arXiv:2209.01952v1 [cs.CR] 5 Sep 2022

Authentication of Underwater Assets

Bálint Z. Téglásy[1*], Emil Wengle[2], John R. Potter[2,3]
and Sokratis Katsikas[4]

[1*]Department of Engineering Cybernetics, NTNU, O. S.
Bragstads Plass 2D, Trondheim, 7034, Norway.
[2]Department of Electronic Systems, NTNU, O. S. Bragstads
Plass, Trondheim, 7034, Norway.
[3]Centre for Geophysical Forecasting, NTNU, O. S. Bragstads
Plass, Trondheim, 7034, Norway.
[4]Department of Information Security and Communication
Technology, NTNU, Teknologivegen 22, Gjøvik, 2815, Norway.

*Corresponding author(s). E-mail(s): balint.teglasy@ntnu.no;
Contributing authors: emil.wengle@ntnu.no;
john.r.potter@ntnu.no; sokratis.katsikas@ntnu.no;

Abstract

Secure digital wireless communication underwater has become a key issue as maritime operations shift towards employing a heterogeneous mix of robotic assets and as the security of digital systems becomes challenged across all domains. At the same time, a proliferation of underwater signal coding and physical layer options are delivering greater bandwidth and flexibility, but mostly without the standards necessary for interoperability. We address here an essential requirement for security, namely a confirmation of asset identities also known as authentication. We propose, implement, verify and validate an authentication protocol based on the first digital underwater communications standard. Our scheme is applicable primarily to AUVs operating around offshore oil and gas facilities, but also to other underwater devices that may in the future have acoustic modems. It makes communication including command and control significantly more secure, and provides a foundation for the development of more sophisticated security mechanisms.

Keywords: Authentication; Acoustic; Underwater; JANUS; Security

1 Introduction

Underwater (UW) environments are increasingly explored and developed for economic benefit, environmental stewardship and research interests. While workhorse-class Remotely-Operated Vehicles (ROV) will continue to play an important role in UW operations, due to requirements for substantial power and/or live video feed, their tethers can weigh several times the ROV itself, dramatically increasing power consumption to move them through the water, reducing maneuverability and creating entanglement and snagging issues [1]. The proliferation of affordable light and agile Autonomous UW Vehicles (AUV) enabled by dramatic improvements in battery technology, cheap and ample processing and memory, developments in control theory and Artificial Intelligence (AI), etc., is empowering a disruptive technology change that is sweeping the field.

Wireless UW Communications and Networking (WUCaN) is essential to support this new wave of autonomous systems. However, WUCaN is currently severely constrained compared to wireless communications in air, not only because of the formidable physical limitations, but also because few standards exist to support inter-operability. Currently the only open standard for UW wireless digital communications, a precursor to a fully-fledged WUCaN capability, is JANUS [2]. Currently, WUCaN, if available at all, is generally conducted via unencrypted bitstreams without an authentication mechanism. In this paper we address and resolve this key shortfall.

We are essentially striving to create an Internet of Underwater Things (IoUT), by which we mean a Wide Area Network (WAN) of inter-operable UW devices. Just as the above-water Internet of Things (IoT) is based on radio links, we would also like a wireless solution. We look for potential authentication methods with an approach that, in principle, is agnostic to the physical layer, including radio frequency electromagnetic, free space optical and acoustic. Radio solutions are generally of very short range $(O(10^0)\text{m})$ but have the benefit of potentially bridging the air-sea interface [3]. Free-space optical solutions have a larger, but still very limited, range of $O(10^1)\text{m}$. Both offer superior bandwidth compared to an acoustic physical layer, at the cost of very limited range. Only the acoustic physical layer has an accepted digital standard. Ultimately, we expect WUCaN systems to be intelligent, adaptive and physical-layer agnostic, but at this initial stage we begin with the most common physical layer, namely acoustics. We explore a baseline solution for civilian authentication requirements, develop a feasible method, and propose an attractive candidate for underwater assets using the JANUS protocol. It is intended primarily for use with AUVs, operating around offshore oil and gas facilities, to improve safety and productivity [4]. The lack of authentication has always been a a primary concern in maritime communications, allowing countless false flag operations throughout history [5]. As far as AUVs are concerned, it is easily imaginable that assets would be captured by adversaries due to the lack of secure communications [6], be it by knowing the location or even sending illegitimate command signals.

The remaining of the paper is structured as follows: In Section 2 we briefly review related work. In Section 3 we specify the requirements that an authentication method for the IoUT should satisfy. In Section 4 we present and discuss our proposal, including how it was implemented, verified, and validated. Finally, Section 6 summarizes our conclusions and outlines directions for future research.

2 Related work

Underlying physical layer technologies are advancing fast and international standardisation efforts are gaining traction, e.g. [7], which represents a bottom-up effort to achieve inter-operability driven by user necessity. WUCaN security threats are discussed by Yang et al. in [8] while Peng et al. [9] offer an encryption algorithm for UW use that is more energy efficient than previous solutions, although the block size of 64 bits poses questions of applicability in a standardised environment. Du et al. [10] present a secure routing scheme for WUCaN, but the encryption method enabling their scheme is not defined in detail and it is not built on an existing physical protocol layer. Dini et al. propose a secure network discovery protocol for WUCaN in [11], where they primarily consider networks established between AUVs. The encryption method, the details of the physical protocol layer and the packet size (specific clear-text length) are not, however, developed. Petroccia et al. [12] report network discovery and encryption with AES in Galois counter mode in the framework of their Cognitive Communications Architecture [13]. This is a promising approach for interoperability as well, since JANUS is one of the physical layer protocols that the architecture is claimed to use. However, an authentication solution has not been described yet. In [14] and [15], communication security for underwater acoustic networks (UWANs) is addressed based on physical security, rather than point-to-point or sequential deterministic authentication. They note that UWAN packets are rarely encrypted, leaving the UWAN exposed to external attacks faking legitimate messages. This is essentially the problem we seek to address with cybersecurity methods. They propose a new algorithm for message authentication by observing that, due to the strong spatial dependency of the underwater acoustic channel, an attacker can attempt to mimic the channel associated with the legitimate transmitter only for a small set of receivers, typically just for a single one. Their scheme relies on trusted nodes that independently help a sink node in the authentication process. For this to happen, we have to start with a set of trusted nodes. Then, for each incoming packet, the sink fuses beliefs evaluated by the trusted nodes to reach an authentication decision. These beliefs are based on estimated statistical channel parameters, chosen to be the most sensitive to the transmitter-receiver displacement. They have simulation results and at-sea experiments demonstrating the effectiveness of their approach. However, their approach relies on spatial dependencies and therefore on physical security; an attacker with an acoustic modem planted on or in the immediate vicinity of a trusted node is not defended against. Here, our

method not relying on physical, but logical security in the form of a pre-shared secret provides a solution. An encrypted communication solution for JANUS, including packet formats for cargo length specification, has been suggested in [16]. The encryption method is intentionally left to the technology supplier or modem manufacturer using the JANUS standard, and the reception of more than a baseline packet is required to enable successful decryption. This solution, while promising, relies on a larger packet not being corrupted and an extension to the baseline JANUS standard. [17] assumes access to a hybrid system with radio communication, a public key system and AES encryption with a block size of 128 bits in the acoustic domain. With a slightly larger coverage of digital signature schemes, [18] also assumes the presence of a network of base stations as an infrastructural pre-condition without getting into detail on how those base stations would be moored, powered or communicated with on a global scale. While public key systems undoubtedly have advantages for securing global systems for communication where the participating devices have no pre-shared keys, these rely on a likewise global public key infrastructure (PKI) to uphold the security properties promised by them. The communication requirements of a PKI would mean that ad hoc networking is not necessarily secure if the authorities in the infrastructure are not available e.g. through acoustic/radio gateways.

