	Proposed a novel model to minimize the sum of all measurement errors, where a ray compensation strategy is incorporated to remove the localization bias from assuming the straight-line transmission. The paper has considered the unsupervised, supervised, and semisupervised scenarios, through which DRL-based localization estimators are utilized to estimate the positions of sensor nodes.	The numerical results have shown that the private position information can be hidden, while the localization accuracy can be enhanced as compared with the other existing works. Moreover, which is more importantly, the model is robust to local optimum for nonconvex and non-smooth localization problem in inhomogeneous underwater medium.

computation to local devices, can solve the previously discussed challenges that are associated with traditional ML approaches. For instance, the authors of [117] propose a trust model that is based on federated DRL. Their approach improves the evidence acquisition mechanism to better accommodate the topological dynamics of UASNs, employs DRL for trust modeling, and implements FL to periodically aggregate and update local models. Simulation results demonstrate it improves the adaptability and scalability in the face of spatio-temporal changes. The following points summarize the motivation for integrating FL in underwater scenarios [125]:

- It handles noisy data better than conventional ML algorithms do.
- It is able to preserve the privacy of sensitive IoUT device data.
- It minimizes the likelihood of data quality issues when the massive volumes of data that are generated by IoUT sensors/devices are transmitted to the cloud.
- It reduces the communication costs and latency involved in data transmission.

In what follows, we discuss in detail the significance of FL from the perspective of security in IoUT networks and focus specifically on its practical applications.

A. UNDERWATER EXPLORATION

Underwater (UW) exploration involves examining the physical, chemical, and biological conditions of the UW

environment for commercial or scientific purposes. This exploration typically employs various technologies, including satellites, buoys, gears, and underwater vehicles. Such activities facilitate the discovery of hidden natural resources and lost treasures, the assessment of fish population density, and the tracking of underwater objects. Privacy concerns, such as device privacy, location privacy, and data privacy, are critical in these scenarios. FL can play a significant role in preserving data privacy by training data locally rather than sharing it with a centralized server. This approach reduces the risk of data breaches and ensures that sensitive information, such as the location of underwater vehicles or collected environmental data, remains confidential. FL enhances security through techniques like secure aggregation, which encrypts individual model updates and combines them to prevent the server or any third party from inferring the original data. Additionally, FL can employ differential privacy, which introduces noise to the model updates, further safeguarding sensitive information. This unique attribute of FL makes it a better choice in this context than classic ML [125].

Recently, Zhao et al. [127] presented a "federated meta-learning enhanced acoustic radio cooperative framework" termed ARC/FML to intelligently use the data gathered from distributed sources like buoy nodes. Their ARC/FML technique facilitates the sharing of data across the water–air interface. It can also be used to share sensitive information related to underwater exploration. The authors used DeepSink and an RF channel dataset to experimentally test the proposed model, and it achieved 97% accuracy.

Similarly, Qin et al. [128] propose a novel edge computing framework that combines FL and blockchain technology to address security concerns in marine IoT systems. Their implementation suggests ways to simulate malicious workers in FL. To measure the quality and reputation of FL workers and, in turn, improve security and efficiency, the authors employed the triple subjective logic model to calculate a node's reputation value from its geographical location, interaction time, and interaction effect. They limited the number of nodes to avoid resource wastage. Furthermore, they designed a consensus method to act as a proof of quality (PoQ) mechanism. The PoQ mechanism is used by task publishers when adding blocks. It helps task publishers select workers with better parameters for addition to the blockchain.

Finally, the authors developed a novel environmental model for solving data security issues in marine environments. They first tested it with a 20% attack intensity, and FL to 0.092. Then, they increased the attack intensity to 80% and obtained a loss function of 0.0195. However, since UW exploration and the collection of UW information are economically important, massive research prospects are expected in this domain.

B. DISASTER PREVENTION AND MITIGATION

The UW environment is always at risk of natural disasters, such as tropical storms, hurricanes, and tsunamis, as well as man-made disasters. For instance, the 2004 Indian Ocean earthquake and subsequent tsunami were among the deadliest natural disasters in recorded history. Man-made disasters generally include illegal dumping, substance and poisonous gas leaks, and oil spills. FL-based solutions can significantly aid in disaster prevention by enabling real-time monitoring of the UW environment. Deploying various devices, such as UUVs, cameras, and sensors, at multiple locations simultaneously allows continuous data collection from the UW environment. FL schemes enhance security in such scenarios by ensuring that sensitive data remains localized, with only model parameters being transmitted. This reduces the attack surface and minimizes the risk of data interception during transmission. Additionally, FL improves resilience against potential adversarial attacks, such as data poisoning or model inversion, by aggregating model updates from multiple devices, making it more difficult for an attacker to compromise the overall system. Techniques like secure multi-party computation (SMPC) and homomorphic encryption can be integrated into FL frameworks to further protect data integrity and confidentiality during the aggregation process. Consequently, FL schemes are very useful in UW disaster prevention as they preserve data privacy and improve the scalability, security, and overall performance of the monitoring system [125].

C. MARITIME TRANSPORTATION SYSTEMS

Applications for FL are being found in several privacy-sensitive sectors that rely on distributed data storage [129]. Very recently, Liu et al. [130] proposed to apply FL to an IoT-based maritime transportation system (MTS) to ensure data privacy during detection model training. However, the irrational subsea communication environment and differences in hardware performance due to device heterogeneity led to a particular problem named the straggler problem, in which FL participants often fail to upload their model parameters for timely model aggregation. Moreover, interference in wireless communication and long training phases can also cause stragglers during FL in MTSs. The straggler problem leads to most FL participants being absent during a few aggregation rounds, which increases the aggregated global model's variance. The model's convergence is hindered in such circumstances, which can lead to the entire FL process failing. This problem is particularly crucial for IoT-based MTSs, for which security and stability are very important.

The authors present a novel multi-layer perception (MLP) and CNN-based model named FedBatch to detect intrusions and address the above-mentioned concerns. FL is employed to train the proposed model. When it comes to each vessel's local detection model, MLP is utilized to classify the attacks, and the CNN is responsible for data feature extraction. Internally, the raw high-dimensional data is transformed into 2D form during data processing to fit the CNN input. After that, an improved FL approach is designed that takes into consideration the attributes of the IoT-based MTS. The authors propose to mitigate the straggler problem by

dynamically adjusting the global model reservation using the batch federated aggregation algorithm. The authors evaluated the efficiency of FedBatch and the efficacy of their MLP and CNN-based local model on the NSL-KDD dataset.

D. INTERNET OF SHIPS

The recent introduction of IoT technologies in the marine sector has led to the launch of a new paradigm: the Internet of Ships (IoS). Lately, several DL-based fault diagnosis mechanisms have been presented that leverage DL and the IoS concept to enhance shipping companies' maintenance performance and minimize their operating expenses. However, the conventional centralized learning (CL) scheme, wherein the different shipping companies' data resources are centralized on a cloud server to train the model, is restricted in real industrial scenarios due to business competition and privacy concerns.

Zhang et al. [131] recently introduced a new scheme named adaptive privacy-preserving FL (AdaPFL) to diagnose faults in the IoS. It facilitates organizing various shipping agents for cooperative model development by enabling model parameter sharing without any risk of data leakage. Initially, the authors use two tasks as an example to show that some model parameters may reveal the shipping agent's raw data. Then, in light of this, they propose a Paillier-based communication mechanism to preserve the privacy of the shipping agents' raw data. Moreover, they propose a control algorithm to handle harsh UW environments by adaptively changing the interval of model aggregation during training to reduce communication costs and cryptography computation. Their experimental results and theoretical analysis show that the proposed AdaPFL approach achieved all the targets defined for diagnosing a fault in the IoS. However, this work could be extended to improve the FL convergence speed. Designing and deploying a main FL distribution scheme in real maritime scenarios are other possible directions for extending this study.

E. MILITARY

Naval defense activities involve surveillance, recovery operations, mine warfare, and submarine detection. Conventionally, humans in UW vessels carry out these activities. However, with the rapid technological advancements, UWSNs have been established as the revolutionary communication infrastructure that can facilitate UW activities without human involvement. These sensors identify and categorize the subjects of interest in the marine environment. The US Navy stresses the capability of their onshore intelligence, drones, submarines, and ships to share data in real-time [132]. The successful deployment of multi-domain operations (MDOs) is majorly hindered by a lack of effectual data leveraging tools. ML- and AI-based schemes may be able to handle massive amounts of data, accommodate uncertainty, reduce manpower requirements, increase action speed, and enhance data analytics for improved decision-making. FL, in particular, is a collaborative training method that does not involve exchanging training data with edge devices, which enables it to overcome the coalition, security, and policy constraints that are associated with sharing training data. In [133], the authors present an FL-based approach for deploying MDOs to address the problems discussed above.

F. NAVIGATION AND LOCALIZATION

State-of-the-art localization and navigation technologies are essential for UW exploration. UW sensors may float freely with the water currents or be anchored to the ocean floor. The information gathered from sensors is only helpful if the location of the sensors can be precisely identified. Sensor positions can also serve as reference points for explorers, divers, swimmers, and other smart objects. Accurate location identification is crucial for tracking and source detection applications.

Conventional localization protocols are often unsuitable for UW applications due to the unique nature of the UW channel. Currently, UW navigation and positioning are critical issues for IoUT. Wormhole, black hole, and Sybil attacks are primary threats that target and alter localization details produced by underwater sensor networks. FL addresses these security challenges by enabling decentralized training of localization models directly on the sensors without sharing sensitive location data with a central server. This approach significantly reduces the risk of data interception or manipulation by adversaries during transmission. Additionally, FL can incorporate secure aggregation techniques, ensuring that even if model updates are intercepted, the underlying data remains confidential. FL also enhances system resilience against these attacks by aggregating updates from multiple sensors, which dilutes the impact of any compromised or malicious sensor, maintaining the integrity and accuracy of the localization information. Moreover, FL's ability to adapt to real-time and streaming UW data makes it an ideal choice for secure and reliable navigation and localization in IoUT environments [125].

