On Securing Underwater Acoustic Networks: A Survey

Shengming Jiang, *Senior Member, IEEE*

***Abstract*—Underwater acoustic networks (UWANs) are often deployed in unattended and untransparent or even hostile environments and face many security threats, while many applications based on UWANs require secure communication, such as costal defense, submarine communication and harbor security. Peculiar features of UWANs such as very constrained resources pose big challenges in defending UWANs against security threats, and many research results are published to address these issues along with several brief surveys available in the literature. This paper aims to provide a comprehensive survey on UWAN security by first discussing the fundamental of network security in general and the main UWAN security threats faced by the physical layer to the transport layer. Then the paper reviews countermeasure schemes against the typical UWAN security threats, securing UWAN protocols and cryptographic primitives designed for UWANs as well as UWAN security structures that address several security issues systematically. The research of UWAN security is still in an early stage, and the paper discusses several important issues necessarily for further studies at the end.**

***Index Terms*—Underwater acoustic network (UWAN), network security, security threat, security measure, security structure.**

I. Introduction

WEAK security is an Achilles' heel of many wireless networks because it is very difficult to secure a channel physically in radio wireless networks (RWNs) with many challenging issues to be addressed [1]–[3]. This situation results because severe network security environments are caused by the broadcast nature of wireless channels and mobility as well as heterogeneity of network nodes. Furthermore, wireless networks are resource-constrained in terms of communication and computation capacity as well as energy supply to handle security threats, particularly in mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs).

The above situation becomes even worse in underwater acoustic networks (UWANs) because the resources are much more constrained while security situation is more severe due to unattended and often untransparent network deploying environments. Furthermore, the following peculiar features of UWANs cause more challenges in handling security threats [4]–[6] as discussed in Sections II-B and II-C. i) Very limited underwater acoustic channel capacity is available with long propagation delay due to slow acoustic wave speed (e.g., 1.5 km/s in seawater). ii) Underwater acoustic channel quality is poor with high dynamics and even asymmetric connectivity [7]. iii) Energy consumed by most currently available underwater acoustic modems for both transmission and reception is much larger than that in RWNs, while UWAN nodes are often battery-operated [8], [9]. Note that although WSNs are similar to UWANs in aspects i and ii, the situation becomes even worse in UWANs as discussed in Section II-C3. In this case, many existing schemes proposed for RWN security (e.g., WSNs) cannot be used directly in UWANs.

As discussed in [6], the limited communication capacity and energy supply are suitable for small message transmission in UWANs, whereas transmission without encryption or authentication is insecure [10]. The popular security mechanisms used to protect confidentiality and integrity of data and enable authentication in RWNs are mainly based on cryptography, particularly symmetric and asymmetric/public key schemes. However, they cause ciphertext expansion due to padding and additional fields to be added in encryption. On the other hand, cryptographic schemes at higher layers suffer from heavy computational complexity, especially in very resource-constrained UWANs [11]–[14]. Particularly with public-key cryptosystems widely used for digital signature and authentication such as the Rivest-Shamir-Adleman (RSA) scheme, they are almost inapplicable in UWANs [15], [16]. More related discussion can be found in Section II-C.

To handle the peculiar features of UWANs for network security, many research results are reported with several reviews available in the literature such as [17]–[19]. Reference [17] discusses possible attacks to UWANs by reviewing 5 countermeasures proposed against these attacks. Reference [18] briefly discusses some aspects for securing underwater acoustic communication and possible attacks layer by layer, with 3 countermeasure schemes against jamming and wormhole attacks. A more comprehensive survey is conducted in [19], reviewing 10 countermeasure proposals without discussing cryptographic primitives. This paper aims to conduct a comprehensive survey on the state-of-the art UWAN security technologies by discussing 35 proposals, most of which have not been reviewed by the above-mentioned surveys. As depicted in Fig. 1, the paper focuses on typical security threats in UWANs and countermeasure schemes against them, securing communication and networking protocols and the fundamental cryptographic primitives designed for UWANs as well as

Manuscript received December 8, 2017; revised June 7, 2018; accepted August 2, 2018. Date of publication August 7, 2018; date of current version February 22, 2019. This work was supported by the National Natural Science Foundation of China for the Project "Basic theory of open network architecture for the marine Internet" under Grant 61472237.

The author is with the Marine Internet Laboratory, College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China (e-mail: smjiang@shmtu.edu.cn).

Digital Object Identifier 10.1109/COMST.2018.2864127

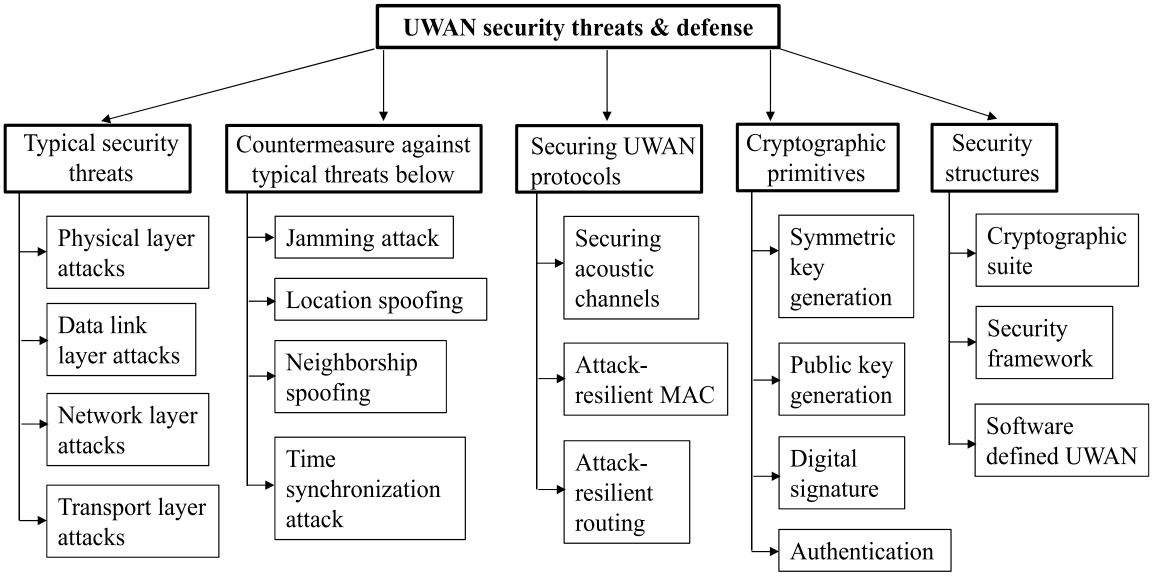

Fig. 1. Typical security threats and security fundamental as well as defense schemes for UWANs.

security structures using cryptographic suites to address several security issues systematically. To the best knowledge of the author, it is the first comprehensive survey on UWAN security, and can provide learners with an overview on UWAN security technologies and the professionals with the state of the art in this field.

The reminder of the paper is organized as follows:

- The network security and the related issues for UWANs are discussed in Section II, including the basic cryptographic primitives and main standards for wireless network security, characteristics of underwater acoustic channels and UWANs as well as challenges for UWAN security.
- Different from other networking issues such as medium access control (MAC) and routing protocols, which are mainly related to only one layer of the OSI reference model, network security involves almost every layer from the physical layer to the application layer, similar to the end-to-end reliable transfer issue discussed in [20]. Therefore, the main security threats in UWANs are summarized according to the layer that attacks may be launched in Section III, and then the typical countermeasures against these threats as well as securing communication and networking protocols in UWANs are reviewed in Sections IV and V, respectively.
- Cryptography is the fundamental for network security. The main problems of the popular cryptographic primitives include ciphertext expansion and computational complexity, which make them unsuitable for UWANs with more constrained channel capacity and larger communication energy consumption than WSNs as discussed in Section II-C. Therefore, several cryptographic primitives designed for UWANs are discussed in Section VI.
- As mentioned above, network security is not an one-layer issue, and should be addressed systematically by taking into account several issues at different layers simultaneously. Three UWAN security structures using cryptographic suites to systematically defend UWANs against security threats are discussed in Section VII.

A comprehensive discussion on the reviewed schemes is conducted in Section VIII, highlighting remaining issues for further research, and the paper is concluded in Section IX.

II. Network Security and Challenges for UWANs

Basically, network security should achieve the following objectives: i) assuring the privacy and integrity of the data transmitted over the network, ii) guaranteeing the data delivery to the real destinations, iii) protecting the systems attached to the network from attacks, and iv) identifying the attack sources if any. To this end, the following security functions are usually implemented provided that the network infrastructure works well to maintain normal network operations [21].

- *Authentication:* ascertaining the user legitimacy of using the network resource.
- *Confidentiality:* protecting the privacy of the data transmitted over the network.
- *Integrity:* identifying whether the data has been altered or not during transmission over the network.
- *No-repudiation:* preventing a sender from denying what has been sent by itself.

Several cryptographic primitives are used to support the above security functions as discussed below.

A. Fundamental of Network Security

This section introduces basic cryptographic primitives and main standards available for network security.

1) Basic Cryptographic Primitives: Cryptography is a science for encrypting and decrypting of information, and is the fundamental of information and network security. Cryptography can be symmetric or asymmetric according to the relationship between encryption keys and decryption keys.

With symmetric key cryptography, the decryption key is the same as the encryption key. With asymmetric key cryptography, two different keys are used for encryption and decryption, respectively. It is also called public key cryptography with the following important property. Given a public key pair (K_1, K_2), if K_1 is used for encryption, only K_2 can be used for decryption, and vice versa. Usually one key is kept secretly, called private key, while the other is open to public, called public key. With equivalent security strength, a symmetric key is much shorter than an asymmetric key, e.g., a 40-56-bit symmetric key is equivalent to a 512-bit asymmetric key [21].

a) Hash function H(x): It can be treated as a black box that accepts a digital object (x) and outputs an identifying number called hash value with the following properties [10]:

- The same input will yield the same hash value, while different inputs should generate different hash values, which means that it is computationally infeasible to find two different inputs x and y such that $H(x) = H(y)$.
- The input x can be of any length, and it should be easy to compute $H(x)$, while the output has a fixed length for easy implementation.
- $H(x)$ should be one-way function, i.e., it is computationally infeasible to find an input that can yield a hash value equal to an existing one.

b) Digital Signature and Certificate: A digital signature is created by encrypting a message with the sender's private key, and the receiver checks the signature through decrypting the message by using the sender's public key. Due to the characteristics of the public key pair mentioned above, only the sender's public key can decrypt the part encrypted with its private key, which ascertains the uniqueness of a digital signature. The public key is inefficient to sign a large message directly due to computational complexity, and a hash function is used to generate a short digest, over which a digital signature is signed. The signed digest is sent together with the message.

A digital certificate establishes a credential relationship between a name or an identity and the information declared by the certificate. A certificate is issued by the authority using its private key to sign it in order to guarantee the authenticity of the issued certificate. The public key of the issuer is used by the user to verify the certificate open to the public [21].

2) Standards for Network Security: As illustrated in Fig. 2, several network security standards have been established to enforce network security, and become the fundamental framework for wireless network security. The typical ones introduced below include authentication and security protocols for the transport layer, the network layer and the data link layer.

Typical authentication protocols include Remote Access Dial-in-User Service (RADIUS) [22], [23] and Diameter [24]. They consist of Authentication, Authorization and Accounting (AAA) protocols. The main transport layer security protocols include Secure Socket Layer (SSL) [25] and its successor Transport Layer Security (TLS) [26]. Wireless TLS (WTLS) is an optional part of the Wireless Access Protocol (WAP) (http://www.wapforum.org). It provides security mechanisms based on public key infrastructures, similar to TLS in protecting integrity and confidentiality of information, authentication and defense against DoS attacks. The main network layer security protocol is IP Security (IPSec) [27], [28]. Typical link layer security protocols include Extensible Authentication Protocol (EAP) [29], IEEE 802.1AE and IEEE 802.1X [30]. EAP provides an authentication framework to support multiple authentication methods. IEEE 802.1X defines a generic framework for authentication and authorization for the security of IEEE LANs. IEEE 802.1AE MAC Security Protocol (MACsec) [31] specifies the cryptographic support of the controlled port for other medium access methods. It maintains the confidentiality and integrity of the transmitted data, and secures MAC services on a frame-by-frame basis.

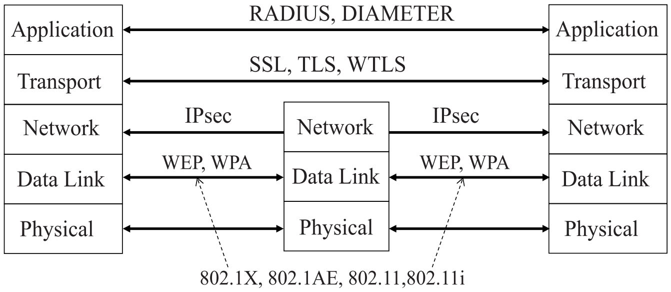

Fig. 2. Standards for network security in general.

B. Characteristics of Underwater Acoustic Channels

The following features characterize underwater acoustic channels.

1) Slow and Variable Propagation Speed: The propagation speed of acoustic wave in seawater is approximately five order of magnitude slower than light speed. It is further affected by temperature, salinity and depth [32], which cause dynamics of propagation speed. The slow propagation speed causes severe Doppler effect in mobile UWANs because the magnitude of this effect is proportional to the ratio of transmitter-receiver relative speed and signal propagation speed. This effect causes considerable frequency shifting and motion-induced distortion [33], which also contribute to dynamics of channel quality [20], [34].

2) Small and Crowded Channel: Only a very limited bandwidth of maximal kHzs is feasible for underwater acoustic communication. It is also shared by underwater localization and navigation. The effective bandwidth is affected by frequency-selective signal-heat conversion and the spreading loss due to the expansion of transmitted energy over a large surface. Both increase with signal propagation distances, which further limits the channel capacity for long range transmission [33], [35]. Currently, achievable acoustic channel data rates are more than 100 kbit/s for short ranges roughly less than 1 km. A maximum rate is about 50 kbit/s for medium ranges roughly less than 10 km, and a maximum rate of 10 kbit/s is possible around 20 km [34].

3) Unreliable and Changing Channel: Multi-path propagation causes a signal from a source may arrive at the receiver in different paths with phase shift [36]. It is caused by acoustic signal reflected from surfaces, seabed and floating objects etc. These out-of-phase simultaneously arriving signals may

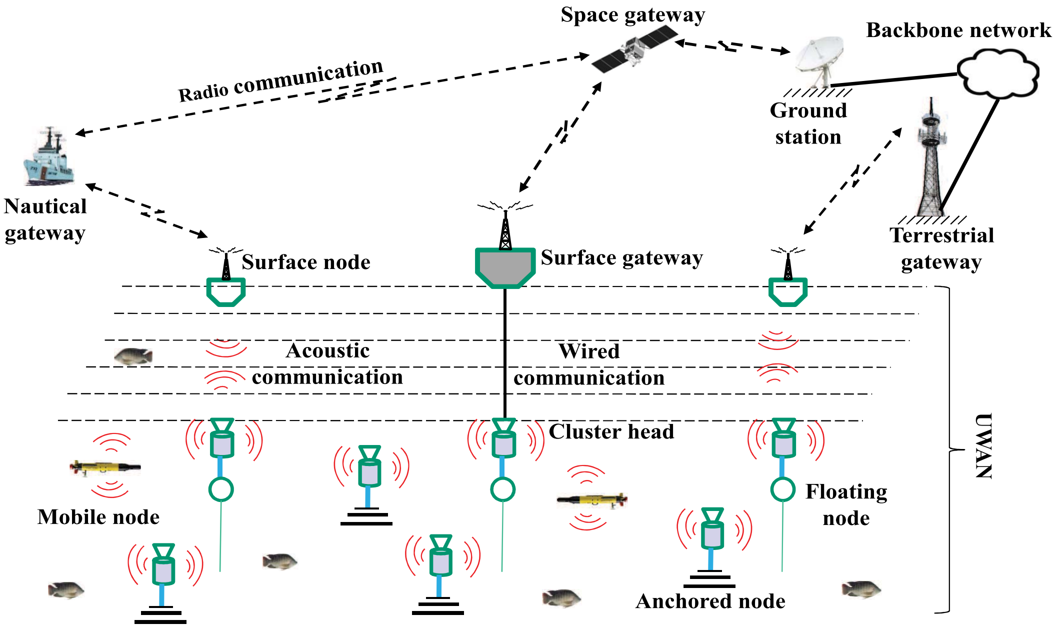

Fig. 3. A diagram of an UWAN connecting other networks via the following nodes: terrestrial gateways, nautical gateways (e.g., ships), space gateways.

cause severe inter-symbol interference (ISI), with which a signal for one symbol may interfere with those for subsequent symbols [34]. In an RF receiver, the ISI may involve only a few symbols, whereas the ISI in a single-carrier UWAN may span tens or even hundreds of symbol intervals [33] due to the long propagation delay, which makes demodulation more difficult to resolve ISI [37].