In Venilia [19] we see many of the same constraints being applied as in our proposal. A symmetric encryption scheme with an even smaller block size is used and epochs based on onboard time are harnessed to generate subkeys through a scheduler. However, there is no authentication protocol or other mechanism to ensure key renewal, such that the security property of forward secrecy [20] is neglected. This is not acceptable in an environment where the scalability of mission duration or of the number of devices is needed. While the loss of confidential information such as keys is always unfortunate, it is catastrophic in the case of systems that only allow the use of a single key for all participants at all times. Venilia includes the routing data in the ciphertext as a sign that only one key can be used in one operations theatre. The risk of compromised keys through physical tampering of individual devices or any other cyber attack surface puts the whole fleet at risk, especially if the remaining payload of 8 bits is used for command and control as proposed. Nevertheless, we see the utility of Venilia in cases where many messages have to be sent back and forth including demands for checkbacks issued randomly, as would be the case for devices at lower levels of autonomy that need constant piloting. In these very limited cases, we concur that the non-determinism of Venilia guaranteed by initialisation vectors (IV) and epochs offers superior security.

To the best of our knowledge, no standardisable solutions for simple WUCaN authentication have been proposed in the literature. Accordingly, the purpose and contribution of this paper is to develop an attractive authentication method. To sum up, our proposed security barrier provides the flexibility to work as a local solution like Venilia, but also has key elements required for a more flexible and scalable solution without requiring infrastructure that would be unreasonable to assume.

3 Requirements specification

3.1 Choice of the Physical Layer

Examples of the approximate bandwidth and range limitations of physical layer technologies are provided in Table 1. We are developing a system that is aware that there are different physical layers of interest, and provides defense in depth by authenticating with additional factors and bands as decreasing range allows.

3.1.1 Electromagnetic

Even though communication in the electromagnetic domain is severely restricted underwater, the possibility to use protocols such as the familiar 802.11b,g provides a tempting interface with enterprise systems, including the established authentication protocols on those systems (e.g. based on Kerberos [21], TACACS [22] or RADIUS [23]). This physical layer also offers a bridge to connect IoT with IoUT, a major issue in its own right.

3.1.2 Free space optical

Laser diodes with a 520 nm wavelength, modulated with Non-Return-to-Zero On-Off Keying (NRZ-OOK), have achieved a data rate of 500 Mbps with a bit error rate of 2.5 x 10^{-3} through clean freshwater in a laboratory [24]. A blue laser (450 nm wavelength) optical modem is now commercially available that claims a robust data rate of 1 Mbps up to 15 m range in practical seawater applications with Ethernet compatibility.

Table 1 Physical Layers for Underwater Communication

Modality	Reference	Bandwidth	Range
Electromagnetic	2,4 GHz WiFi [25]	11 Mbps	15 cm[a]
Free space optical	NRZ-OOK 520 nm [24]	500 Mbps	100 m
Acoustic	JANUS standard [2]	80 bps	10 km

[a][25] indicates that packet loss rises steeply above 15 cm.

3.1.3 Acoustic

Useful UW acoustic communication frequencies span from $O(10^0)$-$O(10^6)$Hz, depending on the desired range and bandwidth considerations, but typically a modem in the 20-30 kHz range might offer $O(10^0)$ kbps over a range of ≈ 5 km. There are many different physical layer protocols for digital acoustic communication, but they are all proprietary and therefore not interoperable, and also the extent to which academic inquiry is possible is limited. Furthermore, in cases where robustness is required, e.g. in noisy environments, the previously mentioned JANUS standard is as of 2021 still the fallback technology

[26]. JANUS was developed as a deliberately simple and robust physical layer protocol suited for initial contact, that could be used as a beacon, for discovery and for negotiation of mutually-available higher-performance communication modes, a function demonstrated in [27]. As such, for lightweight authentication, the JANUS standard, with an 80 bps data rate (using the 11.520 kHz centre frequency specified for the first defined JANUS band), is very suitable. A complete communications system based on the JANUS physical and MAC layer protocols can be phrased in Open Systems Interconnect (OSI) terms as shown Table 2. Whilst JANUS as a physical layer is comparatively simple, it does implement frequency-hopped binary shift keying to provide robustness in the face of multiple signal arrival paths.

Table 2 JANUS implemented in the OSI stack framework

ISO OSI number	Protocol layer	Digital acoustic equivalent
7	Application	
6	Presentation	Implementation in
5	Session	non-standardised applications
4	Transport	(e.g. WetsApp)
3	Network	
2	Data link	partially covered by JANUS[a]
1	Physical	JANUS core specification

[a]JANUS includes the Medium Access Control (MAC) sublayer.

When exploring the service support to be expected from the standard protocol stack, we begin by looking at the data link layer. JANUS includes a Cyclic Redundancy Check (CRC), but other functions of the data link layer such as flow control, acknowledgment, and error notification are absent. This means that all communications are unacknowledged and formally connectionless [28]. The JANUS protocol also includes cross-layer features that may compromise strict adherence to the OSI layer architecture. As of writing, most of the OSI layers are implemented by non-standard user-defined applications. Although non-specified protocol layers facilitate the development of proprietary applications in a geographically and organisationally-segmented WUCaN market, they ultimately limit the inter-operability of networked and secured communication functions, unless they are co-ordinated with major stakeholders and become extensions of the standard. The absent protocol layers also mean that it is not possible to determine which packets arrived and were successfully decoded using only the baseline JANUS protocol. These challenges can be addressed by developing additional protocol elements, but for these to be useful, they must be simple and align with the JANUS philosophy of inclusivity, so that they are attractive to becoming intuitively adopted by the community. We account for this by designing the simplest possible protocol in this first iteration. This means using symmetric cryptography, as the distribution of public keys would impose an additional communication overhead and a public

key infrastructure. It also implies using server-less protocols, because means of communication through centralized nodes and segmented networks are not likely to be available. To navigate the protocol stack and to have our packets be interpreted as part of the proposed protocol, Class IDs would need to be assigned.

Table 3 JANUS Bit Allocation in the Baseline Packet

Bits	Descriptor	Comments
1-4	Version	JANUS defined: unsigned 4 bit integer. Current version is 3.
5	Mobility flag	JANUS defined: Indicates nature of the transmitting platform.
6	Schedule flag	JANUS defined: If On (1), the first bit in the Application Data Block (ADB) indicates a cargo length. For our method, it is off.
7	Tx/Rx Flag	JANUS defined, Transmit/Receive capability: for our purposes, it needs to decode on both devices (1).
8	Forward capability	JANUS defined: Used for routing and Delay Tolerant Networking. For us,it should be 0=no.
9-16	Class User ID	JANUS defined: Allows 256 classes of users, mostly individual nations.
17-22	Application Type	Allows 64 different types of message per class user i.d. to be specified.
23-56	ADB	34 bits of payload. Our proposal: 29 bit timestamp, 3 bit clock accuracy descriptor, 2 cleartext flags.
57-64	8-bit Check-sum	JANUS defined: 8-bit CRC run on the previous 56 bits with $p(x) = x^8 + x^2 + x^1 + 1, init = 0$