G. UAV-BASED MARITIME COMMUNICATION

Maritime communication (MCN) aims to support several applications, including search and rescue (SAR) operations, marine tourism, pollution monitoring, ocean exploration, and trade [134]. The MCN ecosystem relies upon a heterogeneous mix of actuators, sensors, unmanned underwater vehicles (UUVs), unmanned surface vehicles (USVs), platforms, buoys, and vessels [135]. Integrating UAVs in MCN systems can substantially improve reliability, coverage, and deployment flexibility, as well as reduce delays. Secure UAV-assisted communication systems are necessary to overcome various types of attacks aimed at compromising the security of critical infrastructure and the reliability of communication [136]. When it comes to UAV-based maritime communications, disturbances in the UAVs' transmissions by means of identity forging might not be easily identified, particularly in UAV swarm networks. Therefore, UAVs must

be authenticated, and the data received must be scrutinized, which could potentially lead to delays in performance [137].

FL can also enhance the security of UAV-assisted MCNs by enabling decentralized model training directly on UAVs, thereby eliminating the need to transmit raw data over potentially insecure channels. This approach mitigates the risk of eavesdropping and data interception by attackers. FL allows UAVs to collaboratively train a global model while keeping their local data secure, which is crucial in environments where sensitive information, such as navigation data or mission-critical communication, is at stake. The federated averaging algorithm used in FL aggregates the locally trained models from each UAV into a global model, ensuring that no individual UAV's data is directly exposed during the training process. Additionally, FL can be integrated with secure aggregation protocols and differential privacy techniques, adding layers of encryption and noise to the model updates, further safeguarding data from being reverse-engineered or exploited by adversaries.

FL also enhances the resilience of UAV swarms against various types of attacks, such as data injection or identity forging, common in complex MCN environments. By decentralizing the learning process, FL reduces the single point of failure typically present in centralized systems, making it harder for attackers to compromise the entire network. In the event of compromised UAVs, the influence of corrupted data on the global model is minimized, preserving the integrity and reliability of the overall system. FL's ability to operate in real-time with streaming data aligns with the dynamic nature of UAV-assisted MCN systems, ensuring that security measures are continuously updated and adaptive to new threats. This makes FL an ideal solution for enhancing the security of UAV-assisted maritime communications while maintaining high performance and responsiveness [138].

H. MARITIME SUPERVISORY CONTROL AND DATA ACQUISITION SECURITY

Information and communication technology continues to grow and is converging in several sectors, including the maritime industry. It is anticipated that maritime supervisory control and data acquisition (SCADA) security will be strengthened. Nevertheless, attack mitigation remains an open challenge in these areas of application. Maritime SCADA systems are sensitive and must be fully secured. Cyberattacks on maritime SCADA systems mainly result in catastrophic breakdowns in maritime operations and service disruptions. Therefore, developing efficient AI-based intrusion detection systems is pertinent to mitigate attacks.

FL can also play a pivotal role in enhancing the security of maritime SCADA systems by addressing key vulnerabilities inherent in traditional centralized approaches. In a typical SCADA system, data from various sensors and control points is transmitted to a central server for processing and analysis, which presents a single point of failure and a potential target for cyberattacks. FL mitigates this risk by enabling decentralized training of AI models directly on edge devices or within SCADA subsystems. This ensures that sensitive operational data remains localized, reducing the likelihood of interception during transmission. Additionally, FL can incorporate secure aggregation techniques, ensuring that individual model updates are encrypted before being sent to a central aggregator, further safeguarding data from exposure to attackers.

The distributed denial of service (DDoS) attack poses a significant threat to maritime SCADA networks, leading to network congestion and potentially crashing legitimate traffic by using fake source addresses associated with malicious networks [139]. Many studies have investigated using AI approaches to predict and detect attacks and vulnerabilities. When it comes to maritime SCADA security, in particular, most of the available literature focuses on cybersecurity training strategies, risk assessment analysis, and awareness creation [140], [141]. However, a lack of research attention has been paid to intrusion detection approaches. Federated Learning (FL) provides a robust solution for intrusion detection by allowing multiple SCADA nodes to collaboratively detect and respond to attacks in real time without sharing raw data. The FL-based framework proposed by Ahakonye et al. [142] for detecting and mitigating DDoS attacks in maritime SCADA networks is a prime example of this approach. FL's decentralized nature not only preserves data privacy but also reduces latency, which is crucial for real-time detection and response in maritime operations. Furthermore, FL can be coupled with techniques like differential privacy and homomorphic encryption to ensure that even the aggregated model updates remain secure, making it effective against sophisticated attacks like zero-day exploits. This approach's adaptability and security make FL an ideal solution for safeguarding maritime SCADA systems against a wide range of cyber threats.

I. PROTECTING THE PRIVACY OF MARITIME MULTI-AGENT COMMUNICATION

Due to its security and privacy-preserving guarantees, FL is an appropriate option for MCN systems that handle large amounts of distributed data. Traditional centralized learning approaches require the aggregation of raw data from various distributed sources, introducing significant privacy risks, particularly in sensitive maritime environments where data includes navigational, operational, and environmental information. FL mitigates these risks by enabling local model training directly on edge devices, ensuring that raw data never leaves the source. This decentralized approach is particularly advantageous in MCN systems, where heterogeneous devices, ranging from sensors on buoys to UAVs and UUVs, collect widely dispersed data under varying conditions. By keeping data localized, FL inherently reduces the attack surface for potential breaches, as there is no central repository of data that could be compromised by adversaries.

However, a maritime multi-agent communication system's dataset is different from a typical dataset, and its non-uniform

data distribution increases model variation, potentially affecting the global model's performance. The non-independently and identically distributed (non-IID) nature of maritime data, where different nodes may observe vastly different environments or operational states, introduces challenges in ensuring that the global model remains robust and effective. To address this, Han and Yang [143] proposed a part-FL (PFL) scheme that combines the benefits of split learning with traditional FL. In their approach, only a subset of local model parameters is uploaded to the cloud server as shared parameters, while other parts of the model remain localized. This hybrid strategy not only improves the processing performance of non-IID data by tailoring the model updates to the specific data characteristics observed at each node but also enhances privacy by limiting the amount of information shared across the network. Additionally, PFL reduces communication costs, which is particularly important in maritime environments where bandwidth may be limited and intermittent. By minimizing the communication overhead and selectively sharing model parameters, PFL enhances both the efficiency and security of the learning process in maritime multi-agent systems, making it a powerful tool for MCN systems dealing with distributed, sensitive data.

J. COOPERATIVE COLLISION AVOIDANCE FOR INLAND SHIPS

The cooperative avoidance of collisions between inland waterway ships is a service that is expected to be made possible by the Internet of Ships (IoS). This service is intended to ensure safe navigation by optimizing the trajectory of a ship. For successful deployment, accurate and on-time ship position prediction with real-time reactions is required to predict and prevent collisions. Advanced ML techniques are typically used to predict ship location. Traditional ML approaches, however, involve centralized data processing, often by a cloud data center managed by a third party. While effective in some scenarios, such centralized schemes are unsuitable for collision avoidance services in the maritime domain because they expose ships' positioning data to potential breaches. Centralized processing increases the risk of sensitive data being accessed by unauthorized third parties or even by other connected ships, which could compromise operational security and privacy.

FL can also address security concerns in maritime environments by enabling decentralized model training directly on ships or at edge computing nodes, ensuring that sensitive positioning data remains local and is not shared across the network. The FL-based cooperative collision avoidance system proposed by Hammedi et al. exemplifies this approach. In this system, ships collaboratively build a shared positioning prediction model without exchanging raw data, preserving the privacy of their sensitive location information. Deploying FL at the Multi-access Edge Computing (MEC) level further enhances security by supporting low-latency communication, which is critical for timely collision avoidance responses. Moreover, the use of smart contracts and blockchain technology ensures that communications between MEC nodes and ships are authentic and reliable, adding an additional layer of security against tampering or unauthorized data access. By incorporating these technologies, the proposed system maintains the confidentiality of ship data and ensures secure communication channels, making it a robust solution for real-time collision avoidance in inland waterway navigation. Simulation results from the generated dataset depicting ship mobility in France demonstrate the system's effectiveness in ensuring reliable, timely communication and secure collision avoidance between ships.

VIII. CHALLENGES, OPEN ISSUES, AND FUTURE DIRECTIONS FOR INTEGRATING FL IN IOUT

The integration of FL approaches in different applications in underwater settings has been found to show promising results, as discussed previously. However, numerous challenges hinder the deployment of FL in UW scenarios. This section discusses various challenges that are faced when integrating FL techniques in the IoUT, as well as open research issues, and potential solutions for those issues.

A. NETWORK/DEVICE CONFIGURATION

Network/device configuration is necessary when FL is deployed over the network edge. In UW networks, the network configuration is notably complex due to the nodes' mobility, which leads to a disturbance in node connectivity. This disturbance happens because of numerous factors, including the Doppler shift, the multipath effect, noise, and path loss. Edge devices have several constraints, such as limited battery, computational, and storage capacity. Thus, lightweight models with auto/self-configuration mechanisms should be devised to enable FL in the IoUT. In addition, co-designing algorithms and hardware may prove to be very helpful [125].

B. DATA TRANSMISSION

Data transmission is considerably different in the UW environment than in the terrestrial environment. One major issue is the low-frequency range in which signals must be transmitted to avoid being hindered by the water. Because of the long transmission range of acoustic communications, the chance of collision and interference is very high. It becomes a particularly big challenge when FL is deployed in the IoUT since synchronous updating is performed on the server side, and FL requires data from all clients, including the slowest one, to be sent to the server in order to perform aggregation. Nevertheless, because of the customary UW environmental attributes and the transmission, availability, and connectivity issues, there is a strong need for promising solutions to enable FL in the IoUT. Using asynchronous updating on the server end could be a potential approach [147].

