Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 205 (2022) 167–178

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Military Communications and Information Systems (ICMCIS 2022)

Towards Secure and Interoperable Underwater Acoustic Communications: Current Activities in NATO IST-174 Research Task Group

Alexander Hamilton[a], Jack Barnett[a], Amy-Mae Hobbs[a], Konstantinos Pelekanakis[b], Roberto Petroccia[b], Ivor Nissen[c], Dennis Galsdorf[c]

[a] *Defence Science and Technology Laboratory (Dstl), Cyber and Information Systems, Salisbury, United Kingdom*
[b] *NATO Science and Technology Organization Centre for Maritime Research and Experimentation (CMRE), La Spezia, Italy*
[c] *Bundeswehr Technical Center for Ships and Naval Weapons Maritime Technology and Research (WTD71), Kiel, German*

Abstract

Although the area of underwater acoustic networking is getting mature and critical for a wide variety of commercial applications, the lack of secure underwater communication standards presents a major impediment for adopting these networking technologies within NATO operations. The NATO Research Task Group IST-174 "Secure Underwater Communications for Heterogeneous Network-enabled Operations" aims to study and to demonstrate secure underwater communications in a holistic approach. In particular, this group's ambition is to define waveforms, network protocols and architectures that will enable underwater connectivity in a secure and interoperable way. To that effect, this paper presents various security concepts and communication systems currently under development that could be included in those standardisation efforts.

Keywords:
Acoustics; cryptography; low-probability of intercept; JANUS; interoperability; underwater telephone;

1. Introduction

Many maritime warfare disciplines have witnessed an increasing interest in the use of autonomous assets to perform the so called dull, dirty and/or dangerous activities. Such autonomous assets provide a significant capability potential due to the fact that they can be deployed in large numbers and conduct cooperative tasks. Yet, cooperation is limited by the amount of data underwater communications can reliably provide. In the underwater environment, both radio and optical signals are greatly attenuated, and acoustic waves remain the most

*Alexander Hamilton. Tel.: +44 (0) 7808 051265.
E-mail address: ajhamilton@dstl.gov.uk.

10.1016/j.procs.2022.09.018

Table 1: IST-174 work structure.

Work package	Description
1	Military use-cases
2	Cryptography
3	Physical layer
4	Networking layer
5	Digital/analogue hybrid communications
6	At-sea experiments

efficient means to communicate underwater for ranges beyond about 50 m. Nonetheless, acoustic-based underwater communications suffer from long propagation delays and low data rates. Factors affecting the quality of the received signals are extended reverberation, frequency-dependent absorption, high motion-induced Doppler and site-specific plus cyclical (i.e., tidal) ambient noise. In addition to those challenges, the lack of secure underwater digital communications standards represents a major bottleneck for supporting NATO operations such as Rapid Environmental Assessment (REA), Mine Countermeasures (MCM), Anti-Submarine Warfare (ASW), Underwater Maritime Situational Awareness (UW-MSA) with ISR and Search and Rescue (SAR). It is important to provide increased resilience and assurance of underwater communications by improved security awareness (e.g., confidentiality, authentication, integrity protection, jamming detection) and improved security measures (e.g., counter-interception by encryption, anti-jamming/spoofing/tampering/hacking).

Existing underwater acoustic communications technologies do not consider security as a performance indicator and focus on software/hardware implementation, range coverage and achievable data rates [1]. Limited studies on underwater network security have appeared in open literature ([2] and references therein). Additionally, existing security solutions in terrestrial networks cannot be applied directly due to the stark differences between the underwater acoustics and the radio channels. Hence, an attacker could easily compromise an underwater acoustic network (UAN) in numerous ways such as jamming [3, 4], leakage of confidential data [5], re-routing of the transmitted information [6], message replay [7], just to name a few. From a military-application perspective, therefore, there is an imperative to design and test software-defined communication systems which will be able to address security attacks in all layers of the Open Systems Interconnection (OSI) stack.