3.2 Choice of an appropriate encryption algorithm for authentication

Symmetric encryption methods are feasible if a copy of the cryptographic key can be shared, e.g. via WiFi, together with the synchronisation of clocks at some convenient opportunity when the assets are proximate in air, perhaps while batteries are being recharged or the systems are being otherwise prepared for deployment. Protocols based on a multi-step challenge-response and/or handshake are avoided, since short and variable channel coherence and asymmetric links are characteristic of the UW acoustic channel and an overly-demanding exchange could lead to very long or failed authentication processes. Therefore we develop our solution using only the JANUS baseline packet, whose bit allocation is shown in Table 3. This packet is 64 bits long, precluding the use of the Advanced Encryption Standard (AES) where the cipher block size is 128 bits. This is a typical problem in WUCaN, where data rates are typically $O(10^{-5})$ of those enjoyed in the GHz radio world, so that overheads of all types must be drastically reduced. The predecessor of AES, the Data Encryption Standard (DES), has a block size of 64 bits, and is still secure in the adapted version with enlarged key size called Triple DES [29]. However, encrypting the full 64 bit packet would result in a lack of standard-ised bit allocation as formulated by JANUS. A major concern is accidental

integrity loss in transmission; therefore the CRC must remain unencrypted. If we only want to encrypt the user-defined 34 bits in a JANUS packet ADB, the range of encryption methods available is reduced further. To fit the ADB, ciphers having a block size of at most 32 bits are considered. Informed by the list used in [30], we conclude candidate ultra-lightweight ciphers as: RC5 [31], Speck [32], Katan32 [33], Hummingbird-2 [34] and Skipjack32. We include the TUBCipher [35] designed specifically for Venilia for comparison. The characteristics of these algorithms are shown in Table 4. We want to maximise security within the constraints. Since the envisioned key exchange algorithm does not limit the key size, we prioritise those ciphers, within the block size bounds, with a large key (at least 128 bits). These are Hummingbird-2 and RC5. The Hummingbird-2 cipher has been developed with micro-controllers in mind. The simple RC5 code suggests that it might work better in software. Furthermore, the RC5 cipher requires no IV, whereas the Hummingbird-2 is like a stream cipher in this sense since it does. The communication requirements of synchronising an IV would put an additional burden on the complexity and reliability of the acoustic communication. Even if pre-shared, the IV would need to be updated synchronously on A and B. That is not feasible due to the high packet loss. Consequently we select the RC5 cipher.

4 The proposed protocol

4.1 Identification of Friend or Foe

In the following we propose a mutual authentication solution, capable of identifying AUVs with pre-shared, long-term key K_1. The following steps are required, grouped :

1. Device A sends a 64-bit baseline JANUS packet with a 29-bit timestamp T_A, a 3-bit clock accuracy descriptor CD_A in the ciphertext and two 1-bit flags in the unencrypted payload, with the packet header and CRC. The year is assumed known, and the specifying the day as mod(Julian day,6) allows 29 bits to encode milliseconds. The three bits describing the on-board clock accuracy span the $O(10^{-4})$ to $O(10^{-12})$ drift rates. Some functionality, such as current and speed estimation, hinges upon the availability of high accuracy, low drift synchronization of the clocks on devices A and B, such as it is achievable with chip scale atomic clocks [36], while also allowing for more widespread quartz technologies. The remaining two bits should be used to specify: (i) If an answer is expected as a next step in the authentication protocol (SYN), (ii) if the packet being sent is sent as a response to acknowledge an earlier packet (ACK). These remaining two bits also give an indication of which key should be used as per Table 7.

2. Device B receives and decodes the packet. If the received timestamp is within bounds and not used in the current key lifetime, then B responds by sending its own timestamp and clock accuracy descriptor T_B, CD_B encrypted with a pre-shared key K_1 chosen according to the JANUS-defined cleartext

Table 4 Encryption algorithms with block sizes $\leq$ 34 bits

Cipher	RC5	Skipjack	Speck	Katan32	Hummingbird-2	TUBCipher
Cryptanalysis available?	Yes (64 bit[a])	Yes (64 bit[a])	Yes	Yes	Yes	No
Minimum block size [bits]	32	32	32	32	16	27
Maximum key size [bits]	2040	80	64 (32 bit[a])	80	128	256
Needs IV?	No	No	No	No	Yes	Yes
Software optimised	Yes	No	Yes	No	No	N/A

[a]The ciphers marked with these properties have been formulated with different block sizes, but not all block size variants have been subject to peer-reviewed cryptanalysis or have the same key size. Therefore, the variant with the given block size has been evaluated.

header (bits 1-22 in Table 3) identifying a set including Device A. An application type of the class ID in the JANUS cleartext header also needs to indicate that the message is to be understood as one within our authentication framework. The packet including the returned clock signal of B should have its ACK bit set to 1.

3. If device A successfully receives and decodes the returned packet it can estimate the time of flight of the first outgoing packet by the difference T_B-T_A and the reciprocal time of flight for the second packet by the difference T_{A2}-T_B where T_{A2} is its own timestamp at the point of decoding the received response, adjusted by its own (known) decoding and decryption time delay. Given reasonable assumptions about the asymmetry in flight time due to currents (much smaller than the speed of sound in water) and possible mutual clock drift since the devices were synchronised during the key exchange, device A can determine if the received time stamp T_B is within expected margins and also estimate the inter-AUV distance based on a simple calculation using the speed of sound [37]. This third step is optional, since the time window for response validity is already given by the time-of-flight at maximum assumed range and the inputs to the session key calculation (below) are already established in steps 1 and 2. However, since distance is the primary determinant of physical security and safety, the principal enabler of better communications than the initially assumed JANUS [38], and there is no appreciable overhead associated with this additional step, we strongly recommend it is performed.

The proposed method is illustrated in Figure 1, where an AUV and a subsea valve assembly typical for oil and gas production are depicted as communication partners.
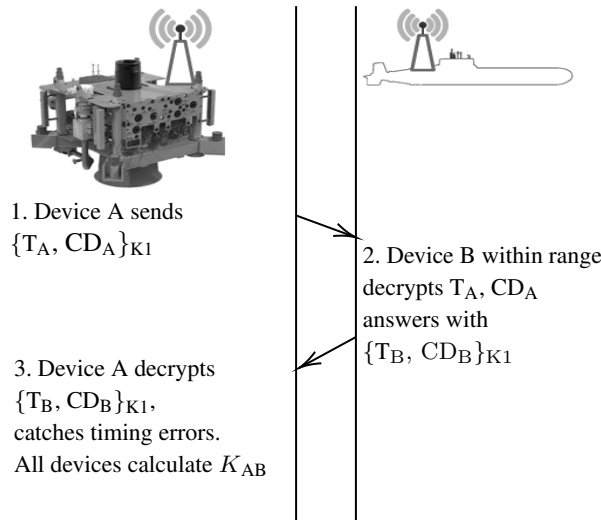

1. Device A sends
$\{T_A, CD_A\}_{K1}$

2. Device B within range
decrypts T_A, CD_A
answers with
$\{T_B, CD_B\}_{K1}$

3. Device A decrypts
$\{T_B, CD_B\}_{K1}$,
catches timing errors.
All devices calculate K_{AB}

Fig. 1 An illustration of the authentication challenge $\{T_A, CD_A\}_{K_1}$ and the response $\{T_B, CD_B\}_{K_1}$.

4.2 Calculating a Session Key

As we have not yet negotiated a shared secret that can be used as a session key in following communications, our method so far might not qualify as full feature authentication. Instead, the main functionality provided up to this point is the positive identification of friends.