TABLE 10. Summary of FL-based techniques for IoUT security.

Ref.	Contributions	Results	Future Direction
[127]	Proposed a novel ARC/FML scheme for securely sharing the sensitive information related to underwater exploration	The proposed C-DNN offers less complexity and improved BER performance compared to the traditional matched filter (MF) and provides better convergence compared to the classic FL under various channels	The current design is for IoT device only, which might be extended to the IoUT scenario by employing UW unmanned submarine vehicle so as to utilize the distributed data to accelerate the learning process further
[128]	Proposed a novel blockchain technology and FL-based edge computing framework for efficiently handling the security concerns in the MIoT systems	The simulation results proved that the proposed mechanism could considerably increase learning accuracy while guaranteeing the reliability and safety of the marine environments	Some novel programs need to be designed for optimizing the number of workers to reduce the high costs linked to large numbers of workers taking part in FL There could be more research on dynamically changing reputation thresholds to reduce the negative influence of malicious workers
[144]	Employed federated DRL for achieving reliable transmission of model parameters in an IoUT network Formulated and solved a joint resource allocation and cell association problem to train the network for capturing unpredictable environmental conditions	The results showed that the proposed algorithm achieved 41% and 80% improvement in performance, in terms of downlink throughput, compared to the DDPG and standard actor-critic respectively	To implement the proposed MADDPG-based multi-agent DRL algorithm in real-world settings, considering FL-specific applications and dataset More measurement metrics can be used for the data-intensive, measurement-based performance evaluations
[130]	Presented a novel CNN-MLP based intrusion detection model, named FedBatch, for IoT-based Marine transportation system, which is trained via FL	The simulation results on NSL-KDD dataset depicted the efficacy of the proposed model in detecting intrusion. The experiments using both non-IID and IID dataset showed that FedBatch effectively improved the training stability and model accuracy	....
[131]	An adaptive, FL-based privacy-preserving scheme, termed AdaPFL, to detect faults in internet of ships. The proposed approach can manage several shipping agents to collectively develop a model through model parameters sharing without any data leakage risk	The experimental results along with theoretical analysis verified the efficiency of AdaPFL on a real non-IID fault data set	Designing and deployment of a key FL distribution scheme in real ship scenariosTo improve the convergence speed of FL
[142]	An FL Framework to detect and mitigate DDoS attacks on Maritime-SCADA Networks	The results validated the feasibility and significance of the proposed approach in DDoS attack detection and mitigation	Evaluation of the proposed framework utilizing Maritime-SCADA datasets
[145]	A novel framework based on Federated Region-Learning to simultaneously solve the model performance and computational efficiency issues	The proposed approach enhances computational efficiency and accuracy compared to normal FL and centralized training mode	Integration of incremental learning into FRL for achieving dynamic model training and reduced calculations
[143]	A new approach for addressing the privacy protection and multi-agent cooperation issues in maritime communication systems having massive volumes of scattered data	This work reasoned out the best proportion information security overhead and distributed communication overhead Achieved remarkable reduction in computation delay and communication cost	.....
[146]	Exploited the state-of-the-art concepts including federated deep learning, Blockchain technology, and MEC to devise a novel collision detection and avoidance system between IoS	Protected sensitive data of ships from getting leaked and achieved high communication efficiency Achieved more than 92% accurate collision detection rate in different scenarios	Integration of other information sources, like Lidars, for ensuring more inclusive sensing capabilities of the ships Computing resources optimization at the MEC hosts

C. UNRELIABLE CHANNEL CONDITIONS

Various factors, such as transmission delays, node mobility, channel noise, and bandwidth limitations, may lead to unreliable channel conditions in a UW environment. Communication bottlenecks have been found to be a big challenge when deploying FL in a UW setting and make it difficult for clients to share local updates with the centralized server. Furthermore, handling the dynamic changes that

occur in IoUT networks is another area in which bottlenecks are observed since the topology itself could change with time because of node mobility. One possible research direction is to devise optimization techniques to deploy FL in IoUT settings. Moreover, aggregation frameworks and gradient compression schemes focused on resource efficiency and effective communication could be employed to handle bandwidth-related problems.

D. SYSTEM HETEROGENEITY

The primary software and hardware systems that are used in an IoUT environment are different from those used in a terrestrial IoT environment in various respects. This leads to system design issues because of the variety of dimensions and data formats involved, and the need to rely on asynchronous communication. Deploying FL schemes in UW environments involves managing heterogeneous devices and their capabilities, with load distributed among devices depending on their availability. Moreover, frameworks that support system heterogeneity could be used here, which would facilitate arriving at a global reference model.

E. PRIVACY

In IoUT environments, the sensor nodes are sparsely deployed, which makes it very difficult to manage privacy. These environments are, therefore, considered to be sensitive and complex. In the context of IoUT, the term "privacy" has a broader sense and covers location, device, and data privacy. Hence, robust privacy-preserving solutions are a must in IoUT networks. FL approaches help to address trust-related concerns. However, FL has certain privacy limitations, such as the need to reconstruct user data from gradient information [148]. Various types of attacks, such as model inversion, can be used to reconstruct images gathered from the IoUT environment. Addressing privacy-related problems in privacy-enabled settings is an open research challenge. Implementing lightweight and secure protocols could be a possible solution [125].

F. REAL-TIME LABEL GENERATION

Class label generation is necessary to apply supervised learning schemes to a dataset. However, real-time label generation is a tedious and time-consuming task in the IoUT. This issue could be addressed by applying unsupervised learning approaches instead, which do not require class label generation. Automated tools could also be used to generate labels in real-time.

IX. DIGITAL TWIN FOR IOUT SECURITY

The security of underwater wireless communication has become a key concern since marine operations are moving towards employing heterogeneous robotic assets and because securing digital systems is becoming challenging across all areas [149].

Recently, DT technology gained considerable research attention in the marine industry. A DT is a virtual model that captures the behavior and state of an actual asset, e.g., a fish farm, an offshore wind turbine, a semisubmersible, or a ship, from sensor inputs, in near real-time. The resolution of the virtual model could be dependent on physics such as fluid mechanics and structural mechanics, or ML and artificial intelligence. A DT is an extension of model analysis and engineering simulation; however, state rendering and analogous performance are derived from real-time sensor observations instead of load estimates [150].

In the marine industry, DT is usually implemented as a complement to other digital asset technologies, such as finite element analysis (FEA), computational fluid dynamics (CFD), product life cycle models, advanced analysis models, ML, and big data. These technologies are not considered alternatives, but instead regarded as complementary technologies that can be combined to gain insights into the modeling and operations of marine systems. Erikstad [150] presented a set of DT design patterns in maritime systems, which is considered a crucial step toward the maturation of this domain. DTs can be used to fulfill a broad range of requirements. As a result, the preferred solution may differ from one case to the next. Design patterns can help to capture the commonalities among alternative implementations, and may reveal the differences as well. Erikstad [150] limited their work to explaining the structural patterns in depth and highlighting potential research topics (Fig. 3) that could be important for society and the marine industry in the coming years.

In what follows, we describe in detail the importance of DT for IoUT security.

A. ADDRESSING CYBERSECURITY THREATS

DTs can be used to address high-level concerns regarding cybersecurity risks owing to increasing cyber-physical systems and connectivity requirements. Corporate operational technology (OT) and information technology (IT) systems are being exposed to ever more external devices and networks through the industrial Internet of Things (IIoT) and as more and more assets become remotely maintained, controlled, and supervised. In a 2017 report, DNV GL (the pioneer in cybersecurity services) [151] claimed that the DTs it had developed were capable of managing both the internal cybersecurity threats that are inherent in integrated systems because of their emergent properties and complexity and external cybersecurity risks like intentional cyberattacks. They focused on early risk management to identify potential threats before they become evident during the development and operation phases. Hence, only an organized approach that is combined with simulation-based examination and verification would provide a viable solution.

The Head of Marine Cybernetics Advisory in DNV GL's Maritime Advisory Group stated that, "DNV GL's proposition is completely novel in the marine industry. The leap in ambition is the combination of a DT for system integration and testing with insights from sensor data. This will propel the industry into a future where model-based

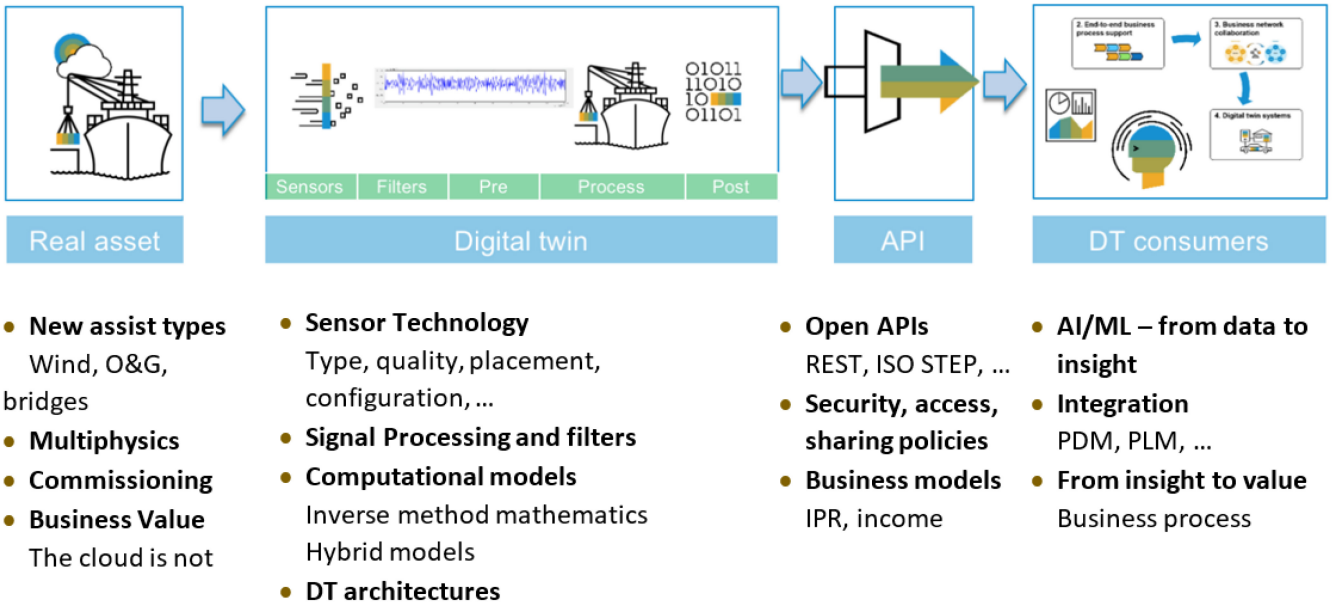

FIGURE 3. Potential Research Areas for Digital Twin Technology [150].

simulation, data analytics, and visualization software connect in the cloud with data from physical sensors" [151].