The NATO Research Task Group (RTG) IST-174 "Secure Underwater Communications for Heterogeneous Network-enabled Operations" is currently investigating different key aspects of secure underwater communications. The work items of the IST-174 are summarised in Table 1 and some of them are further described next:

- **interoperability**: based on existing communication standards, highlight existing gaps in secure underwater communications and propose solutions that could be included in standardisation efforts.
- **cryptography**: solutions tailored to the underwater acoustic domain. Aspects of symmetric vs. asymmetric keys, data overhead and key management are being studied.
- **physical layer**: novel coded modulation schemes with the capability to provide secure and reliable underwater acoustic links. There is a focus on the need to adjust transmission parameters such as carrier frequency, bandwidth, transmission rate in order to provide flexibility for meeting different mission specifications.
- **hybrid communications**: combination of digital with analogue underwater acoustic communications on existing legacy equipment such as the underwater telephone (UT).

This paper is organised as follows. The current status of existing NATO standards for secure underwater acoustic networking systems is presented in Section 2. Section 3 describes our cryptographic efforts leveraging on the JANUS standard. Section 4 describes a novel way to generate a key for symmetric crypto-systems during mission. Section 5 highlights our efforts on digitally modulated signals that can achieve low-probability of intercept (LPI) communications. Section 6 presents a hybrid communications scheme for the underwater telephone. Section 7 describes our recent efforts to collect at-sea data and Section 8 draws the conclusions.

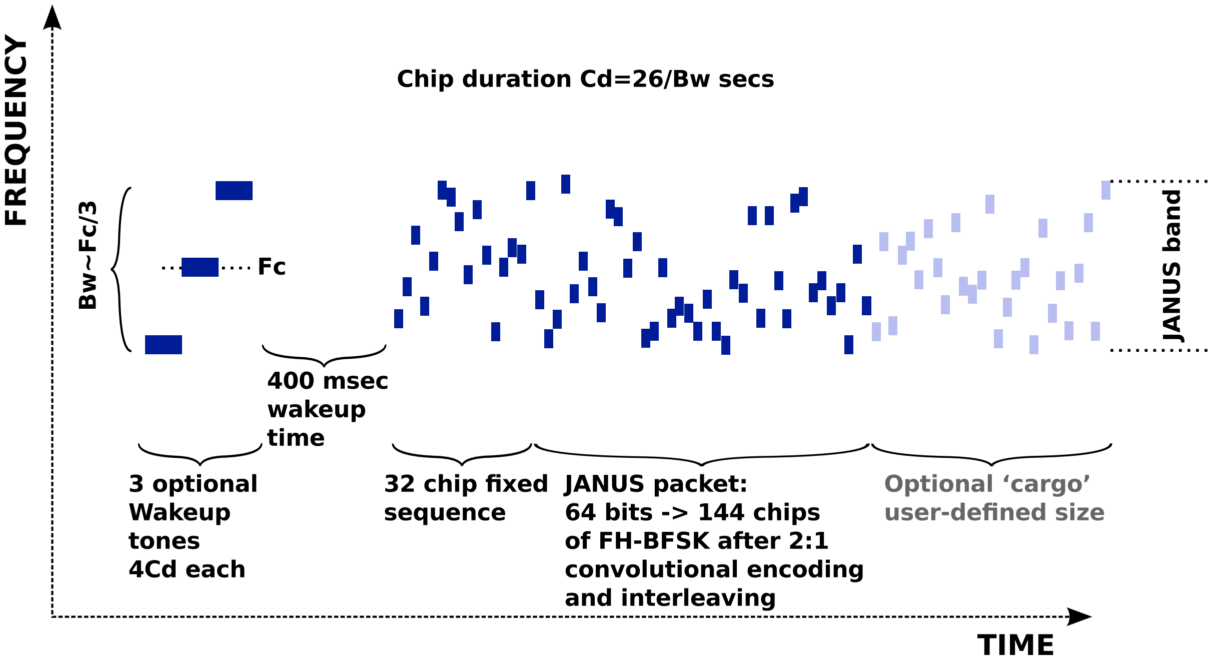


Fig. 1: The JANUS signal in a time-frequency plot.