If the derivation of a common secret is desired, both of the devices can calculate that now based on the timestamp they received from the other device and the one they have transmitted last. Note that other devices C, D, etc. within the reception zone and in possession of the long-term key, therefore declared friendly in our security model, will also be able to derive the session key. Due to the uncertainty resulting from high packet loss rates, device A is in a better position to start using the session key as it has in step 3 received an ACK-flagged confirmation that its timestamp and clock descriptor T_A, CD_A are available to some friendly device B in possession of the long-term key K_1. The common secret would be the pair of securely exchanged payloads $MMSI_A, T_A, CD_A$ and $MMSI_B, T_B, CD_B$. The fresh session key only available to friendly devices is $K_{AB} = f(T_A, CD_A, T_B, CD_B, K_1)$, where f is a combining function that doesn't allow finding $f(., ., K)$ without knowledge of the long-term, pre-shared key K_1 [39]. For f, we propose:

- concatenating $MMSI_A, T_A, CD_A$ and $MMSI_B, T_B, CD_B$,
- bit padding the resulting 124 bits to 512 bits by appending one bit as 1 and 387 bits as zeroes (1000...0),
- Apply the 128-bit block size version of the RC5 cipher in CBC (Cipher Block Chaining) mode with starting variable fixed to 0, as defined in ISO/IEC 10116
- truncating the resulting ciphertext to the first 256 bits

By doing so, we have established forward secrecy: the communications under K_{AB} will remain secure even when the long-term key K_n is compromised, provided that T_A, CD_A and T_B, CD_B are not simultaneously compromised. Note that this third step to establish a session key could be used also when T_A, CD_A and T_B, CD_B have been exchanged in cleartext: this just removes the dependency on K_1 along with the trust that it brings, but this might be necessary if no K_1 is available and instead physical layer security is deemed to be sufficient.

Device A could send T_{A2} as a confirmation under K_{AB} to device B. In the event that B has the less accurate clock, this provides an unambiguous estimate of the differential clock offset and water current velocity projected onto the vector joining the two devices. Additional functionality to synchronize clocks and/or estimate current and/or vehicle speeds can be based upon the exchanged clock accuracies. If one of the authenticated devices has a better clock accuracy than the other, the one with the less accurate clock should synchronize its own by taking the time stamp of the other device as its own (after adding half of the round-trip time). If this is done correctly, the chance of future successful authentications among the same devices increases. In a

model with a variety of devices running different clocks and authenticating with each other at different intervals, this would help ensure that the clocks stay synchronized.

4.3 Exchanging Unique Identifiers, Renewing Long-Term Keys and Further Ranging

In the first three steps, we have provided three of four desired properties of a key agreement protocol. These properties were defined in [39] as follows:

1. Both participants possess K_{AB} which they can verify is new.
2. It is infeasible to find K_{AB} by eavesdropping on the protocol, even if the protocol is repeated many times.
3. Both participants have equal input into the equation that defines K_{AB}.
4. Both participants know the identity of the other party who may possess K_{AB}.

Regarding the fourth property, our solution so far is not necessarily satisfactory. A pre-shared table of K_n with corresponding identities might be used, where the encrypted payload is decrypted with every K_n in the table and the identity is assigned according to the table if one of the timestamps yields a successful authentication. This solution is sub-optimal for two reasons: (1) the false positive rate for adversaries trying to guess the key is increasing with every new K_{n+1} in the table. Although the unusually large key size alleviates these concerns for $n < 1000$, it is still not the scalable solution we are looking for when we aspire for interoperability. (2) the decryption attempts take time and energy. The time component adds complexity to the error-catching based on timestamps.

Assuming that a Class User ID (bits 9-16 in Table IV) can be reserved for our authentication solution, using the cleartext application type allows a receiver to look up one of 64 keys to be used for decrypting messages. The lookup table used for this purpose should have a unique identifier for each device as a primary key. For this purpose we propose a version of the Maritime Mobile Service Identity (MMSI) to be pre-assigned to all marine assets capable of wireless communication. We believe this to be the trend regardless of our underwater communication efforts [40]. The AIS (Automatic Identification System, for tracking ships) builds on MMSI, therefore the fusing of surface and UW assets can be achieved easily if both carry the same individual identifiers. The 9 decimal digits of the MMSI are converted into 30 bits, as such they conveniently fit the 32-bit payload. We have therefore found a way to secure the exchange of unique identifiers. While AIS uses its own physical layer protocol based on ISO/IEC 13239:2002 and has its own proposals for securing it, e.g., [41], the establishment of an underwater AIS seems feasible if the MMSI can be relayed through an acoustic/radio gateway.

A and B can thus securely negotiate much higher bandwidth and/or lower packet loss physical layers, such as those described in [42] or [43].

At the end of the protocol, it is prudent to delete T_A, CD_A and T_B, CD_B from memory after deriving K_{AB}, so that the capture of A or B would not enable an adversary to derive K_{AB} and decrypt previously recorded messages with it. The derived session keys should instead be stored and looked up in a table where the JANUS cleartext header determines the session key to be used. For further communications with the session key, the cleartext SYN and ACK flags should both be set to 0 and 1. Since the introduction of the session key it is not straightforward which key, if any, the devices should use to try to decrypt communications. The keys could all be tried and the cleartext fitted to expectations, but that would require more than necessary computational power and complexity. The following table provides clarification:

Table 5 Flag and key use for the protocol messages

Message Number	SYN	ACK	Key to be used
1.	1	0	K_n
2.	1	1	K_n
3. and following	0	1	K_{AB}
Wide-area transmission when required	0	0	according to MMSI

However, since our session key is only 64 bits long and we used timestamps to derive it, resistance against brute-force attacks is not necessarily ensured in the long term. If secure communication between A and B is desired beyond 10000 packets, K_{AB} can be used as a key wrapper under which a longer key K_2 is communicated between A and B. This could be the case if continuous data transmission is desired. The device making up K_2, for example by randomly generating it, would assume the role A. If this long-term key is a new 2040 bit long-term key, it could be transmitted with a cargo length specified in less than a minute. A series of baseline packets would be possible, but that would waste time and therefore bandwidth due to the repeated need to encode identical headers. Instead, the schedule flag located at the sixth bit of the JANUS header should be set to 1 for this purpose. The 8 remaining bits in the encrypted payload of the last packet should be used to detect adversarial modifications of the long-term key with reasonable probability. This can be achieved by an 8-bit CRC $p(x) = x^8 + x^2 + x^1 + 1$, initialised to 0 (as specified by the JANUS for cleartext use as well) calculated over the cleartext, and including that CRC in the ciphertext in addition to the unchanged CRC of the baseline packet. Having the CRC in the ciphertext will protect against adversarial as well as accidental modifications of the packet. The receiving device could confirm correct (as per encrypted and cleartext CRCs) reception of the K_2 in one baseline packet with the CRC this time being encrypted under the new K_2.

4.4 Unicast secure communication

Once keys have been generated and stored along with unique identifiers of the devices, another application would be secure unicast communication. The
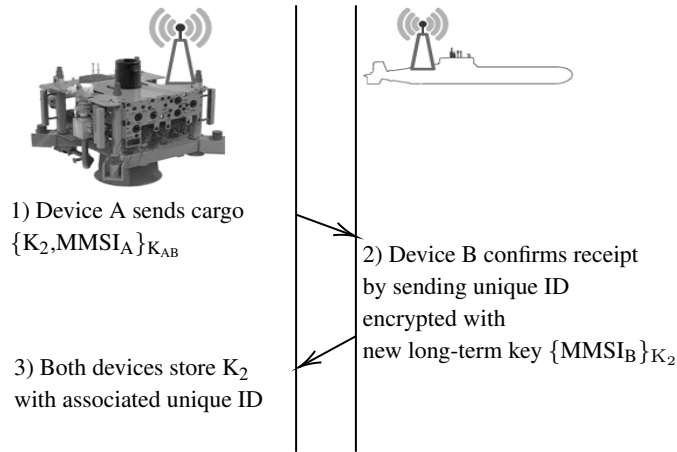
1) Device A sends cargo $\{K_2, MMSI_A\}_{K_{AB}}$

2) Device B confirms receipt by sending unique ID encrypted with new long-term key $\{MMSI_B\}_{K_2}$

3) Both devices store K_2 with associated unique ID

Fig. 2 An illustration of the option to renew a long-term key by wrapping it in the session key.

unicast communication concept would enable the hardening of underwater communication security according to general cyber *need to know* principles. This type of communication would necessitate the unique identifier of the sender to be sent in cleartext so that the corresponding key can be looked up by the recipient. A packet ensuring secure unicast would need to have the following pre-conditions:

- An application type is standardized in the JANUS header that identifies this unicast mode
- Previous steps of our method for deriving a bilaterally shared session key K_{AB} have been successful
- A cargo specification in the JANUS header, because the MMSI as a suitable unique identifier would already take 30 of the 34 bits in the ADB
- A lookup table of MMSI and session key(s) on the recipient device.