Plentiful underwater noises also impact underwater channel quality, mainly including ocean ambient noise and self-noise of vessels [38]–[41]. They affect acoustic communication at different frequencies roughly as follows: turbulence noise for frequencies less than 10 Hz, shipping noise for frequencies between 10 and 100 Hz, wave and other surface motion caused by wind and rain for 100 Hz∼100 kHz, and thermal noise for frequencies over 100 kHz [41]. Furthermore, underwater acoustic channel quality may also change in very short time scale [35], [42].

4) Wideband Communication Channel: Communication systems whose bandwidth is smaller than 1% of the center frequency of the signal are called narrow band, and those between 1% and 20% are called wideband, while the others are called ultra-wideband (UWB) [43]. Popular frequency bands used by acoustic communication vary with communication ranges. For example, a popular frequency band is about 8∼14 kHz for ranges up to a few kilometers, while the upper-frequency limit is 10∼100 kHz [36], [44]. Relatively, underwater acoustic channels can be qualified as wideband [43].

C. Challenges for UWANs Security

Peculiar features of UWANs impose challenges on securing UWANs as discussed below after an introduction to UWANs.

1) Overview of UWANs: As depicted in Fig. 3, a UWAN usually consists of network nodes equipped with acoustic communication capability. These nodes can be anchored on the sea floor, while in some cases they suspend or even float in water and thus drift randomly with current. Mobile network nodes such as Autonomous Underwater Vehicles (AUVs) may also be used to collect data dynamically from sensors deployed in different underwater areas. Acoustic links are usually used for communication between them except in some special occasions, where a cable may be used to link the cluster head of a UWAN to a surface gateway, for example. UWAN nodes on the water surface are used to link UWANs to various kinds of gateways, such as nautical gateways (e.g., a mother ship), terrestrial gateways (e.g., a base station) or even space gateways (e.g., a high platform or a satellite), which connect terrestrial backbone networks such as the Internet. Radio links are used for communication between surface nodes and gateways, while optical fibers are usually used between terrestrial gateways and backbone networks.

2) UWAN Environments: Security and countermeasures against threats in UWANs are also affected by the special underwater network environments as discussed below.

- Underwater nodes are generally deployed in unattended and untransparent or even hostile environments. It is possible for an adversary to compromise or even capture them because it is almost impossible to implement physical countermeasure to protect all of them [45], [46]. Detecting compromised security is often carried out through measuring abnormalities following the expected communication and movement patterns [6]. However, it becomes difficult for passive threats and carefully designed attacks. Even in a local untransparent underwater environment without physical protection, a UWAN can be intruded by adversaries, e.g., eavesdroppers, which cannot be easily identified.
- Removing compromised nodes is necessary but costly. A logical removal of a compromised node should be

TABLE I
COMPARISON BETWEEN FOR UWANS AND RWNS [48]–[50]

Comparison items	Underwater acoustic network (UWAN)	Radio wireless networks	
		WSN	MANET
Network bandwidth	Very small	Small	Moderate
Energy consumption	Large	Lower	Low
Node density	Low	High	Moderate
Node robustness	Good	Poor	Good
Storage capacity	Large	Small	Limited
Processing capability	Powerful	Weaker	Weak
Network environment	Poor	Better	Good
Network cost*	Expensive	Cheap	Moderate

*including costs for manufacturing, deployment, maintenance and restoring service

carried out by rekeying the whole network because of a possible leakage of the secret contained in compromised nodes [6]. However, this may not be sufficient because a compromised node can still jam the network, and a physical removal is essential. A removal of underwater nodes is usually more difficult and costly than in terrestrial environments.

- A threat source could be anywhere and anytime, while an underwater acoustic link is open to any node within the communication range. In this case, an adversary can passively intercept acoustic signal for analysis, actively affects or even disrupts network services such as localization, time synchronization and routing [45].
- Different from radio communications, no standard model is available for underwater acoustic communication [47], and underwater channel quality is affected by various properties of underwater environments such as depth, temperature and salinity. These make it difficult to distinguish clearly between attack evidences and abnormal communication situations when different communication systems coexist in the same location.
- In terrestrial RWNs, GPS can be used for localization and time synchronization, both of which are very important to the performance of the main network protocols such as MAC and routing as well as security. Since GPS cannot work underwater, in UWANs, location information is usually obtained through measurement, while time synchronization is realized via handshaking in UWANs. Actually, these methods also offer opportunities to attackers as discussed in Sections III-B1 and III-B4, respectively.

3) UWANs Versus WSNs: Table I gives a brief comparison between UWANs, MANETs and WSNs. The main differences between UWANs and WSNs include propagation delay, communication energy consumption and node density as well as node mobility, which impose more challenges for UWAN security as discussed below.

The slow acoustic propagation speed makes wormhole attacks much easier in UWANs than in WSNs since an out-of-band low-latency connection can be easily created via a radio link above the water surface [17]. Furthermore, dynamic UWAN topologies due to node's random movement with current facilitate the creation of wormholes and complicate the detection [51]. This attack can compromise the security of other network protocols such as routing and localization as discussed in Section III-B2a.

Although UWANs are similar to radio WSNs in terms of small, crowded and unreliable channels, this situation becomes worse in UWANs. As discussed earlier, the maximum achievable transmission rates in UWANs are around 100 kbps for transmission ranges less than 1 km [33], [35]. For low data rate WSNs, the transmission rate can be up to several hundreds of kbps. For example, the IEEE 802.15.4 based ZigBee can provide transmission rates up to 250 kbps. Alternatively, WSNs can exploit other types of radio links to construct higher data rate backbone at more deployment cost. For example, the IEEE 802.11 based WiFi can easily provide tens and even hundreds of Mbps transmission rates. However, there is no such option available for UWANs. Therefore, UWANs have much less network bandwidth available to enforce network security.

Generally for radio WSNs, the reliability of radio communication channels is considered better than that of underwater acoustic channels in UWANs [52] due to multiple acoustic propagation paths and plentiful acoustic interference sources in oceans, such as marine animals (e.g., whales and even shrimps), rains, ships and even bubbles besides other acoustic devices [20]. For example, the measured bit error rate is 4×10^{-3} for a data rate of 34 kbps over a 1500m-link with 9dB-SNR and 21.25 kHz bandwidth at 85 kHz frequency [53]. Therefore, more bandwidth is needed for reliable transmission in UWANs, resulting in much less bandwidth available for network security.

Electromagnetic wave is the medium for radio signal propagation in WSNs, while water for underwater acoustic signal propagation in UWANs. The latter is affected by the temperature and density of the medium but not for the former. As mentioned earlier, the temperature and density as well as salinity of the current affect underwater acoustic propagation so that even between stationary nodes (e.g., anchored nodes) in UWANs, acoustic channel quality may still change timely. In many radio WSNs, nodes are often stationary [3], and channel quality is relatively stable in this case. This difference along with node mobility in UWANs contributes more dynamics to underwater acoustic channels, making it more difficult to estimate the channel efficiently, resulting in lower channel utilization. This feature worsens the situation of very limited channel capacity available for UWAN security.

Nodes in both WSNs and UWANs are usually battery-operated and it is very difficult to recharge them. However, due to excessive attenuation, communication energy consumption in UWANs is much bigger than in WSNs. For example, for ZigBee, it is about 10 mW and 10 mW∼1000 mW for WiFi. However, in UWANs, tens of Watts are typically required for transmission and up to a few Watts for reception [54]. In this case, UWANs consume much more energy than WSNs for the same communication overhead for network security (e.g., ciphertext expansion discussed in Section VI-A1). Due to expensive network nodes in UWANs (e.g., an acoustic modem with a rugged pressure housing without underwater sensors costs $3k [9]), the node density in UWANs is much smaller with sparser deployment than in WSNs. The distance between nodes in WSNs is up to hundreds of meters, while up to tens of

TABLE II
NETWORK SECURITY THREATS IN THE CONTEXT OF THE LAYERED NETWORK REFERENCE MODEL [55]

OSI layer	Main function	Typical threats†	Defense strategy
Transport Layer	End-to-end transmission control, flow and/or congestion control	Man-in-the-middle (e.g., TCP session hijack), forged ACK	End-to-end authentication and encryption
Network layer	Addressing, routing (congestion control, optional)	Routing attack, packet interception (e.g., black/sink hole attacks)	Routing process authentication, multi-path routing
Data link layer	Medium access control (MAC), error control	Attacks to location, neighborship (e.g., worm-hole, MAC operation), time synchronization	Abnormality detection, neighborship authentication
Physical layer	Signal communication	Channel jamming, signal eavesdropping	Covert communication, cryptographic protection, jamming detection

†: Attack to confidentiality may happen on every layer, and a common defense is to encrypt/decrypt the transmission.

kilometers in UWANs [52], which causes UWANs less sustainable to node failure than WSNs. These features make UWAN operation lifetime more vulnerable than that of radio WSNs to power exhaustion due to security enforcement.

D. Challenges to Attackers

Some features of UWANs also pose challenges to attackers and can be leveraged somewhat in security scheme designs. These features include spare node distribution, low heterogeneity of network nodes, well-planned network deployment with a pre-configuration of security measures [48]–[50], as summarized below.

- There are difficulties in locating a particular node to attack in a sparse UWAN because it is not easy to determine the scale and distribution of a UWAN without any knowledge about it.
- With the current technique, a wideband interfering device will be huge in size and energy-greedy. It is not easy to deploy such an interfering device in the operation area of a UWAN under attack without being detected. Particularly for channel jamming, lack of the knowledge on frequency used by a UWAN makes such attack less effective due to the wideband property of underwater acoustic communication as discussed in Section II-B4.
- The very small acoustic channel also affects the efficiency of certain attacks such as DoS and attacks via repeating trials as discussed in Section VII-A, which shows that low acoustic channel rates may cause an attacker to spend much time to figure out the secret information. Similarly, a channel with a rate much lower than a node computation capacity becomes a bottleneck for DoS attacks launched above the physical layer, while sparse node distributions make distributed DoS (DDoS) attack difficult.

Therefore, UWAN security schemes should also consider the security requirements of applications and leverage the above features to reduce the cost.

III. TYPICAL SECURITY THREATS IN UWANS

There are many security attacks to UWANs as reported in [17], [19], [55], and [56], which are summarized here according to the layer that an attack may be launched as listed in Table II. Generally, attacks may be passive or active according to actions to be taken by attackers in order to complete an attack. With passive attacks, the attacker does not send any signal (e.g., eavesdropping) but has to do with the latter (i.e., jamming). It is difficult to detect passive attacks.

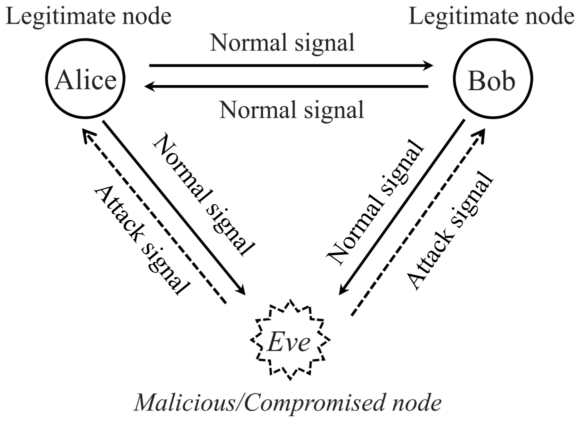

Fig. 4. A default security attack scenario.

Fig. 4 depicts a default security attack scenario, in which Alice and Bob are two legitimate nodes, while Eve is a malicious or compromised node. This default setting will be used in the following discussion if not specified otherwise.

A. Physical Layer Attacks

On this layer, the main active attack is channel jamming,[1] while passive attack is signal eavesdropping.

1) Channel Jamming: One or several attackers emit signals to a channel to interfere the reception of legitimate nodes in order to paralyze the normal communication. Since reliable physical communication is the fundamental of the whole networking operations, the damage of such attack is large and even fatal to the network. If the attacked channel links a special node such as a base station, an access point or a gateway, a successful jamming attack can disrupt the whole network [55].

The effect of such attacks is investigated in [57] and [58] through a real-world field test constructed with own developed jammer hardware and signals, the existing commercial brand acoustic modems and an OFDM modem prototype. In the case of a single attacker, it shows that a UWAN can be easily jammed by carefully timed energy-efficient attacks, with which, the attacker launches jamming once having sensed a transmission activity. This experimental study is extended to

[1] Sometimes such attack is categorized as Denial of Service (DoS). DoS usually refers to attacks targeting at particular nodes attached to a network (e.g., servers) by disabling their normal services.

a collaborative jamming attack in [59], where two or more jamming signals are used in an attempt, showing that collaborative jamming may not be more efficient or effective than a single jamming.

Such attack consumes lots of energy, and is usually easily identified and located, whereas the attacker cannot obtain any useful information. The most effective countermeasure is to eliminate attackers physically. To this end, identification and localization of the attacker have to be carried out first, and then demolishing operation should be enforced. Alternatively, a legitimate node can also increase its transmit power to improve signal-to-interference & noise ratio (SNIR) at the receiver against such attack at the cost of more energy consumption. It is also possible to exploit low-power transmission to tempt a smart attacker to keep attacking until it exhausts its energy.

2) Signal Eavesdropping: An attacker just silently collects signals of an ongoing communication between legitimate nodes by listening. This attack is very easy because wireless communication media are broadcast by nature, and any node can receive the signal from others if it is located in their communication ranges. The collected signals are the fundamental of many other attacks launched at the higher layers. Such attack is very energy-efficient and impossible to be detected.

An analytical model to formulate the probability of eavesdropping attacks in UWANs is discussed in [60] by establishing a relationship between eavesdropping success probability and underwater acoustic channels. This model is validated through computer simulations, which shows that the probability is heavily affected by acoustic signal frequency, spreading factors and node density.

B. Link Layer Attacks

Similar to channel jamming attack, there is also a link jamming attack, with which, an attacker injects many frames into the network at high rates to prevent legitimate users from accessing the medium [61]. If the attacker does not follow the MAC protocol to transmit frames, this attack is just equivalent to channel jamming attack; otherwise, it is a sort of MAC operation attacks. Many other attacks can be launched at this layer, and the typical ones are discussed below.

1) Localization Attack: The typical location information of a node includes positions, relative distances and signal's Direction of Arrival (DoA), which are usually obtained through measurement when GPS is not available. Several attacks can influence successful information collection or the accuracy of the collected information, making a node to appear closer to or farther away from another. Some of such attacks [62] are discussed below with reference to Fig. 4.