B. ANTI-SUBMARINE WARFARE

Submarines are a major combat force in modern marine warfare and the main threat to naval security. The security threats that are associated with submarines make it vitally important to find effective anti-submarine warfare (ASW) methods. ASW is a type of warfare that relies upon submarines, aircraft, or surface warships to fight enemy submarines. Quickly identifying and localizing as many enemy submarines as possible is a fundamental component of ASW.

The technology that is the most vital to successful ASW is sensor control. Hence, researchers in anti-submarine warfare must focus on upgrading online sensor control mechanisms. Several studies have looked into applying simulation-based methods with naval warfare research; however, only a few approaches are able to efficiently combine real ASW with simulation technologies in real-time.

In [152], Wang et al. proposed a novel framework to control sensors in ASW by integrating RFSs and DT theory. The authors present two key algorithms to support their DT-based framework. Firstly, an RFS-based data assimilation algorithm is presented to assimilate the chain of real-time measurements with clutter, noise, data association uncertainty, and detection uncertainty online. Secondly, the outcome of the proposed data assimilation algorithm is used to compute the reward function, which is introduced to find the optimum solution. The proposed mechanism's effectiveness and feasibility were successfully verified by experimental results. The proposed data assimilation algorithm can overcome the shortcomings of classic vector-based algorithms. It is also able to jointly estimate the number of enemy submarines and their respective states.

Wang et al. [152] used the identical twin experiment to evaluate the proposed algorithm. Their results showed that the algorithm assimilates input measurements and improves the accuracy of simulation results. The authors used two different scenarios, i.e., one with multiple submarines and the other with a single submarine, when conducting their experiments to evaluate the proposed sensor control mechanism. Their results proved that the proposed method could effectively control the sensor.

C. INTELLIGENT AND SECURE MTS

In [153], Liu et al. investigate DT-based security improvement in MTSs with the intent to promote the development of intelligent digital maritime transportation. First, the authors obtained and preprocessed chronological transportation data from the Maritime Silk Road since the operational security of the existing MTS is not fully matured. Next, they introduced DTs and incorporated relay nodes into the data transmission paths to construct an IoT-based cooperative relay maritime transportation DT model. Lastly, they conducted simulation experiments to verify the model's security performance.

Their relay security analysis showed that interference information plays a crucial role in safeguarding against information disclosure. Utilizing this information, the proposed model can harvest energy, thereby increasing the data transmission power and enhancing the secrecy rate and communication performance. Moreover, their outage probability analysis showed that the theoretical and simulated results are almost similar. As the system utilizes multiple multi-hop paths in the same environment, an increase in the fading index and the number of relays will lead to lower outage probability and better system performance. The node

secrecy rate attains an optimum value and cannot put undue load on the system when the iterations reach a particular count. Furthermore, a new power distribution equilibrium may be established when the nodes are at different positions to enhance the system's security performance. To summarize, the proposed maritime transportation DT model demonstrated exceptional security and transmission performance and provided an experimental foundation for secure and intelligent marine transportation in the years to come.

However, this study has some limitations. The proposed model contains just one relay and does not consider multi-relay cooperative communication. A single relay can improve system performance only to a limited extent. Nevertheless, the collaboration of multiple relays presents promising application scenarios, particularly in meeting future ultra-high-speed requirements. Thus, a potential avenue for future work could be to combine multi-relay cooperation and relay selection to determine the optimal relay cooperation number or the optimal relay cooperation method to enhance MTS performance.

D. RELIABLE SHIP NAVIGATION PREDICTION

Presently, several countries all across the globe are making groundbreaking research developments in the domain of UWSNs. Some of these projects include CommsNet (Australia), SUNRISE (Europe), Ocean-TUNE (US), and Seaweb (US Navy). These projects have added a lot of understanding to underwater research experiments and attempted to include mobile nodes like AUVs in the networks to obtain satisfactory results. However, there is currently no work that addresses completely self-organized UW mobile cluster networking.

Sufficiently intelligent nodes are the key to achieving unmanned mobile cluster networking, which needs a lot of intelligent algorithm support. Moreover, apart from the intelligence of the clusters, a chain of complicated problems pertaining to network performance must also be considered when conducting research on underwater mobile clusters. With this in mind, Lv et al. [154] explored a marine monitoring network and discussed the network coverage and information transmission methods that are employed in UWSNs. They used sensor nodes as agents and put forward a multiple-access approach that relies on the propagation attributes of UW acoustic signals and utilizes the network node game's power allocation strategy. The authors also presented a reliable UW data transmission protocol for enhancing the robustness and reliability of UW data transmission and conducted simulation experiments to verify its performance. Lastly, they employed physical model-driven and data-driven methods to generate DTs for ship navigation prediction. This paper's fairly systematic research makes up for the lack of information transmission efficiency in the domain of UWSNs. Consequently, it supports the development and enhancement of marine integrated communication network (MICN) systems.

E. BETTER MONITORING OF UNDERWATER OPERATIONS

Advancements in AI technology have substantially enhanced the autonomous monitoring capability of undersea equipment. An autonomous underwater glider (AUG) is a modern energy-efficient marine device that can conduct long-range oceanic investigations. Nevertheless, the communication failures, time delays, power constraints, and other unpleasant elements that are unavoidable in a UW environment have made monitoring the UW operations of multi-AUG systems quite challenging.

Monitoring the cooperative UW operations of multiple AUGs becomes very difficult due to the weakness of the marine communication environment. In [155], Wen et al. established a DT system that is based on the pilot mode for multi-AUG group collaboration, wherein the digital and physical worlds are connected by creating a digital model of an AUG response that incorporates sea tides. For the control model, an AUG behavior design-based artificial field approach is proposed to solve the local optimal problem. The results obtained show that the proposed method successfully controlled the AUG group's collaboration in leader mode and addressed the issue of the AUG falling into the local optimum path.

F. BETTER SAFETY AND MONITORING OF SUBSEA ASSETS

Digital subsea integrity management (SIM) solutions, rely on data to perform several routine operations, such as improving safety, reducing costs, and increasing efficiency [160]. Therefore, innovative technologies and relevant procedures are needed to better monitor subsea assets and increase their safety. DT technology has attracted significant research interest since it can offer reliable and cost-effective ML-based intelligent maintenance strategies [161] that may be able to evaluate life-extension projects. Additionally, the DT concept has been utilized when developing and operating offshore structures like subsea pipelines and platforms.

A recent study by Chen et al. [159] provides a comprehensive survey of the latest publications on various DT applications for subsea pipelines, and considers service life, modeling, construction, and the appraisal of life extension. The study identified that DT construction should begin when designing an offshore structure. The DT model must be updated to reflect the as-built and as-installed conditions. Furthermore, it must be updated swiftly when there is accidental damage so that relevant information is available to assess the safety of the assets in question quickly.

In addition, the study also identified some ways to improve DT-enabled integrity management, which include learning through sharing, automated anomaly detection, standardization, and data contextualization. The remaining fatigue life (RFL) information that is provided by DT models may be useful for appraising whether or not to extend the service life of subsea assets. Moreover, the calibrated DT model can evaluate fatigue damage in real-time during a

TABLE 11. Summary of existing studies.

Ref.	Contributions	Results
[156]	Employed a DT approach to implement a robotic sensing network that could adaptively respond to the dynamic UW environment	The presented solution facilitates reliable evaluation of network with no permanent physical links with deep-sea observation systems
[151]	Employed DT for addressing the huge concerns regarding cyber security threats as connectivity and cyber-physical systems multiply	The developed DTs may handle the internal cyber security risks residing inside the integrated systems because of their intricacy and emergent attributes and the external cyber safety threats like deliberate cyber-attacks
[152]	Introduced a novel RFS and DT-based framework of sensor control in anti-submarine warfare	Addressed the shortcomings of the traditional vector-based algorithms Capable of jointly estimating the number and state of all the enemy submarines Can efficiently control the sensor for both multiple and single submarine scenarios
[157]	Utilized the DT technology for offering ubiquitous information insight and smart decision-making with accuracy and security for better exploitation of marine resources	Achieved effective management and optimization of marine network resources
[153]	Studied the security performance of the DT-based MTS and developed marine transportation towards digitalization and intelligence	The developed maritime transportation DTs model exhibit exceptional safety and transmission performance, offering an experimental foundation for secure and intelligent maritime transportation in the years to come
[158]	Leveraged DT technology to develop AMSVs for resolving the growing requirements of sea safety and water-based navigation	Presented a proof-of-concept that DTs are a safe and agile approach for designing and developing AMSVs
[154]	Introduced a novel UW data transmission protocol for improving the robustness and reliability of UW data transmission	Based on the proposed approach, the intelligent ship designed using the DT architecture offer successful ship operating state prediction information
[155]	Established a DT system based on the pilot mode of multi-AUG collaboration for the reliable monitoring of multiple AUGs in UW cooperative operations	The presented mechanism efficiently achieved the AUG group's collaborative control in the leader mode, and addressed the issue of AUG falling into the local optimal path
[159]	Reviewed the DT applications in subsea pipelines with respect to service life, modeling and construction	Deduced that the DT emergence offers an effective mean of realizing downtime prediction, remote control and monitoring, and risk reduction of gas and oil subsea pipeline systems

pipeline system's service life by taking real environmental conditions into consideration. The authorities and owners could then keep an eye on RFL and develop a plan for fatigue life optimization or provide reinforcements or improvements to extend the life of the assets in question.