This would allow packets of the format $MMSI_B, \{payload\}_{K_{AB}}, HMAC$ to be transmitted securely to device B through a wide area network using the MMSI as an address. The cleartext inclusion of the MMSI is deemed necessary for inter-networking efforts, where devices who received the packet but were not the addressee may choose to re-transmit. The HMAC (keyed-hash message authentication code) should be calculated over the entirety of the packet including the JANUS header using the session key. This would authenticate the information there, most importantly the Class ID that determines which applications are to be used in interpreting the packet. Because of the bandwidth limitations, the HMAC also serves the purpose of a compressed sender designation: the recipient tries to decrypt the packet with all the keys found in its onboard database of MMSI and session key pairs. The session key that can verify the HMAC as authentic will indicate the correct MMSI of the sender in

the lookup table. When considering AUVs, the payload above could be a command and control signal, ideally compressed according to a pre-shared lookup table.

Table 6 JANUS Bit Allocation in the Unicast Secure Packet

Bits	Descriptor	Comments
1-22	Baseline header	JANUS defined as per above
23-30	Cargo length specification	JANUS defined: reserves the channel, in this case with i=60 for another second.
31-54	ADB	24 bits of routing data from the MMSI range for autonomous systems (to be assigned)
55-56	Syn/Ack Flags	Aids the treatment of the packet as per Table 5
57-64	8-bit Checksum	JANUS defined: 8-bit CRC run on the previous 56 bits with $p(x) = x^8 + x^2 + x^1 + 1, init = 0$
65-128	Encrypted Payload Cargo	64 bits can be encrypted with RC-5
129-137	HMAC	Calculated over the last 128 bits, it allows the recipient to authenticity of the message.
138-146	8-bit Checksum	8-bit CRC run on the previous 56 bits with $p(x) = x^8 + x^2 + x^1 + 1, init = 0$

5 Results and Discussion

5.1 Mitigation of selected attacks

As usual with authentication methods, assets participating in our protocol are classified into friendly (well-meaning) and malicious (adversarial) ones according to their ability to prove their identity. Methods to prove a false identity are considered attacks on the authentication method.

Due to our proposed design choice of using only the ADB, we note that the encrypted message can be changed without knowledge of the encryption key along with the cyclic redundancy check. This would allow adversarial submissions of valid JANUS packets which would fail to authenticate. Our proposed mitigation is to eliminate the possibility of attacks based on repeated submissions: error-catching should be implemented for valid packets with an already used timestamp in the decrypted ADB.

Protection against replay of earlier captured messages is achieved by validating the decrypted pongs against a time stamp. If the decrypted device B time stamp does not provide nearly-symmetric packet travel time estimates (allowing for currents and modelled mutual clock drift statistics and corrected for encryption and decryption processing delays), a failed authentication notification results. It is of course possible for an adversary to derive the cryptographic key used for authentication after observing and logging many

authentications with that key [44], but our application is not likely to provide sufficient examples to enable this breach.

Challenge intervals should be informed by the expected maximum approach speeds. E.g. a challenge being sent out every 5 minutes would ensure that an AUV with a maximum speed of 3 m/s gets interrogated within a kilometer of entering the reception range. When rolling over the 6-day interval covered by the 29-bit timestamp, device A is advised to offset its challenge by 30 seconds to mitigate an attack where a ciphertext recorded 6 days ago is replayed. 30 seconds are deemed enough for the signal to be beyond range. These assumptions would result in the necessity to issue new keys every 60 days.

Denial of service (DoS) is possible through repeated re-transmission of earlier messages as well as the modification of the ciphertexts and the corresponding CRC. However, denial of service would also be possible without the proposed security method by making noise. This is the case for all wireless communications, but more so for acoustic communication. Therefore we assign the DoS challenges to the physical layer realm and do not provide design features to avoid them in this paper.

We believe that cybersecurity measures suggested for standardization today should also be vetted for resistance to quantum computers. As our scheme is based on symmetric cryptography, it is somewhat resistant. Furthermore, the unusually large key size gives us sufficient certainty that quantum-enabled algorithms like that of Grover [45] will not compromise our method.

5.2 Ranging functionality and its possible ramifications

Regarding the assumptions made in step 3 of the identification of friend or foe, we assume that over the timescale of the exchange, the primary eigenpath is reciprocal between A an B and does not change appreciably. This is likely the case if the path is not interacting with the sea surface because A and B are at depths exceeding 100 meters. Whilst the symmetry of the acoustic channel between A and B isn't necessarily given, there wouldn't be a successful exchange of data for a challenge and a response in such cases anyways. It might be possible to estimate such asymmetric channels for the use of coherent physical layers, but this wouldn't fit our requirement of using just one JANUS baseline packet each way. It is also likely that the additional complexity introduced with the use of such more advanced physical layers would come at the cost of lost interoperability.

By sending out the authentication challenge in cleartext, device A could give away its clock signal, and with it its location. This expression of trust is not advised in an adversarial environment, because it could enable cyber attacks based on the provoked exhaustion of the ciphertext space by an intruder masquerading as A, or physical attacks based on the necessary response from B confirming its presence. Nevertheless, our present protocol can be modified in line with civilian transponder interrogation such as Mode S in air traffic [46], where collision avoidance and the avoidance of over-interrogation are priorities. Depending on the use case, this might be a proportionate measure to maintain

the interoperability of JANUS across organisational borders while providing accountability. In [47] operational safety is seen to increase by sending location and heading data in addition to the MMSI. The two clock drifts do not impact the range estimate from our protocol, with vehicle motion and water currents contributing only second-order errors, as we show in Appendix A.

5.3 Applicability for different underwater assets

Authentication services create a foundation for an IoUT. Our authentication method can be generalised to a wider range of subsea assets than AUVs; all devices with an acoustic modem would profit from an inter-operable authentication method. Nevertheless, the requirement for secured wireless communication imposes constraints, e.g. cryptographic keys must be securely distributed. The mobility of AUVs makes key distribution through UW WiFi or short-range directive optical communication (which is remarkably secure to interception) easier, and more feasible on a regular basis, than between fixed assets. If new keys cannot be exchanged regularly and if there are many authentication attempts, security might be compromised. For a heterogeneous system that includes both fixed and mobile assets, keys might be regularly exchanged and clocks synchronised by an AUV mule activity, in which an AUV would visit all other assets in the system to perform key exchange and synchronisation by very short-range directive optical communication, which presents a much more challenging task to break into compared to omnidirectional acoustic signalling. In the case of asset classes that can't or don't want to exchange new keys, key derivation should be considered. This could be done using any one-way function, if parts of the initial long-term key and the calendar year and week are inputs to that function.

However, the applicability of the authentication method presented here for use in authenticating more than two devices simultaneously – meaning more than a bilateral relation – is limited. If in addition to devices A and B, a friendly device C is within hearing distance, it could derive wrong MMSI/session key pairs. This shortcoming is not relevant for most underwater economic ecosystems today, but it could be in a future where several previously unidentified friendly devices answer the same call. While mitigation is possible by setting the time window validity lower, we seek a solution that is more scalable. This problem is among those that we intend to address in our future research.