- *Replay attack:* Eve intercepts a message sent by Alice to Bob, and then re-sends it to Bob so that Bob gets imprecise locations of Alice caused by the fake propagation time and signal strength. It is due to that distance is usually estimated according to signal arrival time or difference in signal strength. Eve can delay a relay to make it appear farther away from the sender. To this end, Eve needs to jam the normal reception of Alice's signal at Bob if they are close to each other. Eve may also send the response on behavior of Bob before Bob receives a request sent by Alice to make them seemingly closer to each other. These can also be achieved by making transmit power different from the pre-agreed level. The above attacks forge changes in the network topology.
- *Non-Cooperation:* A minimal number of anchor nodes are often required by a localization scheme for location estimation (e.g., three anchor nodes in [63]), while a distributed localization scheme may further require unknown nodes to cooperate in localization [64]. In these cases, if some nodes are compromised or destroyed, which causes the number of functional nodes falls below a threshold, location estimation will fail. A similar attack can also be carried out by providing false positions of anchor nodes or cooperative unknown nodes.

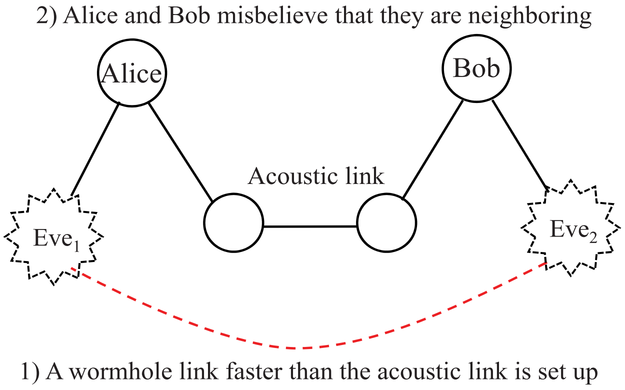
2) Alice and Bob misbelieve that they are neighboring
Alice
Bob
Acoustic link
Eve$_1$
Eve$_2$
1) A wormhole link faster than the acoustic link is set up

Fig. 5. Diagram of wormhole attack.

The performance of localization protocols can be also affected by neighborship attacks discussed below [17].

2) Neighborship Attacks: Such attack aims to establish fake neighborship in order to deviate normal traffic to malicious nodes. For example, Eve can pretend herself as a legitimate node with false link state information (e.g., delay and cost) so that Alice or Bob mistakes Eve as a normal neighbor, and selects Eve as the next hop for routing. Eve can obtain illegally the information routed through herself. Successfully identifying a malicious node through abnormality detection is sometimes difficult because an abnormality may be caused by channel variations rather than attacks [17]. Such attack can be further divided into wormhole attack and Sybil attack.

a) Wormhole attack: As illustrated in Fig. 5, two malicious nodes use an out-band low-latency wormhole link (e.g., RF or wired links) connecting them to create fake neighborship between legitimate nodes [17], [62], [65]. After establishing such a link, one end records packets and forwards them to its colluding end in other parts of the network, which then replays the packets. This attack forges changes in the network topology [62] by either enlarging the neighborhood [66] or shortening the shortest routing path between two legitimate nodes [67]. Furthermore, a wormhole link is most likely selected by routing protocols to set network connections so that the malicious node can have all messages transmitted

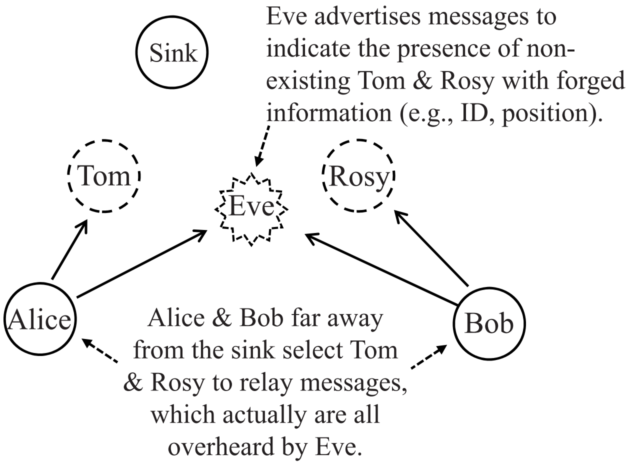
Sink
Eve advertises messages to indicate the presence of non-existing Tom & Rosy with forged information (e.g., ID, position).
Tom
Eve
Rosy
Alice
Bob
Alice & Bob far away from the sink select Tom & Rosy to relay messages, which actually are all overheard by Eve.

Fig. 6. Diagram of Sybil attack.

along the path to monitor the network, and can inject messages or replay received messages with stale information to all connected nodes [17], [55].

Effects of wormhole attacks on UWANs are investigated in [45], which shows that such attacks of any length are low-cost and can disrupt communication in underwater acoustic sensor networks (UWSNs), while existing solutions proposed for RWNs [68] are ineffective. No signal is faster than radio signal, which is exploited by many wormhole countermeasures proposed for RWNs [68] to bound the distance between two nodes. However, acoustic waves propagate at a much slower speed, and network-wise localization incurs significant overhead as shown by a simulation study in [51]. Therefore, effective countermeasure against wormhole attack in UWANs is a challenging issue [45].

b) Sybil attack: As illustrated in Fig. 6, an attacker can forge many identities of legitimate nodes and pretend to be in many places at once [17], [62], [65]. It broadcasts fake messages to mislead the receivers that they have some neighbors, which actually do not exist. The misled nodes will forward packets to these non-existent neighbors so that the attacker can intercept them for further attacks.

3) MAC Operation Attack: This attack aims to disturb or disrupt normal MAC operations or make nodes to consume more energy following the normal operation. For example, with the RTS/CTS handshaking of IEEE 802.11, any node overhearing either an RTS or a CTS should not transmit anything during the time period indicated by the RTS and/or CTS. However, a malicious node may violate this rule by transmitting even after overhearing a CTS destined to other nodes, which causes collision at the receiver. Alternatively, an attacker may repeat sending RTSs to one legitimate node to exhaust its energy with returning many CTSs for the received RTSs [55]. Such attack is more energy-efficient than channel jamming to paralyze the network, and it is more difficult to detect it. For MAC ACKs, a malicious node overhearing frames destined to a node with a weak link or located in a shadow zone sends a fake ACK to the sender [17] so that it will continue sending frames, which actually cannot be received by the real receiver.

4) Time Synchronization Attack: Precise time synchronization is essential to schedule nodes' activities such as transmission, reception, sleeping or wake-up. Attacks to time synchronization process affect the accuracy of the synchronized clocks, which further affects the scheduled operations. Actually, many above-mentioned attacks can affect the accuracy of time synchronization. For example, Sybil, wormhole and replay attacks will cause fake measurement results on ranges or round-trip time (RTT) between legitimate nodes. These results are key parameters for time reference alignment. It is possible to apply cryptographic message authentication to prevent such attacks if attackers have no knowledge of the cipher keys or security procedure [69]. However, it is possible for an attacker to compromise a legitimate node to obtain the necessary secret information. In this case, an attacker can impersonate a neighbor of a legitimate node under synchronizing with its neighbors to launch an insider attack [69].

C. Network Layer Attacks

Typical attacks on this layer include routing attacks and packet interception.

1) Routing Attack: It causes packets unable to be delivered to the destination, and even worse forward them to malicious nodes with fake path information. For example, in a black hole attack (or sinkhole attack), an attacker broadcasts a forged path with the lowest cost or shortest path toward a destination. The receiving nodes select this path which actually goes through the attacker, who can analyze or even drop packets at its will [55]. Such attack becomes easier in wireless ad hoc networks [17] due to broadcast nature of communication media and loose topology control. More smartly, an attacker may drop packets during a certain time period or with a certain percentage to make it difficult to being detected. When multiple nodes are compromised, it is possible to launch collaborative attacks such as distributed DoS (DDoS). Routing process authentication can be used to allow the authorized nodes to exchange routing information, and a new node must pass an identity authentication to join the routing process [55].

Geographic routing protocols are more popular in UWANs because packets are forwarded according to the location information of nodes (e.g., depth) without a dedicated route discovery process. However, such kind of protocol is especially vulnerable to location/neighborship spoofing because broadcast-based information exchange process is vulnerable to the above attacks. Reference [70] investigates effects of location spoofing on a protocol called Depth-Based Routing (DBR) via simulation study, showing its vulnerabilities because the position claimed by a node cannot be verified. Cryptographic schemes are often used to secure routing protocols for integrity, confidentiality and authentication as well as internal attack defense. However, the use of encryption increases not only the size of communication messages but also energy consumption due to high computational complexity. The network wide security key distribution and maintenance are also challenging issues in UWANs due to difficulties in implementing a central node for such purpose [71].

2) Packet Interception: A compromised node, which may be a router, intercepts packets going through it, and selectively drops them or takes other actions. For example, an attacker returns acknowledgments to the source node as if it is the destination node, but drops the corresponding packets. In this case, the destination node cannot receive what are sent to it. An attacker or a compromised node can even inject other packets to the destination node on behavior of the source node [55]. With a man-in-the-middle attack, an attacker secretly relays with possibly modification of the communication between a pair of nodes, and makes them believe that they are directly communicating with each others. By listening to the network and localizing nodes, an attacker can improve attack performance by attacking key nodes such as the root node of a tree topology network [72]. Multi-paths forwarding can be used for defense against packet interceptions but with more bandwidth and energy consumption.

D. Transport Layer Attacks

Many attacks on this layer are related to TCP, e.g., SYN attacks, session attack and man-in-the-middle attack. For example, in a TCP SYN attack, a malicious node floods TCP connection establishment requests (i.e., SYN segments) to a destination node to exhaust its memory. There are several TCP session attacks. For example, an attacker can forges ACKs with fake segment sequence numbers to trigger unnecessary retransmission or block necessary retransmissions [55]. With a man-in-the middle attack, an attacker splits the original TCP connection into two portions so that the attacker can intercept all TCP segments transferred through this connection.

IV. Countermeasures Against UWAN Security Threats

This section reviews some typical schemes proposed to defend UWANs against channel jamming and spoofing attacks. The typical spoofing attacks include location spoofing and neighborship spoofing, which use the false location information of legitimate nodes, impersonate them or even create non-existing nodes to affect the performance of routing and time synchronization. The security of UWAN deployment and restoring the network from the damage caused by attacks are discussed in [73].

A. Channel Jamming

A jamming detection and mitigation scheme is investigated in [61]. Jamming attacks are detected through measuring any abnormality in terms of packet transmission ratio or the amount of energy consumption following the proposal in [74]. Once a jamming attack has been identified, the node sends a high priority packet to its neighbors, and increases sleeping time to save energy. Meanwhile, it also maps a jammed area to prevent data transmission from occurring therein to mitigate jamming effect. Note that the proposed measurement may cause confusion between congestion, jamming and packet losses caused by poor channel quality. All these events may lead to low packet delivery ratios.

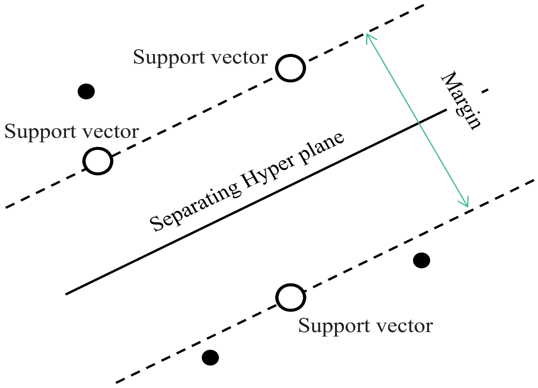

Fig. 7. Attack detection with support vector machine (SVM) [78].

Game theory and reinforcement learning are jointly used to detect jamming attacks by formulating the interactions between underwater nodes and attackers (i.e., players) as an underwater jamming game in [75] and [76]. The players choose their transmit power levels to maximize their individual utilities based on the SINR of the normal signals and transmission costs. The Nash equilibrium of a static jamming game is presented in a closed-form expression for the jamming scenario with known acoustic channel gains. For unknown dynamic underwater environments, a Q-learning-based anti-jamming method is proposed, with which each node chooses its transmit power with no information on the channel gain of the jamming attackers available. Whether such detection method is efficient to smart attackers is an open issue.

Particularly in [76], the above method is used in a hypothesis test based detection for a spoofed MAC address attack in a UWAN, which consists of several sensors at various locations and a surface sink slowly floating in the area. The sink detects spoofing attacks launched by an underwater node through comparing the digital signatures or channel characteristic variance with a test threshold [77]. Once receiving data from underwater nodes, the sink chooses the test threshold in the hypothesis test for spoofing detection. The attacker determines the frequency to send spoofing data. Both players choose autonomously their actions to maximize their utilities in the detection. Simulation results show that the detection method can improve detection accuracy and the utility of UWANs. This detection scheme is complex for high computation load, and infeasible for underwater nodes with limited computation capability and power supply.

A machine learning algorithm using support vector machine (SVM) [79] is studied for attack detection in [78]. An SVM classifies data according to the best fit hyper plane, which divides the entire data points of one class from the others. A so-called margin is the maximum width of the slab parallel to the separating hyper plane, in which no interior data points present as illustrated in Fig. 7. The best-fit hyper plane has the biggest margin between the two classes [80]. The data points nearby the separating hyper plane are called support vectors, which are expected to be on the boundary of the slab [81]. Since SVM is efficient for unreliable data and suitable for the classification of small sample data [79], it is used to classify high-dimension data in UWANs.

With the proposed scheme, during the off-line training phase, the data are gathered from the physical layer to the network layer. The collected data sets are preprocessed by a data trimming scheme to reduce data size before being processed further by SVM, which tries to discover a linear separating hyper plane in the space. The results show that SVM can deliver good result with much smaller training time in comparing with neural networks. The same authors investigate another attack detection scheme based on Dempster-Shafer theory in [82], with which, the probability is described by ambiguity or uncertainty intervals with the following parameters: belief (i.e., the lower bound of the uncertainty interval representing supporting evidence) and plausibility (i.e., the upper bound of the uncertainty interval representing non-refuting evidence) [83]. However, no comparison is given between these two schemes. For both, channels are assumed stable while nodes are stationary, and the system is time synchronized. However, these assumptions may become unrealistic in UWANs.

B. Location Spoofing

The measurement of the distance between neighbors used for localization function in UWSNs can be easily attacked by a jammer. A countermeasure against this attack to localization function is based on a jamming avoidance strategy using a single round distance measurement protocol. This protocol re-executes the communication protocol in the hope to get through when the jammer misses a round for attack [45]. Compared to a multi-round protocol, the single-round protocol re-execution is more practical in UWSNs. The performance of this scheme depends on the attack activity of the jammer.

A silent positioning scheme called UPS (its description is not provided in the reference) is investigated in [64] to improve the robustness for location privacy in UWANs. The time difference in signal arrivals measured locally by a node is used to determine the difference in the ranges between the sensor node and the four anchor nodes. The averaged range differences over multiple beacon intervals are used to estimate the 3D node location via trilateration. The beacon signals are broadcast by the anchor nodes, while the sensor nodes only need to listen. This scheme tries to provide location privacy of underwater nodes to be located without relying on time synchronization. However, the beacon signals can be forged if no signal authentication is in place, which makes the proposed scheme vulnerable to attacks.

C. Neighborship Spoofing

Such kind of attack can be further divided into wormhole and Sybil attacks.

1) Wormhole Attack: With the Distributed-Visualisation of Wormhole (Dis-VoW) protocol investigated in [51], distances calculated according to the signal propagation delay are used to construct a local network topology within two hops. A multi-dimensional scaling scheme is used to visualize distortions in the lengths and angles of edges. To this end, each node needs to collect distance estimation from its neighbors. However, broadcasting messages for distance estimation introduces overheads, and the distance estimation is also vulnerable to attack.