In addition, the survey in [159] pointed out some key challenges associated with using DTs for subsea operations. In most cases, different systems are used to store information about risks and conditions. The fact that access to server data is restricted is another main issue when it comes to using DTs. The virtual and physical facilities must be secured against cyberattacks using high-tech cybersecurity protocols [160], [162], [163]. When it comes to social impact, Chen et al. [159] revealed that DT technology may lead to workplace redistribution with no notable effect on employment. The survey in [164] identified a few ways to increase coherency in DT research and development. These include unifying model standards and data, creating a public database to share models and data, developing services and products to facilitate building and using DTs, developing universal tools and platforms for DT applications, and creating forums for researchers and practitioners.

Overall, the research on employing DT technology in UW networks is still in its infancy. Promoting DT technology is expected to help fuel the development of "Smart Ocean" architectures, which will provide further opportunities to apply DT technology in UW networks and construct intelligent marine and aerial networks [165].

X. CHALLENGES OF USING DT IN THE MARINE INDUSTRY

Despite the many anticipated advantages of using DTs in marine networks, some limitations associated with using DTs are not well-discussed in the existing literature. Johansen and Nejad [166] emphasized that once there is a shift from offline condition monitoring to online condition monitoring and the cost-related concerns associated with sensors and their connectivity are resolved, then there could be a notable progression toward DT implementation being the future of ship operations. However, more studies are required to shed more light on the challenges linked with DT implementation in UW systems. In light of this, Ibrion et al. [167] discuss the aviation industry, where DT technology is more extensively used, to expand upon a few aspects of the challenges

and risks linked with DT implementation in maritime communications.

DT technology has numerous benefits; however, it also has major uncertainties and risks associated with its implementation that should be addressed for not only the marine industry but also the aviation industry, where the technology is already widely used. DT implementation comes with risks that need to be thoroughly assessed. The primary purpose of using DT technology is to reduce operational risks; thus, it must not bring or pose new threats. However, the sensors' vulnerability and the technology's inability to identify system faults during the design phase have resulted in some recent disasters in the aviation industry. The DT that was employed to verify the Boeing 737 Max's system encountered failures. It was ineffective since it was not able to successfully simulate and predict some operational scenarios that might cause deadly accidents.

Furthermore, DT technology might be unable to characterize all the scenarios that could be experienced by a system during its lifespan. Paradoxically, reducing risks is the main motive behind implementing DTs; however, aviation disasters and case studies show that the DT introduces risks. Other challenges linked to DT implementation include taking a multidisciplinary approach to engineering, the integration of expertise, the role of experts, dynamic model updating, real-time and near-real-time DT outcomes, model uncertainty, sensor data quality and the input of sensor data in the virtual model, sensor reliability, and inter-industry learning and collaboration.

The major uncertainties associated with DT technology mean it cannot be considered the technical solution that will solve all the marine industry's issues. Thoroughly understanding the DT technology means not envisioning it solely in terms of its potential advantages; its associated challenges must be resolved in time. The marine industry, mainly autonomous ships, should learn from the aviation industry and incorporate the lessons it has learned regarding DT. DT has been employed in the aviation industry longer than it has in the marine industry; however, digital deployment and operation are not without risk, and complete dependence on DT is not practical. Therefore, the primary challenge is that in the digital era of numerous sophisticated and highly developed technical systems, DT solutions come with their own uncertainties that must be continuously assessed and addressed [167].

XI. CONCLUSION

The evolution of the IoUT presents both promising opportunities and complex challenges. While the IoUT holds great potential for underwater applications, its issues related to data accuracy, information transmission efficiency, and security must be addressed for successful deployment. The state-of-the-art works discussed in this paper serve as a foundation for addressing these challenges and advancing the field of underwater communication and security so that the IoUT can ultimately achieve its full potential.

REFERENCES

[1] J. Zhou, "Secure identity authentication scheme based on PUF for IoUT," *Acad. J. Comput. Inf. Sci.*, vol. 4, no. 1, pp. 7–14, 2021.

[2] D. R. K. Mary, E. Ko, S. G. Kim, S. Yum, S. Y. Shin, and S. H. Park, "A systematic review on recent trends, challenges, privacy and security issues of underwater Internet of Things," *Sensors*, vol. 21, no. 24, p. 8262, 2021.

[3] S. A. H. Mohsan, A. Mazinani, N. Q. H. Othman, and H. Amjad, "Towards the Internet of Underwater Things: A comprehensive survey," *Earth Sci. Inform.*, vol. 15, no. 2, pp. 735–764, 2022.

[4] D. Ekta, Y. Rajendra, and U. Nandini, "Securing underwater wireless communication networks," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 3, pp. 131–135, 2016.

[5] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 729–752, 1st Quart., 2019.

[6] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Netw.*, vol. 142, Apr. 2023, Art. no. 103114.

[7] M. Anowar et al., "A survey of acoustic underwater communications and ways of mitigating security challenges," *Int. J. Res. Eng. Sci.*, vol. 4, no. 6, pp. 43–51, 2016.

[8] Y. Tan, J. Wang, J. Liu, and Y. Zhang, "Unmanned systems security: Models, challenges, and future directions," *IEEE Netw.*, vol. 34, no. 4, pp. 291–297, Aug. 2020.

[9] S. A. H. Mohsan, Y. Li, M. Sadiq, J. Liang, and M. A. Khan, "Recent advances, future trends, applications and challenges of Internet of Underwater Things (IoUT): A comprehensive review," *J. Mar. Sci. Eng.*, vol. 11, no. 1, p. 124, 2023.

[10] A. G. Yisa, T. Dargahi, S. Belguith, and M. Hammoudeh, "Security challenges of Internet of Underwater Things: A systematic literature review," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 3, 2021, Art. no. e4203.

[11] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018.

[12] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Procedia Comput. Sci.*, vol. 147, pp. 210–216, Feb. 2019.

[13] O. Bello and S. Zeadally, "Internet of Underwater Things communication: Architecture, technologies, research challenges and future opportunities," *Ad Hoc Netw.*, vol. 135, Oct. 2022, Art. no. 102933.

[14] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of Underwater Things and big marine data analytics—A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 904–956, 2nd Quart., 2021.

[15] H. Kaushal and G. Kaddoum, "Underwater optical wireless communication," *IEEE Access*, vol. 4, pp. 1518–1547, 2016.

[16] K. Y. Islam, I. Ahmad, D. Habibi, and A. Waqar, "A survey on energy efficiency in underwater wireless communications," *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103295.

[17] N. Morozs, W. Gorma, B. T. Henson, L. Shen, P. D. Mitchell, and Y. V. Zakharov, "Channel modeling for underwater acoustic network simulation," *IEEE Access*, vol. 8, pp. 136151–136175, 2020.

[18] M. Stojanovic and J. Preisig, "Underwater acoustic communication channels: Propagation models and statistical characterization," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 84–89, Jan. 2009.

[19] S. Zhu, X. Chen, X. Liu, G. Zhang, and P. Tian, "Recent progress in and perspectives of underwater wireless optical communication," *Prog. Quantum Electron.*, vol. 73, Sep. 2020, Art. no. 100274.

[20] S. Das, Z. Rahman, and S. M. Zafaruddin, "Optical wireless transmissions over multi-layer underwater channels with generalized gamma fading," in *Proc. IEEE 95th Veh. Technol. Conf. (VTC)*, 2022, pp. 1–6.

[21] Z. Rahman, S. M. Zafaruddin, and V. K. Chaubey, "Direct air-to-underwater optical wireless communication: Statistical characterization and outage performance," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2655–2660, Feb. 2022.

[22] Z. Rahman, N. V. Tailor, S. M. Zafaruddin, and V. K. Chaubey, "Unified performance assessment of optical wireless communication over multi-layer underwater channels," *IEEE Photon. J.*, vol. 14, no. 5, pp. 1–14, Oct. 2022.

[23] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, Feb. 2011.

[24] B. Silverajan, M. Ocak, and B. Nagel, "Cybersecurity attacks and defences for unmanned smart ships," in *Proc. IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, 2018, pp. 15–20.

[25] P. A. Shelar, P. N. Mahalle, and G. Shinde, "Secure data transmission in underwater sensor network: Survey and discussion," in *Internet of Things, Smart Computing and Technology: A Roadmap Ahead*. Cham, Switzerland: Springer, 2020, pp. 323–360.

[26] K. Ashok and S. Gopikrishnan, "Statistical analysis of remote health monitoring based IoT security models & deployments from a pragmatic perspective," *IEEE Access*, vol. 11, pp. 2621–2651, 2023.

[27] A. M. Alnajim, S. Habib, M. Islam, S. M. Thwin, and F. Alotaibi, "A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in Industrial Internet of Things," *Technologies*, vol. 11, no. 6, p. 161, 2023.

[28] B. Halak, "CIST: A threat modelling approach for hardware supply chain security," in *Hardware Supply Chain Security: Threat Modelling, Emerging Attacks Countermeasures*. Cham, Switzerland: Springer, 2021, pp. 3–65.

[29] M.-C. Lu, Q.-X. Huang, M.-Y. Chiu, Y.-C. Tsai, and H.-M. Sun, "PSPS: A step toward tamper resistance against physical computer intrusion," *Sensors*, vol. 22, no. 5, p. 1882, 2022.