5.4 Verification and Validation

We implemented the proposed authentication protocol and tested it in air, in a small water tank, and in seawater in an outdoor harbour environment in the Trondheim fjord.[1] (B2) Two Subnero Research Edition modems were used in these tests. We had to write our own implementation of RC5 in Java for the

---

[1]In addition to these physical tests, in silico testing was performed using the Network Simulator 3 Underwater Acoustic Network (NS3 UAN) library. Electronic supplementary material has been made available to JMST to aid reproduction of all claimed results so far as well as further verification and validation.

agent to call, as the UnetStack Software-Defined Open-Architecture Modem Audio Driver is written in Java/Groovy. (B3) The validation tests successfully demonstrated the authentication protocol by deriving the same session key on the two devices, and put an upper bound of 3 seconds on all communication overhead resulting from the implemented security countermeasure. This overhead could likely be decreased by optimizing the hardware and software.

Our requirements, the specifications we derived from them and fulfilled with our solution can be summed up as follows:

Table 7 Requirements and Specifications in the Authentication of Underwater Assets

Requirement	Specification
Minimized number of packets	2 packets sufficient for friend ID
Fits JANUS baseline ADB	34 bits
Range at least 10 km	10+ km for 11 kHz acoustics
Key size at least 256 bits	2040 bits
Allows autonomous bilateral ranging	Through redundant timestamps
Run-time demonstrated	3 seconds

Before being put to use in industry, a new technology or procedure needs to be extensively verified and validated in several steps. By verification we mean testing that the technology or process meets requirements. At least three verification steps are recommended to be performed *in silico*:

Firstly, crypto-analysis of the RC5 variant proposed to exchange the first two messages[2] should be sought. The small block size might be exploitable, whereas the larger than usual key size and the high number of rounds could compensate for that. Based on crypto-analytic results, the number of rounds might be decreased if reasonable security can be achieved despite the minimal block size.

Secondly, the encryption, coding, decoding and decryption times with the hardware and software available on the UW assets should be characterised, together with the mutual clock drift statistics.

Thirdly, transmission technologies contributing to physical layer security such as predictive beamforming should be integrated in the UW assets [48]. This kind of development would be greatly accelerated by using state of the art digital twins [49] [50] including representative propagation modelling and adequate computational power and memory.

After the verification phase has been initiated, and partially overlapping with it to provide iteration opportunities, operational strategies and technologies should be clarified through validation. The validation stage should include testing unforeseen difficulties with AUVs, in addition to testing already done with modems suspended from the surface. In real WUCaN use cases that impact economic and usability aspects this could involve the tie-in of orthogonal security cross-checks, such as sonar object recognition, so that more

---

[2]In the notation RC5-w/r/b, where w=word size in bits, r=number of rounds, b=number of 8-bit bytes in the key, the variant satisfying our size restrictions and maximising security beyond that which would be known as RC5-16/255/255.

rigorous authentication challenges can be directed at unidentified assets in proximity.

After the method has been rolled out as a pilot project, corporate security audits could use documentation from the verification and validation phase to inform their judgement of underwater communications. This could include penetration testing through partially UW red team exercises, with the validation goal to prove inability to obtain friendly identification without initial knowledge of the key.

5.5 Authentication and Safety

The importance of communication using the JANUS standard for operational safety is discussed in [47], where it is being implicitly assumed that there are only honest underwater assets. Authentication as a foundational requirement for security can help ensure that those operational safety goals are upheld in environments without total trust. Collaborative safety mechanisms have cybersecurity as a cornerstone technological necessity [51].

It is conceivable that AUVs will be credited as a safety barrier for mitigating oil and gas blowouts, similar to how ROVs worked to contain the Deepwater Horizon spill. Many AUVs work concurrently in mitigative scenarios. Valves operated by AUVs in a safety-critical setting can include all-electric valves on the Christmas Trees permanently located subsea [52]. Such solenoid valves could need to be operated by AUVs, e.g to connect emergency power or apply the torque from batteries or motors on an AUV. If the Christmas Tree has an acoustic modem and a wired connection to a control room, operators can use the proposed authentication method to ensure that an AUV with the right key and working acoustic communication is approaching. The authorisation following authentication should be considered an essential service (as in the IEC/ISO 62443 series of international standards, henceforth 62443) for safety-critical resources. While describing the fundamentals of our authentication method, we have employed a pair of pre-shared keys K. In the framework of a more sophisticated access control scheme, an almost arbitrary variety of long-term keys K_1 to $K_{1,26e+614}$ can be issued to different roles or organisations. If this option is used, the long-term keys should be tried for every authentication attempt where no contextual information is available on the claimed unique identity. This will serve to reduce the false negatives due to the use of different keys. Due to the large key size, the false positives will not rise significantly by doing so. The simple approach outlined here may thus be extended not only to assets beyond AUVs but also to more complex and secure nested systems. The key size offers also the opportunity to establish national and global systems, if key management services are provided by maritime authorities. The details of such a key management scheme shall be described in further research, in the meantime it suffices to say that the number of operating organisations is virtually unlimited.

5.6 Compliance with standards

As has been amply demonstrated by IoT developments above water, there is potentially great cost to users who do not establish sufficient communication security and we can expect the same to be true for the IoUT. The 62443 imposes compliance specifications on the security in industrial communication networks. The scope of 62443-1-1, among others, specifically includes: (i) oil and gas production operations as defined by functionality in chapter 1.2, (ii) activities necessary for predictable operation of the process in chapter 1.4, and (iii) assets needed for disaster recovery according to asset-based criteria in chapter 1.5. Based on these scoping criteria, it can be argued that AUVs used for inspections or disaster response are within the purview of 62443. Identification and Authentication Control (IAC) is the Fundamental Requirement 1 in 62443, and IAC influences the security levels (SL) assigned in 62443. This means that compliance with 62443 cannot be achieved as long as there is no authentication in all of the industrial automation and control system components. While UW devices are not yet networked, there is a strong incentive to do so, and if AUVs are networked without authentication, compliance with 62443 will not be possible.

The choice of entity authentication protocols is treated by the ISO/IEC 9798 family of standards, where part 2 concerns those methods using symmetric encryption algorithms. Our proposal is a refinement of the two-pass mutual authentication protocol described in chapter 7.3.2 of that standard, where we did not include a unique identifier of the recipient within the same encrypted package as the timestamp. This is a design option left open by the standard, as it can be also read in the clarification of the relevant standard section provided in [53].

The part of step 3 of our proposal that establishes a session key uses a one-way function established in line with MAC Algorithm 1 described in the ISO 9797-1:2011 standard on Message Authentication Codes using a block cipher. It could be completely and unambiguously defined by the selection of the RC5-64/255/255 block cipher algorithm, padding method 2, and the length of 64 bits.

If, for whatever reason, Venilia [19] is to be used for encrypted communications, the authentication method we describe for deriving a session key might still be useful as an add-on. The 256-bit keys that the Tiny Underwater Block Cipher uses can be derived with our current proposal. This will then provide the forward security property highly recommended for a scalable solution and allow distance to be introduced as a risk metric, e.g. for further use in ensuring physical security or collision avoidance.

6 Conclusion

We have in this paper presented a draft protocol based on the first digital UW communications standard, JANUS. We believe that the initial idea behind JANUS as a 'first contact' handshake protocol is made significantly more

secure by applying our protocol. Two friendly devices could be confirmed as such before deriving a session key under which they could securely negotiate another, hopefully higher bandwidth physical layer for further communications. The physical security elements of the newly negotiated physical layer would therefore remain confidential.