To solve the above problems, a scheme based on the direction of arrival (DoA) of acoustic signals is investigated in [84]. Note that it is not easy for a wormhole attacker to manipulate DoAs but signal power and transmission time. DoAs solely depends on the relative locations of signal transmitters and receivers, and its estimation for a pair of true neighbors needs to satisfy some geometric relationships [84]. So DoA is used in neighbor discovery against wormhole attacks in UWANs without relying on secure and accurate time synchronization, localization and high node density. A key distribution scheme based on the IBC to be mentioned in Section VI-C is assumed available to distribute private keys for signal authentication. However, water current may cause underwater nodes to change their positions frequently in an unpredictable manner, which makes it difficult to determine accurately DoAs for a true pair of neighboring nodes. Although this issue is addressed by a proposed scheme called MA-NDP, it assumes the availability of relative velocities between nodes and their surroundings. How to obtain securely such velocities in underwater environments is an issue.

2) Sybil Attack: An attack detection scheme using the state information of nodes is investigated in [85] by assuming the availability of beacon nodes. Each node is stationary and has the same transmission range over bidirectional links. It works as follows: i) According to the reception status of reply packets, the beacon node judges whether there are suspected Sybil nodes under the normal conditions. ii) The recorded relationship between communication frequency and residual energy is used by the beacon node to detect Sybil nodes. iii) The beacon node determines the suspected node through calculating the related evaluation and comparing two coordinates: one broadcast by the suspected node to the beacon node, and the other calculated according to the distances between the suspected node and the coordinates of three neighbor nodes [85]. The performance of the proposed detection scheme depends on the density of legitimate neighboring nodes.

D. Time Synchronization Attack

A time synchronization protocol is investigated in [69] to resist insider attacks, which cannot be defended effectively by a cryptographic prevention scheme. It is based on a two-step security model. A correlation-based scheme is first used to detect outlier time stamps to find a potential insider attack. Then a long-term statistical trust evaluation is used to identify the real insider attack. This is due to that the distances and propagation delays between neighboring nodes follow a certain probability distribution [86]. Strong correlations between the sending and receiving times should exist. The statistical distribution of the above propagation delays is assumed to be obtained beforehand through training experiments. These assumptions make the scheme not adaptive to dynamic UWANs.

A Cluster-based Secure Synchronization (CLUSS) protocol investigated in [87] works with the following three phases: authentication, inter-cluster and intra-cluster synchronization. It tries to remove malicious nodes as follows: i) Unicast messages are authenticated with unique pair wise keys shared between the related nodes. ii) Broadcast messages are authenticated with digital signatures using public keys. iii) A centered hyper-ellipsoidal SVM (CESVM) [88] is used to detect outlier in a distributed manner. CESVM maps the data vectors to a higher dimensional space, in which a hyper ellipsoid is fitted around the majority of the data vectors. The vectors inside the hyper ellipsoid are classified as normal and those outside as outlier. It also adopts superpower beacon nodes equipped with GPS on the water surface to realize time synchronization. Both pair-wise keys and public keys are used in the authentication process. How these keys are distributed to the relevant nodes are not clearly explained.

V. Securing Communication and Networking Protocols in UWANs

This section reviews some schemes proposed to secure communication and networking protocols to protect confidentiality and integrity in UWANs, which include securing underwater acoustic channels, attack-resilient MAC and routing protocols.

A. Securing Acoustic Channels

The proposals for this part mainly aim to defend acoustic communication against eavesdropping, by exploiting covert communication, interference management and cryptographic methods as discussed below.

1) Covert Communication: It can be used to secure acoustic communication and the transmitter by hiding communication activities with the following properties. An input signal is much weaker than the ambient noise (e.g., -10 dB SNR in the signal band) so that it is difficult for a listener without prior knowledge about the signal to detect it. If the signals are like noise, it is difficult to decode them without a prior knowledge of the structure of the signal [14]. A receiver algorithm is studied for Direct Sequence Spread Spectrum (DSSS) communication between mobile platforms with multi-paths in [89]. An analysis is conducted on the required security level for a given operation area and the corresponding counter detection range by an intruder. The probability of detection by an intruder is minimized due to the decreased SNR outside the operation area. However, covert communication may consume more energy for reception because an amplification of the received signal is necessary for successful decoding.

2) Interference Management: The basic idea of such kind of scheme is to exploit interference to prevent eavesdroppers from successfully decoding the received signal. Two schemes introduced here are Jamming-through-ANC (J-ANC) and one using distributed antenna elements (DAEs) in a coordinated multi-point (CoMP) transmission UWAN.

DS-CDMA is vulnerable to attacks because it is possible for attackers to identify blindly the spreading code used by the legitimate user when neither channel state information (CSI) nor training sequence is available [90]. Reference [14] tries to secure it by using friendly CDMA-based cooperative jammer with analog network coding (ANC). The basic idea of ANC is to allow concurrent transmissions of signals over the wireless medium so that they intentionally interfere with each other to provide covert communications in underwater acoustic channels [91]. As illustrated in Fig. 8, such a jammer transmits the information, which is known a priori to Bob but not to Eve, using the same spreading code as used over the Alice-Bob channel. Although the jammer's frame will interfere the reception at Bob, Bob can suppress the interference to decode Alice's frames by estimating the two multi-path affected channels, whereas Eve cannot.

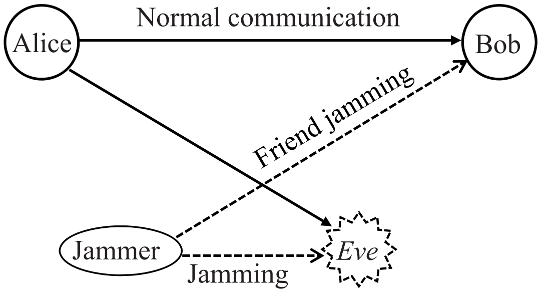

Fig. 8. System model for J-ANC [14].

J-ANC considers a DS-CDMA link between Alice and Bob, and Eve has a better channel quality relative to Bob because she is closer to Alice [14] as illustrated in Fig. 8. Furthermore, Eve has the perfect knowledge of the CSI and the spreading code utilized by Alice and a friendly cooperative jammer. It is selected to transmit the information modulated with the same spreading codes assigned to the Alice-Bob link to make it hard for Eve to intercept the communication. Both Bob and Eve have to remove the jamming signal in order to retrieve Alice's frames. However, Bob knows the information bits transmitted by the cooperative jammer a priori, but not Eve. So Bob can suppress the interference signal and retrieve Alice's frames, but Eve will fail to do so with a high probability. The information transmitted by the jammer needs to be changed frequently and securely in order to prevent it from analysis attacks.

In a CoMP transmission UWAN using DAEs, which are fixed on the bottom and connected by wire lines, and communicate with AUVs, a signal alignment scheme for transmission secrecy is proposed to leverage low sound propagation speed and spatial diversity such that useful signals will collide at the eavesdropper but not at the legitimate user [92]. To this end, the DAE set, transmission schedule and transmit power of each active DAE are jointly optimized to minimize the received SINR of useful signals at the eavesdropper, subjective to the lower bound of the SINR at the legitimate node [92]. Two cases with and without the availability of the location information on the eavesdropper are discussed. However, this scheme cannot assure transmission confidentiality due to the nature of the proposed optimization, which is difficult if the eavesdropper is located near a legitimate node.

3) Cryptographic Protection: The popular RSA encryption scheme is adopted to secure underwater acoustic channels using OFDM modulation to protect confidentiality in [93]. As mentioned earlier, RSA is computationally complex with ciphertext expansion, which consumes lots of energy and bandwidth.

With the scheme proposed in [94], a voice bit stream is encrypted by mapping each frame to a predefined symbol. All symbols are stored in both sides of a communication channel in lookup tables, which was originally designed for hi-fi speech records. For each frame, a unique symbol is produced, and the consequent symbols are windowed, filtered and shaped in order to be transmitted over the channel. To minimize the damage of insider attacks launched by compromised nodes, it is necessary for each pair of nodes to have a unique such table, which should be reconfigured against analysis attack. All these may yield more operational overhead.

B. Attack-Resilient MAC

A secure MAC protocol (SCMAC) for a clustered UWSN is investigated in [95] to ensure data transmission security. The clusters are formed and updated dynamically and securely. After a successful mutual authentication, i) all unicast messages exchanged between nodes are authenticated with the unique pair wise keys shared by them, and ii) broadcast messages are authenticated with the public key based digital signatures [95], similar to the CLUSS mentioned above. Similarly, Reference [96] also tries to secure MAC protocols based on RTS/CTS handshaking by encrypting data frame with a symmetric key algorithm. It seems that both schemes mainly secure data transmission rather than MAC operation following the MAC protocol. For the first one, how a successful mutual authentication can be carried out is not explicitly addressed, and the computation load with public keys and re-keying of pair-wise keys for high security are two issues necessarily for further study. For the second one, how to distribute symmetric keys and re-keying them for high security are not discussed adequately.

C. Attack-Resilient Routing

Three UWAN routing protocols against attacks are introduced here, namely, Secure FLOOD (SeFLOOD), Resilient Channel Aware Routing Protocol (R-CARP) and Resilient Pressure Routing (RPR) protocol. Note that although some proposals are termed “secure routing protocol”, actually they mainly address reliability issue rather than security such as [97]. This kind of protocols are not discussed here, and a detailed survey on transfer reliability can be found in [20].

1) SeFLOOD: FLOOD is a network discovery protocol proposed for a cluster UWAN using flooding. It requires each node to report the information on the link quality such as signal attenuation and link delay to the master. It runs the Dijkstra algorithm with the link quality information to build a routing table, and distributes it to all the nodes [98]. This protocol is vulnerable to several attacks, such as spoofing attack and false information injecting to the report [55].

The SeFLOOD proposed in [99] tries to protect every control message using a cryptographic suite based on the ciphertext stealing technique to be described in Section VII-A. It assumes that a node cannot be compromised physically by an attacker but only being attacked through the network. The main components of SeFLOOD are described below.

- To protect unicast messages between nodes, a link key shared by a pair of neighboring nodes has to be established for each pair of nodes before the routing protocol starts. This key is used to encrypt each unicast message transmitted between the corresponding pair of nodes. It adopts a Link-Key Table (LKT) instead of well-known key agreement protocols (e.g., Elliptic curve Diffie-Hellman [100] or the Blundo [101]) to distribute keys for both simplicity and efficiency. In each node, an LKT stores all the pairwise link keys. This method is said to have an $O(n)$ storage overhead, where n is the number of nodes in a UWAN, and is usually small so that each node has enough memory to store the LKT.
- To protect broadcast messages within a cluster, each node creates a cluster key and distributes it to each member in its cluster secretly by encrypting the cluster key with the corresponding shared link key. This transmission repeats until all the members have been distributed with the cluster key. Similar to the LKT, each node maintains the cluster key for each member of its cluster in a Cluster Key Table (CKT). The node uses the cluster key to authenticate broadcast messages [99].

An LKT should be pre-installed in each node to secure unicast transmission. To reduce the damage caused by a compromised node, a secure resetting LKT is necessary, and this issue is not addressed adequately. A large overhead may be caused by frequently distributing updated cluster keys.

2) RPR: Reference [70] shows that existing geographic routing protocols (e.g., pressure routing) are vulnerable to an insider spoofing attack. With this attack, the entire network traffic can be stopped at specific locations and never reaches the surface due to a fake depth advertised by an attacker, who acts like a legitimate node. The same authors propose the RPR protocol by jointly utilizing cryptographic schemes, geographic constraints and randomization as well as implicit acknowledgments for packet delivery in [102]. To prevent attacks from the deployment area, only nodes knowing the network wide secret key and a legitimate identity can participate in the forwarding process. Nodes outside the current threshold are blocked from forwarding. The thresholds can help to detect fake depth information. However, cryptographic mechanisms cannot prevent insider attacks since such attackers can have all information. So reputation-based authentication makes more sense in this case such as R-CARP discussed below.

3) R-CARP: The CARP [103] is a cross-layer designed routing protocol, which exploits link quality information to achieve robust, energy-aware and adaptive data forwarding. However, it is vulnerable to insider attacks such as the sinkhole attack [104]. That is, if one node becomes malicious or is compromised, it can be chosen as a relay with high probabilities by advertising to its neighbors a high value of the utility function. R-CARP employs digital signatures based on the Boneh-Lynn-Shacham (BLS) scheme to be discussed in Sections VI-D and VII-B2 along with reputation-based mechanism to improve the security [103].

The setup phase of the protocol allows each node to acquire hop-distance information from the sink, with which each node shares the same group key and a unique secret key. When a node has data to forward, it broadcasts a request message (PING) to find the best relay. Once a node receives the PING, it replies with a PONG message containing the estimated information on the hop distance from the sink and link quality, which is estimated according to the number of control and data packets correctly received recently. For each received PONG message, the receiver calculates the reputation of the PONG's sender in terms of ratio N_c/N_f. Here N_c is the number of packets confirmed by the sink that the receiver has forwarded through the sender, and N_f is the total number of packets that the receiver has forwarded through the sender according to the recent history. The higher this ratio, the better is the reputation of the sender. PONG messages are encrypted and authenticated so that any alter on the carried information can be detected. Since forwarded packets without protection may be also forged, how to collect securely the real N_c and N_f is not clear.

VI. Cryptographic Primitives for UWAN Security

Cryptography is the fundamental for network security. Some characteristics of UWANs affects the applicability of the popular cryptographic primitives. This section discusses some basic cryptographic primitives investigated to enable authentication and provide confidentiality, integrity and non-repudiation services in UWANs, after a discussing the main problems of the popular cryptographic primitives.

A. Problems of Cryptographic Primitives

The main problems of the existing cryptographic primitives for UWANs include ciphertext expansion and computational complexity for both asymmetric/public key and symmetric key cryptography, which make them unsuitable for very resource-constrained UWANs as discussed below.

1) Ciphertext Expansion: Message padding and codes for modification identification and message authentication make message length to increase after applying cryptography [10], resulting in an increased transmission time and more consumption of bandwidth and energy. For example, with the Advanced Encryption Standard (AES) [105] encryption, the block size is 128 bits, and the message expansion due to padding would be around 18% for a typical UWAN message of about 720 bits [6]. For message authentication using digital signature, a digest is usually appended to an authenticated message, which also causes expansion and communication overhead. For a digest produced by SHA-256, its size is 256 bits, which causes an additional overhead up to about 35% of an average UWAN message [6].

2) Public Key Cryptography: It is adopted widely in RWNs for symmetric key distributions and digital signature for example. Particularly, for the widely used RSA public-key system, it is computationally intensive with thousands or even millions of multiplication instructions for single cryptographic operation. This causes a resource-constrained wireless device to take an order of tens of seconds or even up to minutes to perform encryption and decryption operations [106]. Furthermore, it usually takes a microprocessor thousands of Nano joules for a simple multiplication operation of a 128-bit result [107]. For real applications, the public modulus should be more than 1024 bits to guarantee security, which causes high energy consumption and makes RSA not suitable for UWANs [108].

3) Symmetric Key Cryptography: A symmetric key cipher is often used to protect confidentiality because of its super cost-efficiency over asymmetric ones. However, the same secret key has to be shared by both the sender and the receiver, which causes difficulties for the generation and distribution of such keys in very resource-constrained UWANs due to difficulties in implementing an online key distribution center for key management. Combining pseudo-random generators and pre-distribution of keys has no true randomness with possible cryptanalytic break. Pre-installing keys on each node has a risk that a single compromised node may make a number of nodes sharing the common key insecure [16].

B. Symmetric Key Generation and Distribution

Here we mainly discuss key generation in reciprocal channels, which is an interesting approach to resolve the symmetric key generation and distribution problem in UWANs.