2. Current status of secure & interoperable underwater acoustic communications

This RTG focuses holistically on secure interoperable underwater communications, with a specific emphasis on cryptography (work package 2) and Physical Layer (work package 3).

2.1. Overview of JANUS

Present NATO underwater communication capabilities are standardised as follows:

- STANAG 1475 (old 1074 and 1298) - analogue tactical and safety communication between operators;
- STANAG 1481 - Identification of Friendly Submarine (IFS - ASIP-01) for the digital secure and covert communication stack from the physical layer to military application layer for manned and unmanned submerged vehicles; and
- STANAG 4748 (JANUS - ANEP-87) - open digital communications.

The IFS is a NATO SECRET standard and so it is not allowed to be used for research purposes with the objective to publish results in the open literature. Hence, we have concentrated on JANUS, which is an open standard and facilitates research outcomes without any bureaucratic restrictions.

JANUS is the first and (as of today) the only open standard for digital underwater acoustic communications. Its bit allocation table and the signal modulation is described in [8] and a reference implementation is freely available online [9]. Figure 1 shows a time-frequency representation of a JANUS packet. Three (optional) ”wake-up” tones are followed by the detection preamble, which is a 32-bit Binary Frequency-Shift-Keying (BFSK) modulated sequence. Then, there is a message of 64 bits that is mapped into a 144-bit Frequency Hopping BFSK (FH-BFSK) modulated sequence. These 144 bits define the ”baseline” JANUS packet. Depending of the message type, 34 bits (application data block) out of 64 bits is the maximum data size that can be used in the baseline packet. If more data is required, a “cargo” signal of arbitrary size can be appended at the baseline packet using the same FH-BFSK modulation. The JANUS waveform has been designed to be scalable in frequency with all parameters being ratiometrically calculated from the centre frequency. A centre frequency of 11520 Hz is chosen, resulting in a frequency band between 9440 and 13600 Hz and in a bit rate of 80 bps. The key characteristics of JANUS are its simplicity of implementation and its ability to cope with noisy and highly reverberant channels. During the last six years, JANUS has been extensively demonstrated in various applications such as transmission of automatic identification system (AIS) and meteorological and oceanographic (METOC) data to underwater assets, in Distressed Submarine (DISSUB) scenarios, and for the exchange of short text messages (*WetsApp* chat) [10].

As originally designed, JANUS had no provisions for native and built-in security aspects. However, the content of a JANUS packet (both cargo payload and application data block) can be encrypted using conventional techniques to ensure confidentiality, integrity and authenticity of the exchanged information. However, given the characteristics of underwater acoustic communications (i.e., limited bandwidth, reduced bit rate, long propagation delay and possible intermittent connectivity), some traditional cryptography approaches may be less practical and effective in UANs, as discussed in Section 2.2.

2.2. Traditional Security Approaches

Particularly for military users, ensuring the confidentiality, integrity and authenticity of information is a key requirement. Confidentiality is usually achieved on traditional above-water systems by the use of cryptographic algorithms to encrypt data at the source and decrypt it at the destination using a key. The most common cryptographic algorithms fall into two categories:

1. Block Ciphers, such as AES [11] in block cipher modes.
2. Stream Ciphers, such as ChaCha [12], or block ciphers in stream cipher modes, such as Galois Counter Mode (GCM).

However, the harsh conditions and long latencies of the underwater acoustic channel drive bit rates below optimal ranges for the majority of standard cryptographic security techniques. This motivates the development and applications of algorithms specific to the underwater use case.

2.3. Block Ciphers

The most widely used block cipher, AES, has a block length of 128 bits, meaning that this is the smallest number of bits that the algorithm can work with. Any data packet of length less than 128 bits must be padded with dummy data to fill the difference. A standard baseline JANUS packet contains only 34 bits of data and so would require an additional 94 bits of padding to be transmitted by extending the packet payload. In this case the 34 bits of user data would make up only 27% of the data transmitted – a huge inefficiency in the already limited underwater channel.