[30] S. Mavrovouniotis and M. Ganley, "Hardware security modules," in *Secure Smart Embedded Devices, Platforms and Applications*. New York, NY, USA: Springer, 2013, pp. 383–405.

[31] F. Salahdine and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey," *Phys. Commun.*, vol. 39, Apr. 2020, Art. no. 101001.

[32] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, p. 1261, 2020.

[33] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[34] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.

[35] L. B. Milstein, "Interference rejection techniques in spread spectrum communications," *Proc. IEEE*, vol. 76, no. 6, pp. 657–671, Jun. 1988.

[36] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[37] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 1354–1367, 2012.

[38] A. Toftegaard, *A System for Hiding Steganography in Plain Sight*, Tech. Univ. Denmark, Kongens Lyngby, Denmark, 2016.

[39] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems," *IEEE Trans. Mobile Comput.*, vol. 15, no. 9, pp. 2247–2259, Sep. 2016.

[40] P. N. Mahalle, P. A. Shelar, G. R. Shinde, and N. Dey, *The Underwater World for Digital Data Transmission*. Singapore: Springer, 2021.

[41] A. Cornellisen, *Covert Channel Data Leakage Protection*, Radboud Universiteit Nijmegen, Nijmejen, The Netherlands, 2012.

[42] S. Shukla, J. P. George, K. Tiwari, and J. V. Kureethara, "Data security," in *Data Ethics and Challenges*. Singapore: Springer, 2022, pp. 41–59.

[43] M. M. Sabale, V. A. Pande, A. A. Tagalpallewar, A. G. Swami, A. T. Pawar, and A. M. Baheti, "Maintaining data safety and accuracy through data integrity (DI): A comprehensive review," *Res. J. Pharm. Technol.*, vol. 17, no. 5, pp. 2431–2440, 2024.

[44] V. Varadharajan and S. Bansal, "Data security and privacy in the Internet of Things (IoT) environment," in *Connectivity Frameworks Smart Devices: The Internet of Things from a Distributed Computing Perspective*. Cham, Switzerland: Springer, 2016, pp. 261–281.

[45] A. Waheed et al., "Analysis of possible attacks on data and possible solutions with comparative analysis of various encryption algorithms and evaluation," *Int. J. Innov. Res. Eng. Manag.*, vol. 9, no. 2, pp. 50–58, 2022.

[46] S. R. Prasanna and B. Premananda, "Performance analysis of MD5 and SHA-256 algorithms to maintain data integrity," in *Proc. Int. Conf. Recent Trends Electron. Inf. Commun. Technol. (RTEICT)*, 2021, pp. 246–250.

[47] H. S. Al-Hashem and H. A. Al-Essa, "Towards data availability solutions during disaster," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manag. (ICT-DM)*, 2019, pp. 1–4.

[48] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: Measurement, analysis, and implications," in *Proc. ACM SIGCOMM Conf.*, 2011, pp. 350–361.

[49] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 729–752, 1st Quart., 2019.

[50] B. B. Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: Issues and challenges," *Inf. Secur. J., A Global Perspect.*, vol. 18, no. 5, pp. 224–247, 2009.

[51] M. Gautam and G. Prabhakar, "Identification of network security issues and challenges in defense environments," *Int. J. Eng. Manag. Technol.*, 2023, to be published.

[52] M. Furdek et al., "An overview of security challenges in communication networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Model. (RNDM)*, 2016, pp. 43–50.

[53] J. Korhonen and Y. Wang, "Effect of packet size on loss rate and delay in wireless links," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2005, pp. 1608–1613.

[54] R. Venkateswaran, "VPN-virtual private network," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, Mar. 2001.

[55] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *J. Inf. Secur. Appl.*, vol. 41, pp. 103–116, Aug. 2018.

[56] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.

[57] G. Deepa and P. S. Thilagam, "Securing Web applications from injection and logic vulnerabilities: Approaches and challenges," *Inf. Softw. Technol.*, vol. 74, pp. 160–180, Jun. 2016.

[58] A. Jaquith, *Security Metrics*. London, U.K.: Pearson Educ., 2007.

[59] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, document SP 800-94, 2007.

[60] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[61] J. Owens and J. Matthews, "A study of passwords and methods used in brute-force SSH attacks," in *Proc. USENIX Workshop Large-Scale Exploits Emergent Threats (LEET)*, 2008, p. 8.

[62] M. Mehmood, R. Amin, M. M. A. Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," *IEEE Access*, vol. 11, pp. 46561–46576, 2023.

[63] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, "Assessment of access control systems," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. 7316, 2006.

[64] A. Jaquith, *Security Metrics*. London, U.K.: Pearson Education, 2007.

[65] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," *Int. J. u-e-Serv. Sci. Technol.*, vol. 2, no. 3, pp. 13–28, 2009.

[66] N. Gunti, W. Sun, and M. Niamat, "I-RBAC: Isolation enabled role-based access control," in *Proc. 9th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, 2011, pp. 79–86.

[67] S. El Jaouhari and E. Bouvet, "Secure firmware over-the-air updates for IoT: Survey, challenges, and discussions," *Internet Things*, vol. 18, May 2022, Art. no. 100508.

[68] J. Samuel, N. Mathewson, J. Cappos, and R. Dingledine, "Survivable key compromise in software update systems," in *Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS)*, 2010, pp. 61–72.

[69] J. Bauwens, P. Ruckebusch, S. Giannoulis, I. Moerman, and E. De Poorter, "Over-the-air software updates in the Internet of Things: An overview of key principles," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 35–41, Feb. 2020.

[70] L. Carnevale, A. Ficara, G. Catalfamo, A. Galletta, M. Fazio, and M. Villari, "Secure and energy efficient filtered over-the-air Internet of Things setup in a wireless mesh network for firmware freshness," in *Proc. IEEE Int. Conf. Big Data (BigData)*, 2023, pp. 3904–3913.

[71] P. E. Lanigan, R. Gandhi, and P. Narasimhan, "Sluice: Secure dissemination of code updates in sensor networks," in *Proc. 26th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2006, p. 53.

[72] H. Zhou, S. Huang, and W. Li, "Parametric acoustic array and its application in underwater acoustic engineering," *Sensors*, vol. 20, no. 7, p. 2148, 2020.

[73] S. Kisseleff, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces in challenging environments: Underwater, underground, industrial and disaster," *IEEE Access*, vol. 9, pp. 150214–150233, 2021.

[74] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[75] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[76] T. Hossain, S. Shabab, A. Badrudduza, M. K. Kundu, and I. S. Ansari, "On the physical layer security performance over RIS-aided dual-hop RF-UOWC mixed network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2246–2257, Feb. 2023.

[77] A. S. Ghazy, G. Kaddoum, and S. Satinder, "IRS-aided secure reliable underwater acoustic communications," *IEEE Trans. Veh. Technol.*, early access, Jun. 28, 2024, doi: 10.1109/TVT.2024.3420779.

[78] P. van Walree, E. Sangfelt, and G. Leus, "Multicarrier spread spectrum for covert acoustic communications," in *Proc. Oceans*, 2008, pp. 1–8.

[79] A. Zhao, Y. Cheng, T. An, and J. Hui, "Covert underwater acoustic communication system using parametric array," *Mar. Technol. Soc. J.*, vol. 53, no. 1, pp. 20–26, 2019.

[80] G. Leus, P. van Walree, J. Boschma, C. Fanciullacci, H. Gerritsen, and P. Tusoni, "Covert underwater communications with multiband OFDM," in *Proc. Oceans*, 2008, pp. 1–8.

[81] J. Zhang, G. Gao, J. Zhang, and Y. Guo, "Secure and noise-resistant underwater wireless optical communication based on spectrum spread and encrypted OFDM modulation," *Opt. Exp.*, vol. 30, no. 10, pp. 17140–17155, 2022.

[82] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Equivocation of eve using two edge type LDPC codes for the binary erasure wiretap channel," in *Proc. Conf. Rec. 44th Asilomar Conf. Signals, Syst. Comput*, 2010, pp. 2045–2049.

[83] S. Bagali and R. Sundaraguru, "Maximize resource utilization based channel access model with presence of reactive jammer for underwater wireless sensor network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 3, p. 3284, 2020.

[84] S. Bagali and R. Sundaraguru, "Efficient channel access model for detecting reactive jamming for underwater wireless sensor network," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw*, 2019, pp. 196–200.

[85] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing underwater acoustic communications through analog network coding," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, 2014, pp. 266–274.

[86] Y. Ye, Z. Peng, and X. Hong, "Active jamming for eavesdropping prevention in underwater wireless networks," in *Proc. Int. Conf. Underwater Netw. Syst.*, 2019, pp. 1–5.

[87] Y. Liu, L. Li, R. Fan, S. Ma, X. Liu, and Y. Su, "A physical layer security mechanism based on cooperative jamming in underwater acoustic sensor networks," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, 2021, pp. 239–243.

[88] Y. Su, L. Li, R. Fan, Y. Liu, and Z. Jin, "A secure transmission scheme with energy-efficient cooperative jamming for underwater acoustic sensor networks," *IEEE Sensors J.*, vol. 22, no. 21, pp. 21287–21298, Nov. 2022.

[89] Y. Su, Y. Liu, R. Fan, L. Li, M. Han, and H. Zhang, "A secure relay selection scheme based on cooperative jamming for underwater acoustic sensor networks," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109307.

[90] Y. Su, Y. Liu, R. Fan, L. Li, H. Fan, and S. Zhang, "A cooperative jamming scheme based on node authentication for underwater acoustic sensor networks," *J. Mar. Sci. Appl.*, vol. 21, no. 2, pp. 197–209, 2022.