1) Key Generation for Reciprocal Channels: The randomness of the input parameters for key generation affects the security strength of the generated key. The basic idea behind this key generation scheme is reciprocity theorem, i.e., the secret key between two nodes is generated through sharing a common source of randomness, which is possible even when the quality of the communication channels between them is worse than that with the eavesdropper [109]. The typical sources of the shared randomness include the impulse response of the reciprocal channel, frequency selectivity and Received Signal Strength (RSS) [110]. As illustrated in Fig. 9, the shared randomness of the communication channels between Alice and Bob can be captured by them but not by Eve due to the high correlation in the Alice-Bob channels. Such kind of randomness is usually obtained through measuring the same probing signals sent by Alice and Bob to each other. For example, Alice and Bob transmit a pure tone signal synchronously to each other during a period. The signals received by them are the random sources for generating a shared key.

This key generation scheme can eliminate the need to deploy an additional key distribution center, which makes it attractive in UWANs. It allows a pair of nodes to update secret keys at any time since the randomness of the key generated by this scheme depends on the entropy naturally available in the environment. For example, the two nodes of a reciprocal channel can produce a shared key through local RSS measurements [111]. An adversary can hardly guess the secret key generated by them if it is not physically located near them, and the spatial diversity of a wireless channel can ensure the secret in the key generation [16].

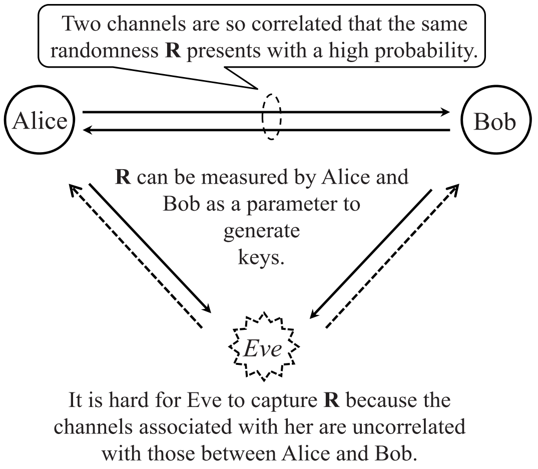
Two channels are so correlated that the same randomness **R** presents with a high probability.
Alice
Bob
R can be measured by Alice and Bob as a parameter to generate keys.
Eve
It is hard for Eve to capture **R** because the channels associated with her are uncorrelated with those between Alice and Bob.

Fig. 9. Principle of symmetric key generation for reciprocal channels.

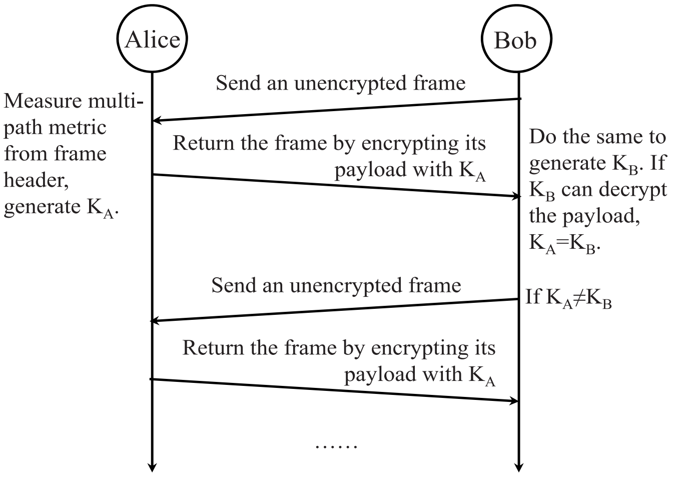
Alice
Bob
Send an unencrypted frame
Measure multi-path metric from frame header, generate K_A.
Return the frame by encrypting its payload with K_A
Do the same to generate K_B. If K_B can decrypt the payload, $K_A=K_B$.
Send an unencrypted frame
If $K_A \neq K_B$
Return the frame by encrypting its payload with K_A
……

Fig. 10. A protocol for symmetric key negotiation in reciprocal channels.

However, the discrepancy between the measurements of Alice and Bob increases with the time interval between when they receive the corresponding probing signals sent to each other, and greatly affects the successful key generation rates. Particularly for time-varying underwater acoustic channels, long propagation delay and low transmission speed increase the time interval. How to overcome this problem to improve key generation performance is still a research issue.

a) Fuzzy information reconciliation: This approach was originally proposed in [112] for RWNs based on the above-mentioned key generation. It uses the deep fading information derived from the envelopes of the received signals as their random sources. Shift differences between Alice and Bob due to time shift and estimation errors are supposed to be corrected by the proposed scheme. Reference [113] expands this scheme to UWANs by further taking into account the peculiar features that affect the performance of the original scheme in UWANs. It tries to correct all kinds of errors for key generation at the cost of more computation and communication. To this end, Alice and Bob transmit a pure tone signal during a period to each other synchronously, and the received signals are the random sources for them to generate the key. However, they will experience different fading characteristics due to the spatial randomness of the channel.

Reference [110] exploits the unique multi-path characteristics between Alice and Bob. The key is the combination of a measured channel multi-path metric and a pseudo random number. The multi-path metric is fed to a k-bit quantizer. An m-bit pseudo random string, which is a function of the packet sequence, is appended at the end of the channel metric to enhance key randomness further, so that the length of the generated key is $k + m$ bits. The key negotiation protocol is illustrated in Fig. 10. Here the key generation time depends on the number of handshaking processes, which is affected by the channel quality.

b) OFDM channels: Reference [114] exploits the channel frequency response of OFDM systems and Bose-Ray-Chaudhuri-Hocquenghem (BCH) codes for information reconciliation in the key generation process. The proposed scheme is validated by a lake test, which shows that the coherence of mutual (reciprocal) channels leads to a high probability of successful key generation. The secret key generation protocol used in lake tests is described below.

- Alice sends two OFDM blocks to Bob: the first one containing the packet number, and second one carrying a probing signal. Once Bob has successfully received them, he replies immediately to Alice the same OFDM probing signal to minimize the interval between the probing signals in order to yield the highest correlation between the mutual channels. Then the decoded packet number is sent to Alice for her to pair the OFDM probing signals.
- Alice first quantizes the observation of the underwater acoustic channel in frequency domain, and uses it to generate the key. Then she sends the syndrome to Bob based on the predefined error correction code, which is used to help Bob to recover the sequences observed by Alice. Bob extracts the keys (generated by Alice) from the received syndrome with the help of the quantized channel frequency response observed by himself. The above two steps repeat until a desired key length is reached.
- Bob generates a hash value of the generated key, and sends it to Alice. She does the same with the same hash function using her generated key as the input. If the two hash values are equal, they have successfully generated a secret key. Then Alice sends a key acknowledgement to Bob; otherwise, the above process is repeated.

Due to noise and channel time variation, the two binary codewords observed by Alice and Bob may not be identical. Thus, a reconciliation process is carried out by error correcting coding following Slepian-Wolf coding [115].

The main problem of such key generation approach is the uncertainty in key generation, which degrades secure transmission performance. Reference [16] evaluates the performance of a variety of RSS-based key generation schemes originally designed for RWNs in underwater environments with the following observations. i) The long transmission time of a probe signal in UWANs results in a low key generation rate. ii) The long propagation delay and large transmission time cause the asymmetry of RSS measurements between two communicating parties more significant in UWANs, which causes a high

TABLE III
KEY LENGTHS (BITS) FOR EQUIVALENT SECURITY STRENGTH WITH TYPICAL CIPHER SCHEMES [123]

Symmetric cipher	ECC cipher	DSA/RSA cipher
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

DSA=Digital Signature Algorithm, RSA=Rivest-Shamir-Adleman

rate of bit mismatch on the shared key. Reference [16] also discusses two proposals to improve the performance of RSS-based key generation with sea trials. The first one is to divide the channel into multiple independent sub-channels, on each of which the RSS measurements can be performed. The second is to use a smooth filter to improve the symmetry of the RSS sequences between two communicating entities. As discussed in [34], dividing a small acoustic channel into sub-channels reduces channel utilization.

2) Key Distribution: It is well-known that symmetric key cryptography outperforms public/asymmetric key cryptography because public key operations are usually an order of hundreds of times more computationally intensive than their symmetric key counterparts [116]. However, network-level key distribution is a hard issue. Thus a key distribution scheme to fit the characteristics of sensors' movement is discussed in [117] to improve the connectivity and security of UWANs. It tries to reduce the redundancy of the key distribution system along with a corresponding secure routing method based on the Focused Beam Routing Protocol (FBR) [118], [119].

C. Public Key Generation

Several non-RSA public-key algorithms have been devised for resource-constrained devices [120], [121]. The typical one is Elliptic Curve Cryptography (ECC) [122] due to its shorter key sizes than other large integer-based algorithms for the same security strength and better computational efficiency [15].

ECC is based on elliptic curves defined by a set of parameters, which are chosen in such a way that it is difficult for an adversary to solve the elliptic curve discrete logarithm problem (ECDLP) in a reasonable time [122]. Table III compares cipher key lengths of some typical cipher schemes for an equivalent security strength. It shows that the key size of ECC is only double the symmetric ones but with a large superior over DSA/RSA ones (DSA is based on discrete logarithm computation). Accordingly, Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Authenticated Encryption Scheme (ECAES) and Elliptic Curve Authenticated Encryption Scheme (ECAES) have also been devised [123]. To match the classical security of RSA, smaller elliptic curve keys are needed so that theoretically it is possible to make a practical attack feasible many years before such an attack to be available on an equivalently secure RSA scheme [124]. Therefore, ECC is expected to be more vulnerable than RSA [125] to attacks using Shor's algorithm [126], which runs on a quantum computer for integer factorization.

TABLE IV
SIGNATURE SIZE, GENERATION TIME AND AUTHENTICATION OVERHEAD OF TYPICAL DIGITAL SIGNATURE SCHEMES [131]

Schemes	Generation time (ms)	Length (bytes)	Overhead
ECDSA	134	40	Largest
ZSS	229	21	Medium
BLS	302	21	Lowest

A study even shows that an asymmetric key protocol using an elliptic curve version of Menezes-Qu-Vanstone (ECMQV) consumes less power than a light-weight symmetric key protocol Kerberos in a standard medium-size WSN because it requires 50% less bits to be exchanged for security purpose [127]. Reference [116] extends this investigation to a UWAN with a typical acoustic transmission rate of 640 bps. It finds that non-interactive identity-based key establishment protocols are most efficient for key distribution in large UWANs. The identity-based cryptography (IBC) aims to simplify certificate management by using an arbitrary string identity uniquely identifying a user (e.g., an e-mail address) as a public key. However, the user cannot compute the corresponding secret key anymore in this case, and must authenticate itself to a key generation center to obtain the corresponding private key via a secret channel [128].

In [15], assembly codes are used to implement the modules of ECC in a Digital Signal Processor (DSP) for all performance-critical operations, i.e., finite field addition, subtraction, multiplication, and modular reduction. The experiments show that it takes 0.81 ms to perform a random point multiplication, 4.7 μs and 4.5 μs for point addition and doubling, respectively. These results indicate a feasibility of adopting ECC algorithms in UWSNs, where the underwater nodes are equipped with DSP. However, no results on energy consumption are reported.

D. Digital Signature

Three digital signature schemes, namely, ECDSA, Zhang-Safavi-Naini-Susilo (ZSS) [129] and Boneh-Lynn-Shacham (BLS) [130], are evaluated for UWSNs in terms of energy efficiency in [131]. Both BLS and ZSS are short signatures, i.e., the signature sizes are about 160 bits with a security level of 280. The signature generation is computationally efficient. BLS also supports signature aggregation to accumulate signatures from different signers and on distinct messages into a single short value. Signatures shorter than 160 bits have also been studied. The two typical independent security parameters of these schemes, i.e., the extension degree and the degree of the hidden polynomial, can make them more flexible than ECC-based schemes. The first can be set small to achieve shorter signatures, while the second one can be tuned independently to achieve the desired security level [122]. Furthermore, ECDSA is a de facto standard in ECC. The above features make these schemes possible candidates to be used in UWANs [131].

Table IV summarizes the main characteristics of these digital signature schemes in terms of key generation time and key length as reported in [131] for a 80-bit security, which is equivalent to the security strength of RSA-1024. Only an end-to-end authentication scenario is considered, with which, signature will be verified by a resource-rich end point. These signature schemes are not suitable for link-layer authentication at intermediate nodes due to their constraint resources and computing capability. Instead, various Message Authentication Codes ($\mathbb{MAC}$) schemes can be used because they are computationally efficient with approximately the same amount of processing and equivalent size codes for a given security level [132]. The results show that schemes performing well in RWNs may not do equally well in UWSNs, and BLS presents the lowest overhead while ECDSA yields the largest [131].

E. Authentication

Authentication is usually carried out through encryption and decryption operations, which are computationally complex with high energy consumption. Another type of authentication using reputation/trust models tries to measure the abnormality based on statistics as discussed below.

1) Encryption-Based Authentication: Reference [108] investigates a low computational complexity authentication scheme for a cluster UWAN based on Vandermonde matrix, which is a matrix with a geometric progression in each row. The matrix multiplication used by an authentication scheme can be replaced by matrix addition to reduce computation overhead. By additionally using orthogonal vectors, the scheme adopts matrix addition to generate key configuration. When a node communicates with each other, the identifications of the nodes sharing the key are verified with a zero-knowledge proof protocol, with which no information apart from the true statement is conveyed from the prover to the verifier. The base station randomly selects Vandermonde vectors (VVs) to generate polynomial for the secret key, and then distributes the configuration (e.g., polynomial, VVs, symmetric matrix and random numbers) to each node. A shared key is generated when two nodes communicate with each other.

2) Reputation-Based Authentication: The Attack-Resistant Trust Model based on multidimensional trust Metrics (ARTMM) [133] uses a reputation model, which takes into account the characteristics of underwater acoustic channels and node's mobility. This model consists of the following components:

- Link trust is assessed according to link quality and link usage. Link quality is measured jointly by packet loss rate (P_l) and packet error rate (P_e), which are determined by channel error rates, i.e., $L_q = (1 - P_l)(1 - P_e)$. Link usage is the ratio of a link that has been used during a time window.
- Node trust is evaluated by node honesty and the residual energy available in the node. Node honesty is measured according to the numbers of successful and unsuccessful communications via the node.
- Data trust (T_{data}) depends on link quality and node honesty. To calculate T_{data}, it assumes that the mean is supposed to be the most trusted one with the highest trust value for a set of data.

A fuzzy membership function trust value based on the interdependency property of the three trust parameters is further defined by the following fuzzy sets: {completely untrust with $trustvalue \in [0, 0.25)$, untrust with $trustvalue \in [0.25, 0.5)$, uncertainty with *trustvalue* $= 0.5$, trust with *trustvalue* $\in$ (0.5, 0.75) and completely trust with *trustvalue* $\in$ [0.75, 1]}.

The main weaknesses of ARTMM are summarized below. i) The complexity of the algorithms invokes lots of computation. ii) Some parameters provided by nodes under evaluation for security (e.g., residual energy) may be vulnerable to attacks, or the source node of data may be compromised or even an attacker. iii) The fuzzy set definitions are subjective, and cannot be adaptive to dynamic UWANs. As pointed in [134], the trust evidence generation does not take into account the influences of malicious attacks, and the fuzzy logic method cannot well describe the uncertainty of the trust relationship with a definite real number. Such uncertainty actually presents fuzziness and randomness among underwater nodes especially strange nodes.

A trust model based on cloud theory (TMC) is proposed in [134] and [135] to solve the above problems. The cloud model is based on the traditional fuzzy set and probability statistics theory [136], and can better evaluate the uncertainty of trust relationship. It claims that this model is good for not only the combination of multiple trust attributes, but also the calculation of recommendation and indirect trust values. However, this enhancement assumes the availability of the position information of each node in UWANs.