2.4. Stream Ciphers

Stream ciphers do not have a minimum length requirement and so do not require any additional padding of transmitted data. Encryption is performed by generating a key-based pseudo-random sequence K and applying the XOR operation, addition modulo 2, bit-wise on the plaintext P to generate the ciphertext C, such that $C = K \oplus P$.

There is, however, a strict requirement to not encrypt different plaintext messages P_1, P_2 using the same keystream K, as doing so would allow an observer to recover both the message and part of the keystream. Reuse of the keysteam can be avoided by either changing the key frequently enough so that every message uses a new key, or including an Initialisation Vector (IV) that changes for every packet encryption. There is no need to keep this IV secret.

The long propagation delays make the frequent key update approach impractical, as the key may change before the message arrives successfully at the destination. This would mean the key used at the receiver to decrypt the message would be different to the key used at the receiver to encrypt the message, and so the decryption would fail. Including an IV as part of the packet would avoid having to frequently update keys but would add additional overhead and so reduce the amount of useful user data that could be transmitted. The number of times a key can be reused securely is proportional to the exponent of the length of the IV, so long duration keys would require more bits to be allocated to the IV. However, when there are no strict constraints on the message length or data rate, sending an IV may not be as problematic, as discussed in Section 2.5.

2.5. Encryption of JANUS cargo messages with AES-GCM

In [13], the authors discuss the challenges of using symmetric (or secret-key) and asymmetric (or public-key) cryptography algorithms for UANs and suggest the use of the AES-GCM algorithm [14], combining AES block cipher in a GCM streaming mode. AES-GCM is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality with a block size of 128 bits. When encrypting the message for confidentiality, the ciphertext has the same size of the plaintext. However, when authenticity is also required, an authentication tag is added using a hash function computed within a binary Galois field. Finally, there is the possibility to add to the message authenticated information that is not encrypted but it is used when computing the authentication tag. For all these options, the usage of an initialization vector is still required, which has to be unique for every packet encryption.

We have successfully employed AES-GCM to encrypt JANUS cargo data during at sea experiments, as reported later in Section 7. A common symmetric key of 256 bits was shared in the network (preloaded on the nodes before deployment). A hash tag was added to ensure not only confidentiality but also authenticity. For traditional terrestrial networks, the size of the tag needs to be larger than 96 bits in order to meet the recommended security requirements. However, in the underwater acoustic domain, where the number of exchanged messages is limited (due to long delays and low bit rates), a shorter tag of 64 or 32 bits can also be used. This is one of the cases where the the limitations of the communication channel can be used as an advantage to reduce the introduced overhead[1]. A hash tag of 32 bits was considered in our experiments. Finally, an IV of 128 bits was used. To avoid sharing the entire IV for each transmission, part of it (112 bits) was static and preloaded on the nodes, while another part (remaining 16 bits) was dynamic and changing at run time. To avoid the same IV twice in the network, the dynamic part was a combination of the node ID and an incremental counter. Each node ID was unique and 4 bits long, since no more than 16 IDs were used in the network. The counter was 12 bits long, since each node was not transmitting more than 4096 messages, and it was increased at each transmission. Using this approach, the 16 bits of the dynamic part of the IV were added to the packet as part of the authenticate information, which was available in clear at the receiver(s) to recompose the IV and proceed with message decryption (i.e., authenticity check and extraction of plaintext). This way of composing/sharing the IV was mainly a proof of concept and different approaches can be used, which may require less bits, in case additional assumptions are made in the network (e.g., nodes synchronization), or more bits, if a larger network or a larger number of transmissions by each node is expected.