While the timestamps we propose to be sent for authentication purposes enable ranging through a Time-of-Flight principle, we have not yet conducted tests to determine how accurately this ranging can be performed in practice. Depending on the accuracy of range authentication, actions of different criticality could be authorized. Factors influencing this accuracy will include, but are not limited to: modulation speed of the individual data packets, tick period length of the real time systems used to decrypt and encrypt, and variations in signal speed. Authorization should be defined on the basis of our authentication method to complete an access control framework for AUVs. In the absence of a docking station providing underwater WiFi connection to an enterprise-level authentication solution, AUVs could still derive long-term keys for encrypted communication. One potential solution could be the use of a shared medium or of Physically Unclonable Functions (PUFs) as a source of additional keys [54, 55]. This development can be observed in above water IoT radio frequency applications (Wi-Fi) that are also physically exposed [56], resource- and power-constrained [57], and mobile [58]. By deriving keys from sonar signatures instead of radar, and acoustic instead of radio channel state information, similar security [59] could be provided underwater. We intend to pursue this line of research in the future.

Appendix A   Establishing the theoretical accuracy of the ranging functionality

Suppose device A transmits an interrogating ping at T_0. Device A has a clock offset δ_A, which we will assume is constant over the authentication protocol execution.

If the distance between A and B is d, the speed of sound is c and the current velocity along the line joining A and B is v, then B receives the ping at time

$$T_1 = T_0 + \frac{d}{c + v}$$

Ignoring the motions of A and B (which can be included in v) and the processing times (which, if known, can be subtracted out) then the ping timestamp T_{A0} is given by

$$T_{A0} = \delta_A$$

Device B responds with

$$T_{B1} = T_1 + \delta_B$$

and device A receives this 'pong' at time T_2 given by

$$T_2 = T_1 + \frac{d}{c - v}$$

so device A now knows

$$T_{B1} - T_{A1} = T_0 + \frac{d}{c + v} + \delta_B - (T_0 + \delta_A)$$

which is equivalent to

$$T_{B1} - T_{A1} = \frac{d}{c + v} + (\delta_B - \delta_A) \tag{A1}$$

device A also knows $T_{A2} - T_{B1}$, where

$$T_{A2} = T_2 + \delta_A = T_1 + \frac{d}{c - v} + \delta_A$$

such that

$$
\begin{aligned}
T_{A2} - T_{B1} &= T_1 + \frac{d}{c - v} + \delta_A - (T_1 + \delta_B) \\
&= \frac{d}{c - v} + (\delta_A - \delta_B)
\end{aligned}
\tag{A2}
$$

By adding A1 and A2 we obtain

$$
\begin{aligned}
T_{A2} - T_{A1} = \frac{d}{c + v} + \frac{d}{c - v} &= \frac{(dc - dv) + (dc + dv)}{c^2 - v^2} \\
&= \frac{2dc}{c^2 - v^2} = \frac{2d/c}{1 - (v^2/c^2)}
\end{aligned}
\tag{A3}
$$

which, given c, gives us a good estimate of d without any involvement of the clock drifts, however large. If v is roughly $10^{-3}c$, we get an estimate of d with error on the order of 10^{-6}.

References

[1] Bleicher, A.: The gulf spill's lessons for robotics. IEEE Spectrum **47**(8), 9–11 (2010)

[2] Potter, J., Alves, J., Green, D., Zappa, G., Nissen, I., McCoy, K.: The janus underwater communications standard. In: 2014 Underwater Communications and Networking (UComms), pp. 1–4. https://doi.org/10.1109/UComms.2014.7017134. https://ieeexplore.ieee.org/document/7017134/

[3] Che, X., Wells, I., Dickers, G., Kear, P.: Tdma frame design for a prototype underwater rf communication network. Ad Hoc Networks **10**(3), 317–327 (2012). https://doi.org/10.1016/j.adhoc.2011.07.002

[4] Shukla, A., Karki, H.: Application of robotics in offshore oil and gas industry—a review part ii. Robotics and Autonomous Systems **75**, 508–524 (2016)

[5] Politakis, G.P.: Modern Aspects of the Laws of Naval Warfare and Maritime Neutrality. Routledge, Geneva (2018)

[6] Nong, H.: Analysis from the maritime awareness project: Beyond the unmanned underwater vehicle incident in the south china sea. The National Bureau of Asian Research (2017)

[7] Smerdon, A., Bustamante, F., Baker, M.: The swigacoustic standard: An acoustic communication standard for the offshore energy community. In: 2016 IEEE Third Underwater Communications and Networking Conference (UComms), pp. 1–4. https://doi.org/10.1109/UComms.2016.7583467. https://ieeexplore.ieee.org/document/7583467/

[8] Yang, G., Dai, L., Si, G., Wang, S., Wang, S.: Challenges and security issues in underwater wireless sensor networks. Procedia Computer Science **147**, 210–216 (2019)

[9] Peng, C., Du, X., Li, K., Li, M.: An ultra-lightweight encryption scheme in underwater acoustic networks. Journal of Sensors **2016**, 8763528 (2016). https://doi.org/10.1155/2016/8763528

[10] Du, X., Peng, C., Li, K.: A secure routing scheme for underwater acoustic networks. International Journal of Distributed Sensor Networks **13**(6), 1550147717713643 (2017). https://doi.org/10.1177/1550147717713643

[11] Dini, G., Duca, A.L.: Seflood: A secure network discovery protocol for underwater acoustic networks. In: 2011 IEEE Symposium on Computers and Communications (ISCC), pp. 636–638. https://doi.org/10.1109/ISCC.2011.5983910

[12] Petroccia, R., Sliwka, J., Grati, A., Grandi, V., Guerrini, P., Munafo, A., Stipanov, M., Alves, J., Been, R.: Deployment of a persistent underwater acoustic sensor network: The commsnet17 experience, pp. 1–9 (2018). https://doi.org/10.1109/OCEANSKOBE.2018.8559262

[13] Petroccia, R., Zappa, G., Furfaro, T., Alves, J., D'Amaro, L.: Development of a software-defined and cognitive communications architecture at cmre. In: OCEANS 2018 MTS/IEEE Charleston, pp. 1–10 (2018). IEEE

[14] Khalid, M., Zhao, R., Wang, X.: Node authentication in underwater acoustic sensor networks using time-reversal. In: Global Oceans 2020: Singapore–US Gulf Coast, pp. 1–4 (2020). IEEE

[15] Diamant, R., Casari, P., Tomasin, S.: Cooperative authentication in underwater acoustic sensor networks. IEEE Transactions on Wireless Communications **18**(2), 954–968 (2018)

[16] Sieger, M.: Proposal for a sms (chat) application. In: Fifth JANUS Workshop (2019)

[17] Ghannadrezaii, H., Bousquet, J.-F.: Securing a janus-based flooding routing protocol for underwater acoustic networks. In: OCEANS 2018 MTS/IEEE Charleston, pp. 1–7 (2018). https://doi.org/10.1109/OCEANS.2018.8604858

[18] Souza, E., Wong, H.C., Cunha, Í., Cunha, Í., Vieira, L.F.M., Oliveira, L.B.: End-to-end authentication in under-water sensor networks. In: 2013 IEEE Symposium on Computers and Communications (ISCC), pp. 000299–000304 (2013). IEEE

[19] Hobbs, A.-M., Holdcroft, S.: Janus Class 17 "Venilia": Secure Pre-Canned Messaging. Dstl Cyber and Information Systems, 1–22 (2021)

[20] Boyd, C., Gellert, K.: A modern view on forward security. The Computer Journal **64**(4), 639–652 (2021)

[21] Neuman, C., Yu, T., Hartman, S., Raeburn, K.: The kerberos network authentication service (v5). Report, RFC 4120, July (2005)

[22] Finseth, C.: An access control protocol, sometimes called tacacs. Report, RFC 1492, July (1993)

[23] Rigney, C., Willens, S., Rubens, A., Simpson, W.: Remote authentication dial in user service (RADIUS). Internet Engineering Task Force RFC 2865, June (2000)