VII. Structures for UWAN Security

Several security structures have been proposed to provide a set of security services in UWANs simultaneously for confidentiality, integrity, authentication and non-repudiation along with attack-resilient networking protocols as introduced below.

A. A Cryptographic Suite

A cryptographic suite is proposed for a clustered UWAN comprising stationary and mobile nodes as well as a gateway in [6] and [137]. It is further investigated and tested for the group communication of a underwater vehicle team in [138]. It aims to allow a node to join the system to start a mission and leave after the event easily with a support of secure reconfiguration to handle node's mobility. The suite consists of a secure routing protocol and a set of cryptographic primitives (i.e., cipher, digest and re-keying), which are used to secure underwater communication in one-to-one and one-to-many modes via the gateway, considering the characteristics of underwater acoustic channels as described below. The field test results show that the communication and energy consumption overhead introduced by the security measurements is limited and sometimes negligible [6], [137].

- *Confidentiality:* The cipherText Stealing technique is used for encryption by altering the processing of only the last two blocks of a plaintext. Basically, it "steals" a portion of

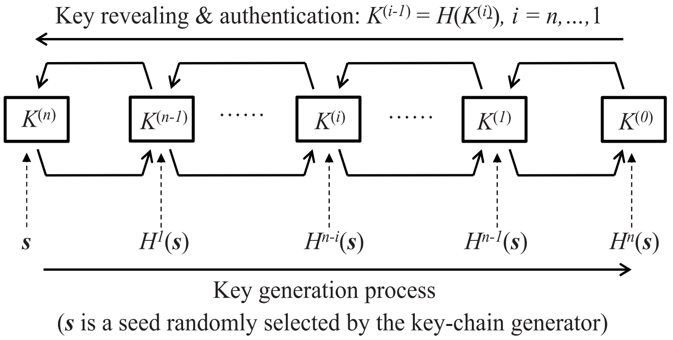
Key revealing & authentication: $K^{(i-1)} = H(K^{(i)})$, $i = n, ..., 1$
$K^{(n)}$
$K^{(n-1)}$
......
$K^{(i)}$
......
$K^{(1)}$
$K^{(0)}$
s
$H^1(s)$
$H^{n-i}(s)$
$H^{n-1}(s)$
$H^n(s)$
Key generation process
(s is a seed randomly selected by the key-chain generator)

Fig. 11. Key chain for group key management [6]: $K^{(j-1)} = H(K^{(j)})$, and $K^{(i)} = H^{n-i}(s)$, where $H^i(s)$ means applying i times $H()$ to s.

the second-last block's ciphertext to pad the last plaintext block, which is then encrypted as usual without ciphertext expansion [139].

- *Integrity:* It uses a 4-byte digest through truncating the real hash function value such that the overhead becomes around 4.4% of the average UWAN message without harm to security [140]. It is pointed that in this case, an attacker has 1 in 232 chances to blindly forge a digest, and maximally needs to repeat 231 trial transmissions to the authorized receiver to break a digest. In a UWAN with a 500-bps channel, sending 231 trial messages each with 184 bits requires about 306 months.
- *Group key management:* It is based on a key-chain scheme, which is a set of symmetric keys and each key is the hash value of the previous one in the key generation process as illustrated in Fig. 11. That is, given a key in the key-chain, one can compute all the previous keys but not the reverse ones. Once a node leaves the system, the gateway generates and distributes a new group key to prevent the leaving one from reading new messages. The secure and scalable rekeying protocol (S2RP) employing an one-way hash function for resource-constrained devices [141] is adopted here for rekeying due to the following advantages. It provides an efficient proof of key authenticity by computing a digest without requiring additional information. The number of rekeying messages logarithmic in the number of nodes makes the key distribution highly scalable [6].
- *Secure routing:* The SeFLOOD [99] discussed in Section V-C1 is used here to distribute the cluster keys. It also supports mobile nodes without adding overheads in terms of the number of messages. Nodes are assumed loosely time synchronized because they need to emerge periodically to synchronize with GPS. After revoking the group key, the gateway deletes the compromised node from the routing tables, and re-calculates the related paths to secure data forwarding.

The key exchange process of this cryptographic suite is vulnerable to spoofing attacks. Reference [142] tries to improve the process security for a clustered UWAN, in which all the nodes are within the communication range of each other or the cluster head. It adopts a public key based scheme to secure key exchanges, and fully relies on the information pre-stored in the related nodes before UWAN deployment. For example, a cluster-member must store a private-key of its own and a public-key of the cluster head. The head has to store a private-key of its own and a secret message to be used in the authentication key exchange process. It does not discuss the effect of compromised nodes on UWAN security.

B. A Security Framework

A Security Framework for Underwater acoustic sensor Networks (SecFUN) is investigated in [122]. It is based on the building block Galois Counter Mode (GCM) [143] for encrypting and authenticating data with a 128-bit block cipher such as the AES. The following features of GCM make it abstractive to UWANs. i) No ciphertext expansion problem exists for authentication but with only a small tag ($\leq$ 128 bits), which is also used to verify the integrity of an encrypted data to avoid any decryption operations. ii) The authenticated-only message mode (GMAC) of GCM is used when no encryption is required. iii) For a changed data, it is possible to access only the changed portions for recomputing authentication tags. iv) GCM has been designed to support message authentication in one pass. A transfer procedure to encrypt/decrypt the aggregated data in UWSNs is also discussed in [144] to provide security for a tree topology UWAN.

1) Symmetric Key Based Authentication: The Message Authentication Codes ($\mathbb{MAC}$) in the Galois field is used to provide the authentication and integrity of messages. A symmetric key, an initialization vector and a plaintext as well as an additional data to be authenticated compose the inputs of GCM. GCM yields the corresponding ciphertext and an authentication tag used to verify the integrity and authenticity of the encrypted data. The tag can be verified without any decryption operations, and its length ranges from 0 to 128 bits, depending on the required security level, with 64$\sim$128 bits being recommended [143].

2) Asymmetric Key Based Authentication: ECC-like schemes using a bilinear map with pairing-based cryptography are used to provide digital signature. Particularly, the BLS and ZSS schemes can provide signatures of 160 bits for a security level of 280, while 128 bits with Quartz [145], which however yields expensive signature generation. This is because the signature generation with Quartz needs to compute four roots of polynomials and multiply two affine polynomials [122].

3) Routing Protocol: SecFUN also extends the CARP mentioned earlier to support security with the AES-GCM encryption (Se-CARP). A node shares the same group key with each other, and has a unique key with the sink [103]. This unique key is used to encrypt and authenticate all the packets exchanged with the sink. Short digital signatures (e.g., BLS, ZSS and Quartz) are also adopted to provide source authentication with non-repudiation at the application layer [103].

C. A Software Defined UWAN

Reference [146] discusses how to leverage the Software Defined Network (SDN) approach (www.opennetworking.org) to improve UWAN security for the ARTMM mentioned in Section VI-E2. With SDNs, the network control functions are centralized to allow a simple and efficient management of the nodes via software with open and flexible interfaces to the nodes. Basically, the control plane of SDNs can help detecting abnormality and mitigating the impact by instructing the network nodes to overcome the problem, or ignore the data reported by untrusted nodes [147]. Furthermore, the global view available at the control plane also provides a better understanding of the security situation for proper actions. A detailed structure is presented in [71] and [110] with the following components but without validation.

1) Jamming-Resilient Communication: Although encrypted reliable and robust waveforms at the physical layer can secure communication, it is still vulnerable to jamming attacks. A cognitive scheme based on network cooperation is proposed to improve network adaptability to changing environments by monitoring the status of the system and attacks. The cooperation of stationary and mobile nodes is a key to improve defense efficiency by exploiting node mobility to adapt the network topology following on-going attacks. This can help avoiding a single point of failure and to enable energy-efficient data transfer.

2) Multi-Metric Reputation Model: To evaluate reputation, a node usually keeps a reputation value for each its neighbor, which is evaluated according to the historical information, such as the success of the past transmissions [71], [110]. However, security attacks such as wormhole attacks can make two far-away nodes to falsely believe neighboring. Thus, a multi-metric based reputation scheme is proposed to consider jointly the following aspects: channel unreliability, possible attacks, energy consumption and node mobility [146].

3) Adaptive Secure UWAN Deployment: The requirement of network security levels vary for different applications and adaptive deployments are necessary. For example, some applications (e.g., military, coastguard and homeland security) want to keep the UWANs undetected, while some others (e.g., scientific and industrial operations) mainly want to secure communications with no need of remaining incognito. A discussion on these issues is provided in [146].

VIII. Discussion

Table V summarizes the main UWAN security schemes reviewed in Sections VI–VII. Several interesting approaches taking into account the peculiar features of UWANs have been investigated, such as friend jammer against signal eavesdropping (e.g., J-ANC [14]), DoA-based countermeasure against wormhole attacks (e.g., [84]), reputation-based authentication (e.g., ARTMM [133]), symmetric key generation in reciprocal channels (e.g., [113]) and energy-efficient cryptographic primitives (e.g., ECC [15]). There are also some proposals aiming to address several security issues in UWANs systematically, such as [137]. However, several important issues have not been addressed adequately as discussed below.

A. Strategic Framework of UWAN Security

So far no strategic framework is available to guide the distribution of UWAN security functions for cost-effective security enforcement in UWANs by taking into account the peculiar features of UWANs. As mentioned above, network security is a complex issue that spans from the physical layer to the application layer. Particularly for the reviewed UWAN security proposals, they actually focus on the physical layer to the network layer, while no transport layer security schemes are investigated so far. This situation is similar to the reliable transfer issue in UWANs as discussed in [20] because long propagation delays significantly degrade TCP performance (See Section VIII-B). Actually, many schemes using TCP have been investigated to provide reliable transport services in WSNs (e.g., [148]), and similarly for using end-to-end security schemes to secure WSNs (e.g., TLS in [149]). As discussed in Section II-C, in comparison with WSNs, UWANs are more resource-constrained in communication bandwidth, and many environmental differences besides much longer propagation delays and much larger communication energy consumption affect protocol design in UWANs. In this case, a strategic framework able to provide an optimal distribution of various security functions among the layers is important to minimize resource consumption without jeopardizing security.

The above issue has not been addressed in the literature, leading to redundant functions proposed on different layers for the same security objective. For example, to protect communication confidentiality in UWANs, we can find different schemes are investigated for the physical layer (e.g., [93], J-ANC [14]), the data link layer (e.g., SCMAC [95]) as well as the network layer (e.g., secure routing protocols). However, to protect end-to-end confidentiality, if there is no guarantee that per-hop confidentiality can be provided by each hop through either the physical layer or the data link layer, the path-level confidentiality must be in place via either the network layer or the transport layer (e.g., secure TCP). In this case, these functions implemented on the physical layer and/or the data link layer to protect confidentiality become redundant, wasting very constrained UWAN resources. A similar situation may occur for per-hop authentication versus end-to-end authentication. A possible optimized distribution of security functions can allow the physical layer to focus on defending UWANs against channel jamming attacks, and the data link layer to control medium access to the legitimate nodes, while the network layer or above is responsible for confidentiality protection.

B. High-Layer UWAN Security

High-layer security can be provided by the transport or application layers. The above discussion shows that UWAN security schemes investigated so far mainly focus on the low three layers, taking into account peculiar UWAN features. However, it is difficult for the low layers alone to guarantee end-to-end security. An efficient high-layer security scheme can simplify intermediate nodes in securing UWANs, and can also provide on-demand and differentiated security services

TABLE V
SUMMARY OF THE SURVEYED UWAN SECURITY SCHEMES (IN THE ORDER OF REVIEWING)

Scheme/Ref.	Items	Key points	Remarks
	Threats	Countermeasures against typical threats	
[61]	Jamming attack	Jamming detection through abnormality measurement	Possible misjudgement on jamming attack events
[75]		Game theory and reinforcement learning jointly used to detect jamming attack	Open issues on detecting smart attack
[76]		A hypothesis test of a method [75] in a UWAN	Complex with high computation load
[78]		Support vector machine (SVM) used in attack detection	Difficult assumptions: stable channels, stationary nodes, synchronized system time
[82]		Dempster-Shafer theory used for attack detection	
[45]	Location spoofing	Jamming avoidance realized by a single-round protocol	Performance affected by the jammer's activity
UPS[64]		Anchor nodes used to broadcast beacons while nodes listen silently	The beacon signals can be forged without authentication.
Dis-VoW[51]	Wormhole attack	Visualizing distortions in the lengths and angles of edges for attack detection	Insecure distance estimation may affect detection accuracy
[84]		Signal's direction of arrival (DoA) which is not manipulatable is used in attack detection	Affected by unpredictable node mobility caused by water currents
[85]	Sybil attack	A special node used to broadcast beacon messages for attack detection	Affected by the availability of beacon nodes and node density
[69]	SYN attack	Statistical correlation between sending and receiving times used in attack detection	Poor protocol adaptability to dynamic UWANs
CLUSS[87]		Centred hyper ellipsoidal SVM used to detect outlier	More study needed for key distribution process
	Schemes	Securing communication and networking protocols	
[89]	Securing acoustic channel	Convert communication used against eavesdropping	More reception energy for signal amplification
J-ANC[14]		Jamming signal used to interfere the reception of eavesdroppers	Large overhead for changing jamming signals for high security
[92]		Signal aligned to minimize SINR at eavesdroppers	No guarantee on confidentiality protection
[93]		Rivest-Shamir-Adleman (RSA) used to encrypt and decrypt signals	Large overhead for computation and bandwidth with more energy consumption
[94]		Table used to store keys to encrypt/decrypt signal	Possible large overhead to secure reconfiguartion
SCMAC[95]	Attack-resilient MAC	Securing MAC frame transmission rather than MAC operation	High computation for public/pairwise keys, unclear symmetric key distribution & rekeying processes
[96]			
SeFLOOD[99]	Attack-resilient routing	Cryptographic protection of every control message	Big overhead for key updating, unclear rekeying process
RPR[102]		Cryptographic authentication for forwarding process	Difficulties in preventing insider attacks
R-CARP[103]		Cross-layer designed with reputation-based authentication	Open issues on securing information collection for reputation evaluation
	Primitives	Cryptographic primitives	
[113]	Symmetric key generation and distribution	Using fuzzy information reconciliation with deep fading information as random sources in RCs	Large overheads of computation and communication with more energy consumption
[110]		Combining a measured channel multipath metric and random numbers to enhance key randomness in RCs	Probably long key generation time
[114]		Exploiting OFDM channel frequency response and BCH codes for information reconciliation in RCs	Probably large overhead for key generation
[16]		Jointly using multichannel and smooth filter	Low channel utilization
[116]	Public key generation	Showing the efficiency of identity-based key establishment in UWANs	Requiring a pre-established center and secure channel
[15]		DSP implementation of the Elliptic Curve Cryptography (ECC) module for UWSNs	Showing the feasibility of the adopted algorithms in UWSNs
[131]	Digital signature	Three digital signature schemes evaluated for end-to-end authentication with BLS yielding the lowest overhead	
[108]	Authentication	Matrix multiplication replaced by matrix addition for authentication	Reduced computation overhead and energy consumption
ARTMM[133]		A reputation-based authentication model considering underwater acoustic channel characteristics	Complexity with measurements vulnerable to attack
TMC[134]		A cloud theory based trust model used to enhance ARTMM	Better evaluation of trust relationship uncertainty, requiring node's position information
	Structures	Security structures	
[137]	Cryptographic suite	Providing confidentiality and integrity with group key management and secure routing protocol	Field tested with open issue on secure key distribution process
SecFUN[122]	Security framework	Providing symmetric/asymmetric-key based authentication, digital signature and secure routing protocols	No field test results are reported
[71]	Software defined UWAN	Using SDNs, jamming-resilient communication, multi-metric reputation and adaptive secure deployment	No validation results are reported

BCH=Bose-Ray-Chaudhuri-Hocquenghem, BLS=Boneh-Lynn-Shacham, DSP=Digital Signal Processor, RC=Reciprocal Channel, SDN=Software defined network, UWSN=Underwater Acoustic Sensor Network

according to application requirements. However, as mentioned earlier, the current high layer security schemes are computationally complex with cipher expansion, which results in more consumption of bandwidth and energy. Furthermore, end points in a UWAN may be asymmetric in terms of computing capability and resource capacity, such as the difference between a surface gateway and an underwater sensor node, end-to-end security schemes for UWANs need an investigation.