3. Venilia

When transmitting only the JANUS baseline packet with no cargo data, the usage of AES-GCM is not practical and a different strategy needs to be used to encrypt the information included in the application data block (up to 34 bits). To address this issue, the Defence Science and Technology Laboratory (Dstl) and the National Cyber Security Centre (NCSC), with support from the IST-174 RTG, developed Venilia, which is an enhancement to JANUS that addresses the need for interoperable, secure, low-latency underwater messaging [15]. Defined as an additional *User Class* of JANUS packet, Venilia specifies the content and format of the standard 34 bit data payload, bits 23 to 56, to include an 8 bits of user data and the remaining 26 bits for network addressing and validation[2]. The structure of Venilia is shown in Fig 2. These 8 bits can represent up to 256 distinct values, which can map to 256 unique messages pre-agreed by users, known as *pre-canned messages*.

[1] It is interesting to notice that while for traditional terrestrial networks recommendations are available regarding parameters or mode of operation settings, this is not yet the case for underwater acoustic networks.

[2] Venilia is specifically designed to encrypt the content of the JANUS application data block and may be less efficient when applied to long messages (e.g., JANUS cargo) for which AES-GCM can be used.

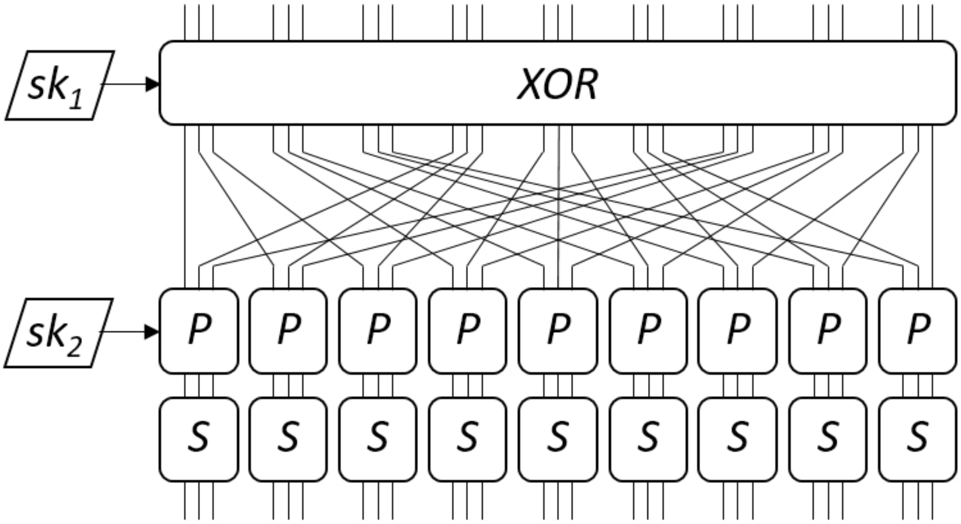


Fig. 3: Bit mapping and basic round structure for one round of TUBcipher. Subkeys sk_1 and sk_2 change for each of the 56 rounds.

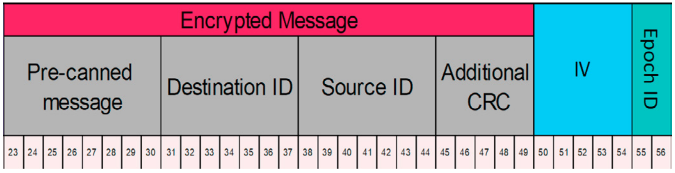


Fig. 2: Venilia bit structure, as part of the larger 64-bit JANUS packet, containing an 8-bit pre-canned message, source and destination IDs, 5 bits of Cyclic Redundancy Check (CRC), a 5-bit IV and 2 bits as a time epoch flag.

The core component of a Venilia packet is an 8-bit integer that represents one of 256 (2^8) possible messages that have been pre-agreed by users, known as a pre-canned messages. This provides a data efficient method of exchanging information, acting as a form of compression for user data to minimise the required packet length, and so reduce the time energy is transmitted through water. Along with the user data, the network address of the sending node and chosen destination address are included, each represented by 8 bit values and 5 bits of cyclic redundancy check to detect any changes to the data in transit and verify the integrity of the message. The CRC is based on the International Telecommunications Union Cyclic Redundancy Check (CRC-5-ITU) and is defined by the polynomial $z = x^5 + x^4 + x^2 + 1$ [16].