[91] Y. Huang, P. Xiao, S. Zhou, and Z. Shi, "A half-duplex self-protection jamming approach for improving secrecy of block transmissions in underwater acoustic channels," *IEEE Sensors J.*, vol. 16, no. 11, pp. 4100–4109, Jun. 2016.

[92] 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, Feb. 2019.

[93] M. Khalid, R. Zhao, and N. Ahmed, "Physical layer authentication in line-of-sight underwater acoustic sensor networks," in *Proc. Global Oceans Singapore–U.S. Gulf Coast*, 2020, pp. 1–5.

[94] M. Khalid, R. Zhao, and X. Wang, "Node authentication in underwater acoustic sensor networks using time-reversal," in *Proc. Global Oceans Singapore–U.S. Gulf Coast*, 2020, pp. 1–4.

[95] R. Zhao, M. Khalid, O. A. Dobre, and X. Wang, "Physical layer node authentication in underwater acoustic sensor networks using time-reversal," *IEEE Sensors J.*, vol. 22, no. 4, pp. 3796–3809, Feb. 2022.

[96] C. Liu, R. Zhao, T. Shi, and H. Wang, "Node authentication for underwater sensor networks based on time reversal and LinUCB," in *Proc. Oceans Limerick*, 2023, pp. 1–5.

[97] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, "Impersonation detection in line-of-sight underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 44459–44472, 2018.

[98] T. Shi, R. Zhao, X. Shen, and H. Wang, "Database-based physical layer authentication for dynamic underwater acoustic networks," in *Proc. Oceans Limerick*, 2023, pp. 1–4.

[99] P. Casari, F. Ardizzon, and S. Tomasin, "Physical layer authentication in underwater acoustic networks with mobile devices," in *Proc. 16th Int. Conf. Underwater Netw. Syst.*, 2022, pp. 1–8.

[100] W. Aman, S. Al-Kuwari, and M. Qaraqe, "Location-based physical layer authentication in underwater acoustic communication networks," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC)*, 2023, pp. 1–6.

[101] W. Aman, S. Al-Kuwari, and M. Qaraqe, "A novel physical layer authentication mechanism for static and mobile 3D underwater acoustic communication networks," *Phys. Commun.*, vol. 66, Oct. 2024, Art. no. 102430.

[102] L. Bragagnolo, F. Ardizzon, N. Laurenti, P. Casari, R. Diamant, and S. Tomasin, "Authentication of underwater acoustic transmissions via machine learning techniques," in *Proc. IEEE Int. Conf. Microw., Antennas, Commun. Electron. Syst. (COMCAS)*, 2021, pp. 255–260.

[103] F. Ardizzon, R. Diamant, P. Casari, and S. Tomasin, "Machine learning-based distributed authentication of UWAN nodes with limited shared information," in *Proc. 6th Underwater Commun. Netw. Conf. (UComms)*, 2022, pp. 1–5.

[104] F. Ardizzon, P. Casari, and S. Tomasin, "A RNN-based approach to physical layer authentication in underwater acoustic networks with mobile devices," *Comput. Netw.*, vol. 243, Apr. 2024, Art. no. 110311.

[105] L. Xiao, G. Sheng, X. Wan, W. Su, and P. Cheng, "Learning-based PHY-layer authentication for underwater sensor networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 60–63, Jan. 2019.

[106] R. Zhao, T. Shi, C. Liu, X. Shen, and O. A. Dobre, "Physical layer authentication without adversary training data in resource-constrained underwater acoustic networks," *IEEE Sensors J.*, vol. 23, no. 22, pp. 28270–28281, Nov. 2023.

[107] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, and J. A. Ansere, "A synergetic trust model based on SVM in underwater acoustic sensor networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11239–11247, Nov. 2019.

[108] Y. Su, S. Ma, H. Zhang, Z. Jin, and X. Fu, "A redeemable SVM-DS fusion-based trust management mechanism for underwater acoustic sensor networks," *IEEE Sensors J.*, vol. 21, no. 22, pp. 26161–26174, Nov. 2021.

[109] Y. He, G. Han, J. Jiang, H. Wang, and M. Martinez-Garcia, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 3, pp. 811–821, Mar. 2022.

[110] Y. Li, L. Xiao, Q. Li, and W. Su, "Spoofing detection games in underwater sensor networks," in *Proc. Oceans MTS/IEEE Washington*, 2015, pp. 1–5.

[111] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[112] G. Han, Y. He, J. Jiang, H. Wang, Y. Peng, and K. Fan, "Fault-tolerant trust model for hybrid attack mode in underwater acoustic sensor networks," *IEEE Netw.*, vol. 34, no. 5, pp. 330–336, Oct. 2020.

[113] J. Du, G. Han, C. Lin, and M. Martínez-García, "LTrust: An adaptive trust model based on LSTM for underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7314–7328, Sep. 2022.

[114] M. Zhang, R. Feng, H. Zhang, and Y. Su, "A recommendation management defense mechanism based on trust model in underwater acoustic sensor networks," *Future Gener. Comput. Syst.*, vol. 145, pp. 466–477, Aug. 2023.

[115] K. Liang, H. Huang, X. Huang, and Q. Yang, "CS-based homomorphism encryption and trust scheme for underwater acoustic sensor networks," in *Proc. Int. Conf. Mach. Learn. Big Data Anal. IoT Security Privacy*, 2020, pp. 394–399.

[116] K. Liang, S. Sun, X. Huang, Q. Yang, and N. X. Neal, "A trust-based malicious detection scheme for underwater acoustic sensor networks," in *Proc. 8th Int. Conf., Artif. Intell. Secur. (ICAIS)*, Qinghai, China, 2022, pp. 427–440.

[117] Y. He, G. Han, A. Li, T. Taleb, C. Wang, and H. Yu, "A federated deep reinforcement learning-based trust model in underwater acoustic sensor networks," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 5150–5161, May 2024.

[118] L. Xiao, Q. Li, T. Chen, E. Cheng, and H. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2015, pp. 1–6.

[119] L. Xiao, Donghua, X. Wan, W. Su, and Y. Tang, "Anti-jamming underwater transmission with mobility and learning," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 542–545, Mar. 2018.

[120] L. Xiao, D. Jiang, Y. Chen, W. Su, and Y. Tang, "Reinforcement-learning-based relay mobility and power allocation for underwater sensor networks against jamming," *IEEE J. Ocean. Eng.*, vol. 45, no. 3, pp. 1148–1156, Jul. 2020.

[121] Y. Liu, C. Liu, Z. Zhao, and W. Qu, "Anti-interference transmission strategy for underwater acoustic communication based on deep reinforcement learning," in *Proc. IEEE 25th Int. Conf. Comput. Support. Cooper. Work Design (CSCWD)*, 2022, pp. 1167–1172.

[122] C. Liu, Y. Zhang, G. Niu, L. Jia, L. Xiao, and J. Luan, "Towards reinforcement learning in UAV relay for anti-jamming maritime communications," *Digit. Commun. Netw.*, vol. 9, no. 6, pp. 1477–1485, 2023.

[123] J. Yan, Y. Meng, X. Yang, X. Luo, and X. Guan, "Privacy-preserving localization for underwater sensor networks via deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1880–1895, 2020.

[124] J. Yan, H. Zhao, Y. Meng, and X. Guan, "Deep reinforcement learning based privacy preserving localization of USNs," in *Localization Underwater Sensor Networks*. Singapore: Springer, 2021, pp. 177–215.

[125] J. Pei, W. Liu, L. Wang, C. Liu, A. K. Bashir, and Y. Wang, "Fed-IoUT: Opportunities and challenges of federated learning in the Internet of Underwater Things," *IEEE IoT Mag.*, vol. 6, no. 1, pp. 108–112, Mar. 2023.

[126] M. Alazab, R. M. S. Priya, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3501–3509, May 2022.

[127] H. Zhao, F. Ji, Q. Li, Q. Guan, S. Wang, and M. Wen, "Federated meta-learning enhanced acoustic radio cooperative framework for Ocean of Things," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 474–486, Apr. 2022.

[128] Z. Qin, J. Ye, J. Meng, B. Lu, and L. Wang, "Privacy-preserving blockchain-based federated learning for marine Internet of Things," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 159–173, Feb. 2022.

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

[130] W. Liu et al., "Intrusion detection for maritime transportation systems with batch federated aggregation," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2503–2514, Feb. 2022.

[131] Z. Zhang, C. Guan, H. Chen, X. Yang, W. Gong, and A. Yang, "Adaptive privacy-preserving federated learning for fault diagnosis in Internet of Ships," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6844–6854, May 2022.

[132] M. Karagoz, "Maritime security operations and the combined joint operations from the sea Center of excellence," in *Maritime Security and Defence Against Terrorism*. Amsterdam, The Netherlands: IOS Press, 2012, pp. 87–91.

[133] G. Cirincione and D. Verma, "Federated machine learning for multi-domain operations at the tactical edge," in *Proc. Artif. Intell. Mach. Learn. Multi-Domain Oper. Appl.*, 2019, pp. 29–48.

[134] A. Haidine, A. Aqqal, and A. Dahbi, "Communications backbone for environment monitoring applications in smart maritime ports—Case study of a moroccan port," in *Proc. IEEE Asia-Pac. Conf. Geosci., Electron. Remote Sens. Technol. (AGERS)*, 2021, pp. 136–140.

[135] Y. Wang, W. Feng, J. Wang, and T. Q. Quek, "Hybrid satellite-UAV-terrestrial networks for 6G ubiquitous coverage: A maritime communications perspective," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3475–3490, Nov. 2021.

[136] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected UAVs," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 28–35, Feb. 2019.

[137] S. A. Chaudhry et al., "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2401–2410, Feb. 2023.

[138] N. Nomikos, P. K. Gkonis, P. S. Bithas, and P. Trakadas, "A survey on UAV-aided maritime communications: Deployment considerations, applications, and future challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 56–78, 2023.