C. Cryptographic Primitives Suitable for UWANs

For cryptographic primitives, some proposals such as ECC have been shown more energy-efficient with less computation complexity than the popular ones adopted in RWNs (e.g., RSA). Their performance in real UWANs needs more tests in terms of energy consumption as well as the effect of no availability of the required special nodes in UWAN networking environments. Due to difficulties in establishing a public key facility in UWANs, symmetric key based security schemes become more important, whereas the key generation and distribution in UWANs need further study for such environments. Although properties of reciprocal channels can be leveraged to achieve the above purpose, successful key generation rates need to be further improved with less communication overhead. The feasibility of such approach also requires more study for asymmetric underwater acoustic channels due to uncertainties in connectivity.

For the authentication based on reputation models, several issues need to be addressed before such kind of scheme can be applied in practice. For example, how to secure the information collection process used in reputation evaluation, how to distinguish between abnormality due to attacks and that caused by malfunctions of nodes, and how to set the thresholds used by such schemes.

D. Operational Conditions

Some revised schemes assume the availability of precise time synchronization or the location information of nodes, both which are difficult issues in UWANs as discussed in [34]. Furthermore, the processes used to provide these services may also suffer from attacks and themselves become security vulnerability as discussed in Section II-C2. Some schemes also assume the availability of special nodes for security enforcement such as beacon nodes, which limits their application. Furthermore, how to protect these special nodes from attacks is another important issue, which however has not been addressed adequately.

On the other hand, some peculiar features of UWANs also pose challenges to attackers as discussed in Section II-D, which may be leveraged in designing cost-effective countermeasures to some threats. For example, small communication channels make it difficult to launch DoS attacks to nodes attached in a UWAN through the normal network services, and similar for attacks through repeating trials as discussed in Section VII-A. These discussions also show that it is very difficult to counter against the signal jamming attack although several proposals have been investigated to detect the ongoing attacks and avoid transmissions during a jamming period. However, unlike WSNs, underwater acoustic transmission consumes much large energy, which can be leveraged to paralyze a jamming attacker by exhausting its energy in UWANs.

E. Securing Configuration Resetting for Security

Due to the special networking environment of UWANs mentioned in Section II-C2, it is very difficult to figure out whether a deployed UWAN is compromised or not, while it is almost impossible to detect some ongoing attacks such as eavesdropping. In this case, frequently resetting security configuration of a deployed UWAN is important in order to remove the effect of adversary or compromised nodes for UWAN security. Such reconfiguration is especially important to the security configuration pre-installed during the network deployment to maintain UWAN security. It is also useful to handle the changes in a deployed UWAN caused by node's joining and leaving. Obviously, the resetting process itself must be secure, whereas how to secure the resetting process is ignored by many revised schemes.

IX. CONCLUSION

This paper reviews some security approaches and schemes proposed for UWANs, which are usually deployed in harsh underwater environments with much constrained network resources and large communication energy consumption. The survey focuses on countermeasures against the typical attacks, securing the main network protocols such as MAC and routing, cryptographic primitives with less cryptographic overhead and less computing operations, key generation and distribution feasible for UWANs, as well as security suites that systematically address several security issues.

Note that, only a few of the revised proposals have been tested in practical underwater environments, such as those discussed in [58], [114], and [138], while the overwhelming majority are theoretical studies. Since underwater acoustic networking environments are complex and dynamic, it is difficult to efficiently model them, and the effective validation method is field test. Therefore, the research of UWAN security is still in an early stage, and more researches with practical tests are necessary. In this case, a strategic framework for efficient cooperation among different layers is important to minimize resource consumption for a required security strength. On the other hand, some features of UWANs also impose challenges to attackers, and should be leveraged in enforcing UWAN security. A UWAN may be designed for particular applications, while different applications have different security requirements, which can be taken into account in designing practical UWAN security schemes.

REFERENCES

[1] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 4, pp. 2–28, 4th Quart., 2005.

[2] Z. S. Bojkovic, B. M. Bakmaz, and M. R. Bakmaz, "Security issues in wireless sensor networks," *Int. J. Commun.*, vol. 2, no. 1, pp. 106–115, 2008.

[3] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.

[4] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM Mobile Comput. Commun. Rev.*, vol. 11, no. 4, pp. 34–43, Oct. 2007.

[5] H. F. Jiang and Y. Xu, "Research advances on security problems of underwater sensor networks," *Adv. Mater. Res.*, vols. 317–319, pp. 1002–1006, Aug. 2011.

[6] G. Dini and A. L. Duca, "A secure communication suite for underwater acoustic sensor networks," *Sensors*, vol. 12, no. 11, pp. 15133–15158, Nov. 2012.

[7] M. Stojanovic, "Optimization of a data link protocol for an underwater acoustic channel," in *Proc. MTS/IEEE OCEANS*, Brest, France, Jun. 2005, pp. 68–73.

[8] I. F. Akyildiz and X. D. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23–S30, Sep. 2005.

[9] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," in *Proc. ACM Int. Workshop Underwater Netw. (WUWNet)*, Los Angeles, CA, USA, Sep. 2006, pp. 17–24.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[11] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[12] T. Melodia, H. Kulhandjian, L.-C. Kuo, and E. Demirors, "Advances in underwater acoustic networking," in *Mobile Ad Hoc Networking: The Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds. Hoboken, NJ, USA: Wiley, 2013, ch. 23, pp. 804–852.

[13] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[14] K. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing underwater acoustic communications through analog network coding," in *Proc. Annu. Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw. (SECON)*, Singapore, Jul. 2014, pp. 266–274.

[15] H. Yan, Z. J. Shi, and Y. Fei, "Efficient implementation of elliptic curve cryptography on DSP for underwater sensor networks," in *Proc. Workshop Optim. DSP Embedded Syst. (ODES)*, Seattle, WA, USA, Mar. 2009, pp. 7–15.

[16] Y. Luo, L. N. Pu, Z. Peng, and Z. J. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, Feb. 2016.

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

[18] M. A. Habib, M. J. Uddin, and M. Islam, "Safety aspects of enhanced underwater acoustic sensor networks," *Int. J. Emerg. Tech. Adv. Eng.*, vol. 2, no. 8, pp. 385–390, Aug. 2012.

[19] G. J. Han, J. F. Jiang, L. Shu, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, Aug. 2015.

[20] S. M. Jiang, "On reliable data transfer in underwater acoustic networks: A survey from networking perspective," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1036–1055, 2nd Quart., 2018.

[21] R. Hunt, "Network security—Systems and architecture 2003," in *Proc. Total Focus Conf.*, Singapore, Mar. 2003. [Online]. Available: http://www.cosc.canterbury.ac.nz

[22] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (RADIUS)," Internet Eng. Task Force, Fremont, CA, USA, RFC 2865, Jun. 2000.

[23] A. DeKok and A. Lior, "Remote authentication dial-in user service (RADIUS) protocol extensions," Internet Eng. Task Force, Fremont, CA, USA, RFC 6929, Apr. 2013.

[24] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn, "Diameter base protocol," Internet Eng. Task Force, Fremont, CA, USA, RFC 6733, Oct. 2012.

[25] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," Internet Eng. Task Force, Fremont, CA, USA, RFC 6101, Aug. 2011.

[26] T. Dierks and C. Allen, "The transport layer security (TLS) protocol, version 1.2," Internet Eng. Task Force, Fremont, CA, USA, RFC 5246, Aug. 2008.

[27] S. Kent and K. Seo, "Security architecture for the Internet protocol," Internet Eng. Task Force, Fremont, CA, USA, RFC 4301, Dec. 2005.

[28] S. Bellovin, "Guidelines for specifying the use of IPsec version 2," Internet Eng. Task Force, Fremont, CA, USA, RFC 5406, Feb. 2009.

[29] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," Internet Eng. Task Force, Fremont, CA, USA, RFC 3748, Jun. 2004.

[30] *Port Based Network Access Control*, IEEE Standard 802.1X, 2004.

[31] *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*, IEEE Standard 802.1AE, Aug. 2006.

[32] P. C. Etter, *Underwater Acoustic Modeling, Principles, Techniques and Applications*, 2nd ed. London, U.K.: E & FN Spon, 1996.

[33] M. Stojanovic, "Underwater acoustic communications: Design considerations on the physical layer," in *Proc. Annu. Conf. Wireless Demand Netw. Syst. Services (WONS)*, Garmisch-Partenkirchen, Germany, Jan. 2008, pp. 1–10.

[34] S. M. Jiang, "State-of-the-art medium access control (MAC) protocols for underwater acoustic networks: A survey based on a MAC reference model," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 96–131, 1st Quart., 2018.

[35] J. C. Preisig, "Acoustic propagation considerations for underwater acoustic communications network development," in *Proc. ACM Int. Workshop Underwater Netw. (WUWNet)*, Los Angeles, CA, USA, Sep. 2006, pp. 1–5.

[36] J. A. Catipovic, "Performance limitations in underwater acoustic telemetry," *IEEE J. Ocean. Eng.*, vol. 15, no. 3, pp. 205–216, Jul. 1990.

[37] M. Lanzagorta, *Underwater Communications*. San Rafael, CA, USA: Morgan & Claypool, 2012.

[38] M. Stojanovic, "Underwater acoustic communication," in *Wiley Encyclopedia of Electrical and Electronics Engineering*, Wiley, 1998, pp. 688–698.

[39] A. A. Syed and J. Heidemann, "Time synchronization for high latency acoustic networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006, pp. 1–12.

[40] D. Makhija, P. Kumaraswamy, and R. Roy, "Challenges and design of MAC protocol for underwater acoustic sensor networks," in *Proc. Model. Opt. Mobile Ad Hoc Wireless Netw.*, Apr. 2006, pp. 1–6.

[41] G. E. Burrowes and J. Y. Khan, "Investigation of a short-range underwater acoustic communication channel for MAC protocol design," in *Proc. Signal Process. Commun. Syst. (ICSPCS)*, Gold Coast, QLD, Australia, Dec. 2010, pp. 1–8.

[42] K. Kredo, II, P. Djukic, and P. Mohapatra, "STUMP: Exploiting position diversity in the staggered TDMA underwater MAC protocol," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 2961–2965.

[43] P. A. van Walree and R. Otnes, "Ultrawideband underwater acoustic communication channels," *IEEE J. Ocean. Eng.*, vol. 38, no. 4, pp. 678–688, Oct. 2013.

[44] J. Catipovic and S. Etchemendy, "Development of underwater acoustic modems and networks," *Oceanography*, vol. 6, no. 3, pp. 112–119, 1993.

[45] J. Kong *et al.*, "Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks," in *Proc. ACM Workshop Wireless Security (WiSe)*, Cologne, Germany, Sep. 2005, pp. 87–96.

[46] P. Patron and Y. Petillot, "The underwater environment: A challenge for planning," in *Proc. Workshop U.K. Plan. Scheduling Special Interest Group*, Edinburgh, U.K., Dec. 2008.

[47] R. Urich, *Principles of Underwater Sound*. New York, NY, USA: McGraw-Hill, 1983.

[48] Y. Z. Dong and P. X. Liu, "Security considerations of underwater acoustic networks," in *Proc. Int. Congr. Acoust. (ICA)*, Sydney, NSW, Australia, Aug. 2010.

[49] Y. Z. Dong and P. X. Liu, "Security analysis on underwater acoustic networks," in *Proc. MTS/IEEE OCEANS*, Yeosu, South Korea, May 2012, pp. 1–4.

[50] Y. Dong, H. Dong, and G. Zhang, "Study on denial of service against underwater acoustic networks," *J. Commun.*, vol. 9, no. 2, pp. 135–143, Feb. 2014.

[51] W. C. Wang, J. J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: A distributed approach," *Int. J. Security Netw.*, vol. 3, no. 1, pp. 10–23, Jan. 2008.

[52] D. N. Sandeep and V. Kumar, "Review on clustering, coverage and connectivity in underwater wireless sensor networks: A communication techniques perspective," *IEEE Access*, vol. 5, pp. 11176–11199, 2017.

[53] Y. Zhou, A. Song, and F. Tong, "Underwater acoustic channel characteristics and communication performance at 85 kHz," *J. Acoust. Soc. America*, vol. 142, no. 4, 2017, Art. no. EL350.

[54] L. Freitag *et al.*, "The WHOI micro-modem: An acoustic communications and navigation system for multiple platforms," in *Proc. MTS/IEEE OCEANS*, vol. 2. Washington, DC, USA, Sep. 2005, pp. 1086–1092.

[55] Y. P. Cong, G. Yang, Z. Q. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. Int. Conf. Commun. Mobile Comput. (CMC)*, vol. 1. Shenzhen, China, Apr. 2010, pp. 162–168.

[56] A. P. Das and S. M. Thampi, "Secure communication in mobile underwater wireless sensor networks," in *Proc. Int. Conf. Adv. Comput. Commun. Informat. (ICACCI)*, Kochi, India, Aug. 2015, pp. 2164–2173.

[57] M. M. Zuba, Z. J. Shi, Z. Peng, and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proc. ACM Int. Workshop Underwater Netw. (WUWNet)*, Seattle, WA, USA, Dec. 2011, p. 12.

[58] M. Zuba, Z. J. Shi, Z. Peng, J.-H. Cui, and S. L. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security Commun. Netw.*, vol. 8, no. 16, pp. 2635–2645, Nov. 2015.

[59] X. Peng, M. Kowalski, D. Mcculley, and M. Zuba, "An experimental study of jamming attacks in underwater acoustic communication," in *Proc. ACM Int. Conf. Underwater Netw. Syst. (WUWNet)*, Arlington, VA, USA, Oct. 2015, p. 12.

[60] Q. Wang, H.-N. Dai, X. R. Li, and H. Wang, "Eavesdropping attacks in underwater acoustic networks," in *Proc. Int. Conf. Inf. Comput. Security (ICICS)*, Singapore, Dec. 2015, pp. 1–5.

[61] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, "Jamming in underwater sensor networks: Detection and mitigation," *IET Commun.*, vol. 6, no. 14, pp. 2178–2188, Sep. 2012.

[62] H. Li, Y. H. He, X. Z. Cheng, H. S. Zhu, and L. M. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 56–62, Nov. 2015.

[63] T. Bian, R. Venkatesan, and C. Li, "Design and evaluation of a new localization scheme for underwater acoustic sensor networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBOCOM)*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 1–5.

[64] X. Z. Cheng, H. N. Shu, Q. L. Liang, and D. H.-C. Du, "Silent positioning in underwater acoustic sensor networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1756–1766, May 2008.

[65] S. S. Shahapur and R. Khanai, "Localization, routing and its security in UWSN—A survey," in *Proc. Int. Conf. Elect. Electron. Optim. Techn. (ICEEOT)*, Chennai, India, Oct. 2016, pp. 1001–1006.

[66] V. Chandrasekhar and W. Seah, "An area localization scheme for underwater sensor networks," in *Proc. MTS/IEEE OCEANS*, Singapore, May 2007, pp. 1–8.

[67] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," *Telecommun. Syst.*, vol. 22, nos. 1–4, pp. 267–280, 2003.

[68] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in *Proc. ACM Workshop Security Ad Hoc Sensor Netw. (SASN)*, Fairfax, VA, USA, Oct. 2003, pp. 21–32.