[24] Wang, J., Lu, C., Li, S., Xu, Z.: 100 m/500 mbps underwater optical

wireless communication using an nrz-ook modulated 520 nm laser diode. Optics Express **27**(9), 12171–12181 (2019). https://doi.org/10.1364/OE.27.012171

[25] Lloret, J., Sendra, S., Ardid, M., Rodrigues, J.J.P.C.: Underwater wireless sensor communications in the 2.4 ghz ism frequency band. Sensors (Basel, Switzerland) **12**(4), 4237–4264 (2012). https://doi.org/10.3390/s120404237

[26] Mangione, S., Galioto, G.E., Croce, D., Tinnirello, I., Petrioli, C.: A channel-aware adaptive modem for underwater acoustic communications. IEEE Access **9**, 76340–76353 (2021). https://doi.org/10.1109/ACCESS.2021.3082766

[27] Petroccia, R., Cario, G., Lupia, M., Djapic, V., Petrioli, C.: First in-field experiments with a "bilingual" underwater acoustic modem supporting the janus standard. In: OCEANS 2015-Genova, pp. 1–7. IEEE

[28] ISO/IEC: Standard 8802-2 information technology — telecommunications and information exchange between systems — local and metropolitan area networks — specific requirements — part 2: Logical link control (1998)

[29] Barker, E., Mouha, N.: Recommendation for the triple data encryption algorithm (tdea) block cipher. Report, National Institute of Standards and Technology (2017)

[30] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., Manifavas, C.: A review of lightweight block ciphers. Journal of cryptographic Engineering **8**(2), 141–184 (2018)

[31] Rivest, R.L.: The rc5 encryption algorithm. In: International Workshop on Fast Software Encryption, pp. 86–96. Springer

[32] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: Simon and speck: Block ciphers for the internet of things. IACR Cryptol. ePrint Arch. **2015**, 585 (2015)

[33] De Cannière, C., Dunkelman, O., Knežević, M.: Katan and ktantan — a family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Gaj, K. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2009, pp. 272–288. Springer

[34] Engels, D., Saarinen, M.-J.O., Schweitzer, P., Smith, E.M.: The hummingbird-2 lightweight authenticated encryption algorithm. In: International Workshop on Radio Frequency Identification: Security and Privacy Issues, pp. 19–31. Springer

[35] Hobbs, A.-M., Holdcroft, S.: Tiny Underwater Block cipher (TUBcipher): 27-bit Encryption Scheme for JANUS Class 17. Dstl Cyber and Information Systems, 1–22 (2021)

[36] Kebkal, K., Kebkal, O., Glushko, E., Kebkal, V., Sebastiao, L., Pascoal, A., Gomes, J., Ribeiro, J., SIlva, H., Ribeiro, M., *et al.*: Underwater acoustic modems with integrated atomic clocks for one-way travel-time underwater vehicle positioning. In: Proceefings of the Underwater Acoustics Conference and Exhibition (UACE) (2017)

[37] Del Grosso, V., Mader, C.: Speed of sound in sea-water samples. The Journal of the Acoustical Society of America **52**(3B), 961–974 (1972)

[38] Stojanovic, M.: On the relationship between capacity and distance in an underwater acoustic communication channel. SIGMOBILE Mob. Comput. Commun. Rev. **11**(4), 34–43 (2007). https://doi.org/10.1145/1347364.1347373

[39] Boyd, C.: Towards a classification of key agreement protocols. In: Proceedings The Eighth IEEE Computer Security Foundations Workshop, pp. 38–43 (1995). IEEE

[40] Ferreira, F., Alves, J., Leporati, C., Bertolini, A., Bargelli, E.: Current regulatory issues in the usage of autonomous surface vehicles. In: 2018 OCEANS - MTS/IEEE Kobe Techno-Oceans (OTO), pp. 1–9 (2018). https://doi.org/10.1109/OCEANSKOBE.2018.8558875

[41] Goudosis, A., Katsikas, S.: Secure ais with identity-based authentication and encryption. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **14**(2) (2020)

[42] Chitre, M., Shahabudeen, S., Freitag, L., Stojanovic, M.: Recent advances in underwater acoustic communications & networking. In: OCEANS 2008, pp. 1–10 (2008). IEEE

[43] Kilfoyle, D.B., Baggeroer, A.B.: The state of the art in underwater acoustic telemetry. IEEE Journal of oceanic engineering **25**(1), 4–27 (2000)

[44] Biryukov, A., Kushilevitz, E.: Improved Cryptanalysis of RC5, pp. 85–99 (2006). https://doi.org/10.1007/BFb0054119

[45] Bernstein, D.J.: Grover vs. mceliece. In: International Workshop on Post-Quantum Cryptography, pp. 73–80 (2010). Springer

[46] Trim, R.: Mode s: an introduction and overview. Electronics & Communication Engineering Journal **2**(2), 53–59 (1990)

[47] Ferreira, F., Petroccia, R., Alves, J.: Increasing the operational safety of autonomous underwater vehicles using the janus communication standard. In: 2018 IEEE/OES Autonomous Underwater Vehicle Workshop (AUV), pp. 1–6 (2018). IEEE

[48] Song, A., Stojanovic, M., Chitre, M.: Editorial underwater acoustic communications: Where we stand and what is next?, 1–6 (2019). https://doi.org/10.1109/JOE.2018.2883872

[49] Luo, H., Wu, K., Ruby, R., Hong, F., Guo, Z., Ni, L.M.: Simulation and experimentation platforms for underwater acoustic sensor networks: Advancements and challenges. ACM Computing Surveys (CSUR) **50**(2), 1–44 (2017)

[50] Ulmstedt, M., Stålberg, J.: GPU Accelerated Ray-tracing for Simulating Sound Propagation in Water (2019)

[51] IEC Market Strategy Board safety in the future project team, directed by Dr Kazuhiko Tsutsumi, MSB Convenor, Mitsubishi Electric Corporation, with major contributions from the lead project partner, Dr Coen van Gulijk, TNO: Safety in the future. White paper, International Electrotechnical Commission (2020)

[52] Mahler, C., Glaser, M., Schoch, S., Marx, S., Schluenss, S., Winter, T., Popp, J., Imle, S.: Safety capability of an all-electric production system. In: Offshore Technology Conference. Offshore Technology Conference

[53] Boyd, C., Mathuria, A., Stebila, D.: Protocols for Authentication and Key Establishment vol. 1. Springer, ??? (2003)

[54] Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 523–540. Springer

[55] Mayrhofer, R., Gellersen, H.: Shake well before use: Intuitive and secure pairing of mobile devices. IEEE Transactions on Mobile Computing **8**(6), 792–806 (2009)

[56] Zenger, C.T., Pietersz, M., Zimmer, J., Posielek, J.-F., Lenze, T., Paar, C.: Authenticated key establishment for low-resource devices exploiting correlated random channels. Computer Networks **109**, 105–123 (2016). https://doi.org/10.1016/j.comnet.2016.06.013. Special issue on Recent Advances in Physical-Layer Security

[57] Zenger, C.T., Chur, M., Posielek, J., Paar, C., Wunder, G.: A novel key generating architecture for wireless low-resource devices. In: 2014

International Workshop on Secure Internet of Things, pp. 26–34 (2014). https://doi.org/10.1109/SIoT.2014.7

[58] Staat, P., Elders-Boll, H., Heinrichs, M., Kronberger, R., Zenger, C., Paar, C.: Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. arXiv preprint arXiv:2010.06613 (2020)

[59] Guillaume, R., Winzer, F., Czylwik, A., Zenger, C.T., Paar, C.: Bringing phy-based key generation into the field: An evaluation for practical scenarios. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), pp. 1–5 (2015). https://doi.org/10.1109/VTCFall.2015.7390857