[139] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. Lee, and D.-S. Kim, "Composite and efficient DDoS attack detection framework for B5G networks," *Comput. Netw.*, vol. 188, Apr. 2021, Art. no. 107871.

[140] I. de la Peña Zarzuelo, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue," *Transp. Policy*, vol. 100, pp. 1–4, Jan. 2021.

[141] D. Dalaklis, N. Nikitakos, and R. Yaacob, "Cyber security training strategy: Dealing with maritime SCADA risks," in *Proc. Int. Maritime Lecturers Assoc. (IMLA)*, 2021, pp. 53–61.

[142] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "FED-MARINE: Federated learning framework for DDoS detection and mitigation in maritime-SCADA network," in *Proc. 1st Int. Conf. Maritime IT Converg.*, 2022, pp. 1–3.

[143] C. Han and T. Yang, "Privacy protection technology of maritime multi-agent communication based on part-federated learning," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, 2021, pp. 266–271.

[144] D. Kwon, J. Jeon, S. Park, J. Kim, and S. Cho, "Multiagent DDPG-based deep learning for smart ocean federated learning IoT networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9895–9903, Oct. 2020.

[145] Y. Gao, L. Liu, B. Hu, T. Lei, and H. Ma, "Federated region-learning for environment sensing in edge computing system," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2192–2204, Dec. 2020.

[146] W. Hammedi, B. Brik, and S. M. Senouci, "Toward optimal MEC-based collision avoidance system for cooperative inland vessels: A federated deep learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2525–2537, Feb. 2023.

[147] M. R. Sprague et al., "Asynchronous federated learning for geospatial applications," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*, Dublin, Ireland, 2019, pp. 21–28.

[148] J. Geiping, H. Bauermeister, H. Dröge, and M. Moeller, "Inverting gradients-how easy is it to break privacy in federated learning?" in *Proc. 34th Conf. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 16937–16947.

[149] B. Z. Téglásy, E. Wengle, J. R. Potter, and S. Katsikas, "Authentication of underwater assets," *Comput. Netw.*, vol. 241, Mar. 2024, Art. no. 110191.

[150] S. Erikstad, "Design patterns for digital twin solutions in marine systems design and operations," in *Proc. 17th Int. Conf. Comput. IT Appl. Marit. Ind. (COMPIT)*, 2018, pp. 354–363.

[151] O. Smogeli, *Digital Twins at Work in Maritime and Energy*, DNV-GL Feature, Bærum, Norway, 2017.

[152] P. Wang, M. Yang, Y. Peng, J. Zhu, R. Ju, and Q. Yin, "Sensor control in anti-submarine warfare—A digital twin and random finite sets based approach," *Entropy*, vol. 21, no. 8, p. 767, 2019.
[153] J. Liu, C. Li, J. Bai, Y. Luo, H. Lv, and Z. Lv, "Security in IoT-enabled digital twins of maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2359–2367, Feb. 2023.
[154] Z. Lv, D. Chen, H. Feng, W. Wei, and H. Lv, "Artificial intelligence in underwater digital twins sensor networks," *ACM Trans. Sens. Netw.*, vol. 18, no. 3, pp. 1–27, 2022.
[155] J. Wen, J. Yang, Y. Li, J. He, Z. Li, and H. Song, "Behavior-based formation control digital twin for multi-AUG in edge computing," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2791–2801, Sep. 2023.
[156] A. Barbie et al., "Developing an underwater network of ocean observation systems with digital twin prototypes—A field report from the baltic sea," *IEEE Internet Comput.*, vol. 26, no. 3, pp. 33–42, Jun. 2022.
[157] Z. Wang and B. Lin, "A digital twin enabled maritime networking architecture," in *Proc. IEEE 95th Veh. Technol. Conf. (VTC)*, 2022, pp. 1–5.
[158] M. Raza, H. Prokopova, S. Huseynzade, S. Azimi, and S. Lafond, "Towards integrated digital-twins: An application framework for autonomous maritime surface vessel development," *J. Mar. Sci. Eng.*, vol. 10, no. 10, p. 1469, 2022.
[159] B.-Q. Chen, P. M. Videiro, and C. G. Soares, "Opportunities and challenges to develop digital twins for subsea pipelines," *J. Mar. Sci. Eng.*, vol. 10, no. 6, p. 739, 2022.
[160] H. P. Ellingsen, *How Digital Tools and Solutions Can Improve Subsea Integrity Management*, DNV-GL, Høvik, Norway, Dec. 2020.
[161] S. Bhowmik, "Digital twin of subsea pipelines: Conceptual design integrating IoT, machine learning and data analytics," in *Proc. Offshore Technol. Conf. (OTC)*, 2019, Art. no. D011S010R004.
[162] T. R. Wanasinghe et al., "Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges," *IEEE Access*, vol. 8, pp. 104175–104197, 2020.
[163] E. Altamiranda and E. Colina, "A system of systems digital twin to support life time management and life extension of subsea production systems," in *Proc. Oceans Marseille*, 2019, pp. 1–9.
[164] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *IEEE Access*, vol. 8, pp. 21980–22012, 2020.
[165] M. Dai et al., "A survey on integrated sensing, communication, and computing networks for smart oceans," *J. Sens. Actuator Netw.*, vol. 11, no. 4, p. 70, 2022.
[166] S. S. Johansen and A. R. Nejad, "On digital twin condition monitoring approach for drivetrains in marine applications," in *Proc. Int. Conf. Offshore Mech. Arctic Eng.*, 2019, Art. no. V010T09A013.
[167] M. Ibrion, N. Paltrinieri, and A. R. Nejad, "On risk of digital twin implementation in marine industry: Learning from aviation industry," *J. Phys., Conf. Ser.*, vol. 1357, no. 1, 2019, Art. no. 12009.

NADIR ADAM received the B.Sc. degree in electrical and electronic engineering from the University of Khartoum, Sudan, in 2009, the M.Sc. degree in electrical engineering from the United Arab Emirates University, UAE, in 2015, and the Ph.D. degree in electrical and computer engineering from the University of Rochester, USA, in 2020. He is currently a Postdoctoral Research Fellow with the École de Technologie Supérieure, Université du Québec, Montreal, Canada, and also affiliated with the Resilient Machine Learning Institute. His work is published in prestigious journals, such as IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and *ACM Transactions on Sensor Networks*, among other leading journals and conferences. His research focuses on wireless sensor networks, terrestrial and nonterrestrial networks, and machine learning applications in wireless systems.

MANSOOR ALI received the B.S. degree in electrical engineering from the National University of Computer and Emerging Sciences, Peshawar, Pakistan, in 2013, the M.S. degree in electrical engineering from the CECOS University of IT and Emerging Sciences, Peshawar, in 2016, and the Ph.D. degree in electrical engineering from the National University of Computer and Emerging Sciences. Since 2021, he has been working as a Postdoctoral Research Fellow with the Electrical Engineering Department, École de Technologie Superieure (ÉTS), Montreal, Canada. His research interests include the load forecasting in a power system networks, fuzzy control, and power flow control under various disturbances.

FAISAL NAEEM is an Assistant Professor with the University of Fraser Valley, with expertise in integrating AI techniques for optimizing 6G networks. His research focuses on reinforcement learning, generative AI, federated learning, and large language models, addressing key issues, such as resource management, network security, and performance optimization in next-generation communication systems. He has extensive experience, having worked as a Postdoctoral Research Fellow with the École de Technologie Supérieure, where he collaborated with ULTRA TCS on AI-driven solutions for threat detection in underwater networks and distributed AI systems for 6G performance enhancement. He also served as a Senior AI Research Engineer with the Resilient Machine Learning Institute, Montreal. His work has been published in prestigious journals like IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and *IEEE Communications Magazine*.

ABDALLAH S. GHAZY was born in Giza, Egypt, in 1983. He received the B.Sc. degree in electrical engineering from Al-Azhar University, Egypt, in 2007, the M.Sc. degree in electrical engineering from the Electrical and Computer Engineering School, Egypt-Japan University for Science and Technology, Alexandria, Egypt, in 2016, and the Ph.D. degree in electrical engineering from the Electrical and Computer Engineering School, McMaster University, Ontario, Canada, in 2021. From 2008 to 2017, he worked in VoIP and Data Networks, Telecom-Egypt, and AVAYA Inc., Cairo, Egypt. In 2012, he joined the Electrical Engineering School, Al-Azhar University. He is currently on leave from Al-Azhar University and is a Ph.D. Research Fellow with the École de Technologie Supérieure, Université du Québec, Montreal, Canada. His main research interests include but are not limited to communication systems and networks, signal processing, and machine learning.

GEORGES KADDOUM (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the École nationale supérieure de techniques avancées (ENSTA Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (High Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, University of Toulouse, Toulouse, France, in 2009. He is currently a Professor and the Research Director of the Resilient Machine Learning Institute, and the Industrial Research Chair and the Tier 2 Canada Research Chair of the École de technologie supérieure (ÉTS), Université du Québec, Montreal, Canada. He has published over 300 journal articles, more than 100 conference papers, two chapters in books, and has eight pending patents. His recent research interests include wireless communication networks, tactical communications, resource allocations, and network security. He received the prestigious MITACS Award for Exceptional Leadership in 2023 and won the IEEE Technical Committee on Scalable Computing Award for Excellence (Middle Career Researcher) in 2022. Additionally, he was honored with the Research Excellence Award from ÉTS in 2019 and from the Université du Québec in 2018. His work has also garnered multiple Best Paper Awards, including those from the 2023 IEEE International Wireless Communications and Mobile Computing Conference, the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications, and the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications. Furthermore, he received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award in 2019, 2017, and 2015. He served as an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE COMMUNICATIONS LETTERS. He is currently serving as an Area Editor for the IEEE TRANSACTIONS ON MACHINE LEARNING IN COMMUNICATIONS AND NETWORKING and an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS. In 2024, he was elected as a College Member to the Royal Society of Canada.