[69] F. Hu, Y. Malkawi, S. Kumar, and Y. Xiao, "Vertical and horizontal synchronization services with outlier detection in underwater acoustic networks," *Wireless Commun. Mobile Comput.*, vol. 8, no. 9, pp. 1165–1181, Nov. 2008.

[70] M. Zuba, M. Fagan, J.-H. Cui, and Z. J. Shi, "A vulnerability study of geographic routing in underwater acoustic networks," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, National Harbor, MD, USA, Oct. 2013, pp. 109–117.

[71] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in *Proc. IEEE Underwater Commun. Netw. Conf. (UComms)*, Lerici, Italy, Oct. 2016, pp. 1–5.

[72] X. Y. Lu, M. Zuba, J.-H. Cui, and Z. J. Shi, "Uncooperative localization improves attack performance in underwater acoustic networks," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 454–462.

[73] Y. Z. Dong and P. X. Liu, "Simulation study on self-reorganization of underwater acoustic networks," in *Proc. Int. Conf. Inf. Autom.*, Shenzhen, China, Jun. 2011, pp. 595–600.

[74] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Urbana, IL, USA, 2005, pp. 46–57.

[75] L. Xiao, Q. D. Li, T. H. Chen, E. Cheng, and H. Y. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Proc. IEEE Glob. Commun. Conf. (GLOBOCOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[76] Y. Li, L. Xiao, Q. D. Li, and W. Su, "Spoofing detection games in underwater sensor networks," in *Proc. MTS/IEEE OCEANS*, Washington, DC, USA, Oct. 2015, pp. 1–5.

[77] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[78] M. R. Ahmed, S. M. Tahsien, M. Aseeri, and M. S. Kaiser, "Malicious attack detection in underwater wireless sensor network," in *Proc. IEEE Int. Conf. Telecommun. Photon. (ICTP)*, Dhaka, Bangladesh, Dec. 2015, pp. 1–5.

[79] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Print Kernel-based Learning Methods*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[80] S. S. Keerthi and C.-J. Lin, "Asymptotic behaviors of support vector machines with Gaussian kernel," *Neural Comput.*, vol. 15, no. 7, pp. 1667–1689, Jul. 2003.

[81] G. C. Calafiore and L. E. Ghaoui, *Optimization Models*. Cambridge, U.K.: Cambridge Univ. Press, 2014.

[82] M. R. Ahmed, M. Aseeris, M. S. Kaisert, N. Z. Zenia, and Z. I. Chowdhury, "A novel algorithm for malicious attack detection in UWSN," in *Proc. Int. Conf. Elect. Eng. Inf. Commun. Tech. (ICEEICT)*, Dhaka, Bangladesh, May 2015, pp. 1–6.

[83] K. Sentz and S. Ferson, "Combination of evidence in Dempster–Shafer theory," Sandia Nat. Lab., Livermore, CA, USA, Rep. SAND 2002-0835, Apr. 2002.

[84] R. Zhang and Y. C. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[85] X. Li, G. J. Han, A. H. Qian, L. Shu, and J. Rodrigues, "Detecting Sybil attack based on state information in underwater wireless sensor networks," in *Proc. IEEE Int Conf. Softw. Telecommun. Comput. Netw. (SoftCOM)*, Primošten, Croatia, Sep. 2013, pp. 1–5.

[86] R. Urick, *Principles of Underwater Sound*. New York, NY, USA: McGraw-Hill, 1991.

[87] M. Xu, G. Z. Liu, D. Q. Zhu, and H. F. Wu, "A cluster-based secure synchronization protocol for underwater wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2014, no. 1, pp. 1–13, Apr. 2014.

[88] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 518–533, Sep. 2010.

[89] T. C. Yang and W.-B. Yang, "Low probability of detection underwater acoustic communications for mobile platforms," in *Proc. MTS/IEEE OCEANS*, Quebec City, QC, Canada, Sep. 2008, pp. 1–6.

[90] M. Li *et al.*, "Cognitive code-division links with blind primary-system identification," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3743–3753, Nov. 2011.

[91] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," in *Proc. ACM SIGCOMM*, Kyoto, Japan, Aug. 2007, pp. 397–408.

[92] C. F. Wang and Z. H. Wang, "Signal alignment for secure underwater coordinated multipoint transmissions," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6360–6374, Dec. 2016.

[93] A. Katariya, A. Arya, and K. Minda, "Coded under water acoustic communication (UWA) with cryptography," in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, Bhopal, India, Nov. 2010, pp. 493–497.

[94] H. Peyvandi and S. J. Park, "Security in data communication and privacy in conversations for underwater wireless networks using scrambled speech scheme," in *Proc. MTS/IEEE OCEANS*, Waikoloa, HI, USA, Sep. 2011, pp. 1–3.

[95] M. Xu, G. Z. Liu, and J. H. Guan, "Towards a secure medium access control protocol for cluster-based underwater wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2015, no. 1, Apr. 2015, pp. 1–11.

[96] M. Ibragimov *et al.*, "CCM-UW security modes for low-band underwater acoustic sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 479–499, May 2016.

[97] Y. Z. Dong and P. X. Liu, "A comparison of two secure routing protocols in underwater acoustic network," in *Proc. Int. Congr. Acoust. (ICA)*, Sydney, NSW, Australia, Aug. 2010.

[98] H. Rustad, "A lightweight protocol suite for underwater communication," in *Proc. Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Bradford, U.K., May 2009, pp. 1172–1177.

[99] G. Dini and A. L. Duca, "SeFLOOD: A secure network discovery protocol for underwater acoustic networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Kerkyra, Greece, Jun./Jul. 2011, pp. 636–638.

[100] E. Barker, D. Johnson, and M. Smid, *Recommendation for Pairwise Key Establishment Schemes Using Discrete Logarithm Cryptography*, document NIST Special Publication 800-56A, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Mar. 2006.

[101] C. Blundo *et al.*, "Perfectly-secure key distribution for dynamic conferences," in *Proc. Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1993, pp. 471–486.

[102] M. M. Zuba, M. Fagan, Z. J. Shi, and J.-H. Cui, "A resilient pressure routing scheme for underwater acoustic networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBOCOM)*, Austin, TX, USA, Dec. 2014, pp. 637–642.

[103] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: A channel-aware routing protocol for underwater acoustic wireless networks," *Ad Hoc Netw.*, vol. 34, pp. 92–104, Nov. 2015.

[104] A. Capossele, G. D. Cicco, and C. Petrioli, "R-CARP: A reputation based channel aware routing protocol for underwater acoustic sensor networks," in *Proc. ACM Int. Conf. Underwater Netw. Syst. (WUWNet)*, Arlington, VA, USA, Oct. 2015, Art. no. 37.

[105] S. Heron, "Advanced encryption standard (AES)," *Netw. Security*, vol. 2009, no. 12, pp. 8–12, Dec. 2009.

[106] M. Brown *et al.*, "PGP in constrained wireless devices," in *Proc. USENIX Security Symp. (SSYM)*, Denver, CO, USA, Aug. 2000, p. 19.

[107] D. W. Carman, P. S. Krus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs, Netw. Assoc. Inc., Santa Clara, CA, USA, Rep. 00-010, 2000.

[108] C. Yuan, W. P. Chen, Y. Q. Zhu, D. Y. Li, and J. Tan, "A low computational complexity authentication scheme in underwater wireless sensor network," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Netw. (MSN)*, Shenzhen, China, Dec. 2015, pp. 116–123.

[109] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[110] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the development of secure underwater acoustic networks," *IEEE J. Ocean. Eng.*, vol. 42, no. 4, pp. 1075–1087, Oct. 2017.

[111] M. Guillaud, D. T. Slock, and R. Knopp, "A practical method for wireless channel reciprocity exploitation through relative calibration," in *Proc. Int. Symp. Signal Process. Appl.*, Sydney, NSW, Australia, Aug. 2005, pp. 403–406.

[112] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Oct./Nov. 2007, pp. 401–410.

[113] Y. C. Liu, J. W. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *Proc. Int. Conf. Signal Process. (ICSP)*, Beijing, China, May 2008, pp. 1838–1841.

[114] Y. Huang, S. L. Zhou, Z. J. Shi, and L. F. Lai, "Experimental study of secret key generation in underwater acoustic channels," in *Proc. Asilomar Conf. Signal Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2014, pp. 323–327.

[115] L. F. Lai, Y. B. Liang, and W. L. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[116] D. Galindo, R. Roman, and J. Lopez, "A killer application for pairings: Authenticated key establishment in underwater wireless sensor networks," in *Proc. Int. Conf. Cryptol. Netw. Security (CANS)*, Hong Kong, Dec. 2008, pp. 120–132.

[117] C.-G. Liu, C.-H. Chao, C.-W. Leou, and J.-S. Li, "Iterative key distribution based on MAD neighborhood in underwater mobile sensor networks," *Comput. J.*, vol. 55, no. 12, pp. 1467–1485, Dec. 2012.

[118] J. M. Jornet, M. Stojanovic, and M. Zorzi, "Focused beam routing protocol for underwater acoustic networks," in *Proc. ACM Int. Workshop Underwater Netw. (WUWNet)*, San Francisco, CA, USA, Sep. 2008, pp. 75–82.

[119] J. M. Jornet, M. Stojanovic, and M. Zorzi, "On joint frequency and power allocation in a cross-layer protocol for underwater acoustic networks," *IEEE J. Ocean. Eng.*, vol. 35, no. 4, pp. 936–947, Oct. 2010.

[120] D. Pompili and I. F. Akyildiz, "Overview of networking protocols for underwater wireless communications," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 97–102, Jan. 2009.

[121] D. Pompili, T. Melodia, and I. F. Akyildiz, "A CDMA-based medium access control for underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1899–1909, Apr. 2009.

[122] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security framework for underwater acoustic sensor networks," in *Proc. MTS/IEEE OCEANS*, Genoa, Italy, May 2015, pp. 1–9.

[123] J. López and R. Dahab, "An overview of elliptic curve cryptography," Inst. Comput., State Univ. Campina, Campinas, Brazil, Rep. IC-00-10, 2000.

[124] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Inf. Comput.*, vol. 3, no. 4, pp. 317–344, 2003.

[125] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 553–558, May 1990.

[126] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, Dec. 2010.

[127] J. Großschädl, A. Szekely, and S. Tillich, "The energy cost of cryptographic key establishment in wireless sensor networks," in *Proc. ACM Symp. Inf. Comput. Commun. Security (ASIACCS)*, Singapore, 2007, pp. 380–382.

[128] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1984, pp. 47–53.

[129] F. Zhang, R. Safavinaini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Proc. Int. Workshop Pract. Theory Public Key Cryptography (PKC)*, Singapore, Mar. 2004, pp. 277–290.

[130] B. Dan, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, Gold Coast, QLD, Australia, Dec. 2001, pp. 514–532.

[131] E. Souza *et al.*, "End-to-end authentication in under-water sensor networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Split, Croatia, Jul. 2013, pp. 299–304.

[132] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," in *Proc. Annu. ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, Rome, Italy, Jul. 2001, pp. 521–534.

[133] G. J. Han, J. F. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015.

[134] J. F. Jiang, G. J. Han, L. Shu, S. Chan, and K. Wang, "A trust model based on cloud theory in underwater acoustic sensor networks," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 342–350, Feb. 2017.

[135] J. F. Jiang, G. J. Han, C. S. Zhu, S. Chan, and J. J. P. C. Rodrigues, "A trust cloud model for underwater wireless sensor networks," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 110–116, Mar. 2017.

[136] D. Y. Li, H. J. Meng, and X. M. Shi, "Membership clouds and membership cloud generators," *J. Comp. Res. Develop.*, vol. 32, no. 6, pp. 15–20, 1995.

[137] G. Dini and A. L. Duca, "A cryptographic suite for underwater cooperative applications," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun./Jul. 2011, pp. 870–875.

[138] A. Caiti, V. Calabro, G. Dini, A. L. Duca, and A. Munafo, "Secure cooperation of autonomous mobile sensors using an underwater acoustic network," *Sensors*, vol. 12, no. 2, pp. 1967–1989, Feb. 2012.

[139] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. New York, NY, USA: Wiley, 1995.

[140] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. Int. Conf. Embedded Netw. Sensor Syst.*, Baltimore, MD, USA, Nov. 2004, pp. 162–175.

[141] G. Dini and I. M. Savino, "S2RP: A secure and scalable rekeying protocol for wireless sensor networks," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Vancouver, BC, Canada, Oct. 2006, pp. 457–466.

[142] M. R. Islam, S. Azad, and M. M. Morshed, "A secure communication suite for cluster-based underwater surveillance networks," in *Proc. Int. Conf. Elect. Eng. Inf. Commun. Tech. (lCEEICT)*, Dhaka, Bangladesh, Apr. 2014, pp. 1–5.

[143] M. J. Dworkin, "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," NIST, Gaithersburg, MD, USA, Rep. SP 800-38D, 2007.

[144] G. Khan, K. K. Gala, and R. Rathore, "Robust data aggregation, encryption and data transfer in UWSNs," in *Proc. Int. Conf. Next Gener. Comput. Technol. (NGCT)*, Dehradun, India, Sep. 2015, pp. 403–407.

[145] N. T. Courtois, M. Daum, and P. Felke, "On the security of HFE, HFEv- and quartz," in *Proc. Int. Workshop Theory Pract. Public Key Cryptography (PKC)*, Miami, FL, USA, Jan. 2003, pp. 337–350.

[146] G. Toso, D. Munaretto, M. Conti, and M. Zorzi, "Attack resilient underwater networks through software defined networking," in *Proc. ACM Int. Conf. Underwater Netw. Syst. (WUWNet)*, Rome, Italy, Nov. 2014, Art. no. 44.

[147] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 681–694, Apr. 2014.

[148] J. Kim, K.-Y. Jang, H. Choo, and W. Kim, "Energy efficient LEACH with TCP for wireless sensor networks," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, Kuala Lumpur, Malaysia, Aug. 2007, pp. 275–285.

[149] S. Wöhrl and B. C. Schmitt, "TLS solutions for wireless sensor networks," in *Proc. Seminar Future Internet Netw. Archit. Services*, Aug. 2012, pp. 31–38, doi: 10.2313/NET-2012-08-1_06.

Shengming Jiang (A'96–M'00–SM'07) received the bachelor's degree in computer science from Shanghai Maritime Institute, China, in 1988, the master's degree in computer science from the University of Paris VI, France, in 1992, and the Doctoral degree in computer science from the University of Versailles Saint-Quentin-En-Yvelines, France, in 1995. He is a Professor and the Dean of the College of Information Engineering, Shanghai Maritime University. From 1988 to 1990, he was an Assistant Engineer with Nanjing Petrol Transportation Company, China. He was a Research Associate with the Department of Electrical and Electronic Engineering and the Computer Science Department, Hong Kong University of Science and Technology, from 1995 to 1997. He was a Technical Staff Member with the Centre for Wireless Communications, National University of Singapore, from 1997 to 2000, and a Senior Member of Technical Staff as well as the Acting Leader of the Network Strategic Group from 2001 to 2003. He was an Associate Lead Scientist and the Leader of the End-to-End QoS Laboratory with the Institute for Infocomm Research, Singapore, from 2003 to 2004. He was a Principal Lecturer with the Faculty of Advanced Technology, University of Glamorgan (currently, the University of South Wales), U.K., from 2007 to 2009. He was a Professor with the School of Electronic and Information Engineering, South China University of Technology from 2004 to 2013.

His research interest includes networking issues in both wired and wireless networks as well as mobile computing with over 25 years of international research and development experiences in France, Hong Kong, Singapore, U.K., and China, respectively. He is currently leading in the research of marine Internet. He has published two monographs (Springer) and over 160 papers on related areas, some of which were published in prestigious international journals and conferences such as the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGIES, and *ACM SIGCOMM Computer Communication Review* as well as IEEE INFOCOM.