Combined, the pre-canned message, source and destination network addresses, and CRC total 27 bits, which are encrypted together using TUBCipher (Tiny Underwater Block Cipher), a novel ultra-short block-length cipher described in section 3.1 below.

An epoch is a period of time of a fixed duration known implicitly to every device on a network, that acts as a nonce (number used once) for the encryption algorithm, so that the same plaintext produces different ciphertext if encrypted in different epochs. It is ordinarily based on system or Unix time. The least significant two bits of this 32-bit variable at the time of encryption defines the Epoch Identifier. Epoch Identifier uniquely resolves the ambiguity of the receiver in which epoch was used to encrypt a message.

An initialisation vector (IV) of 5 bits is included as part of a Venilia packet to reduce the viability of frequency analysis attacks on the encrypted payload. The IV should be updated after every message in an epoch, such that no two messages are encrypted with the same IV in the same epoch.

3.1. TUBCipher

TUBcipher is a substitution-permutation network, a common type of block cipher, producing 27 bits of ciphertext from 27 bits of plaintext [17]. TUBcipher was built by accepting generalisations to PRINTcipher, a pair of block ciphers built for printing on integrated circuits for applications such as radio frequency identification (RFID) tags [18]. TUBcipher expands PRINTcipher in accordance with the former's higher power applications, using independently random, distinct exclusive-or operations for each of its 56 iterations. This independence of "subkeys" - generated by cryptographically mixing the epoch and IV - from one round to the next prevents a viable type of cryptanalysis called a slide attack, an attack that focuses on weak or predictable key schedules.

The round structure of TUBcipher is given in Fig. 3. TUBcipher's similar architecture ensures it inherits much of the security analysis of PRINTcipher; and by extension, the resilience of Venilia to some common cryptographic and communications exploits including spoofing.

However, this work is just encryption; whilst encryption of Venilia's CRC gives some tamper protection, the link itself is still vulnerable to eavesdropping and semantic analysis by an attacker. Future generations of underwater acoustic communications require protections for the packet, not just the payload.

4. Physical layer security

A major challenge in symmetric crypto-systems is key allocation and management. Typically, this is accomplished by pre-loading all keys in all nodes before the mission. This approach is inflexible when a new node joins the network during the mission because no key is allowed to be transmitted over the water in unsecured links. In addition, in the event that a key is compromised, then the entire network is not secure any more.

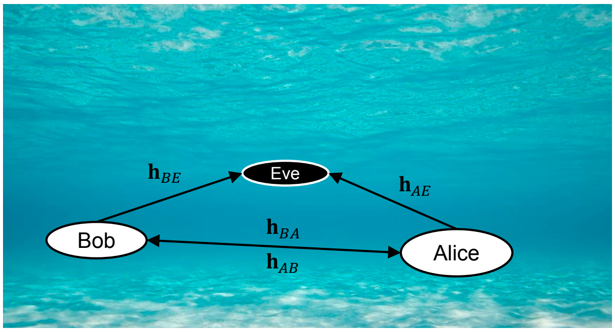


Fig. 4: Scenario of interest: two legitimate users, Alice and Bob, wish to establish secure communications in the presence of eavesdropper Eve.

As Fig. 4 illustrates, Physical Layer Security (PLS) aims to generate a key on the fly between two authenticated nodes (Alice and Bob) without the need to share the actual key [19]. The novelty is that the key generation process requires a few (publicly known) signals to be exchanged between Alice and Bob. The received signals are expected to be highly correlated due to channel reciprocity, which holds under two assumptions: (a) the transmitting transducer and the receiving hydrophone on a node are co-located; (b) the channel time fluctuations are slower than the propagation delay. Typical PLS analysis assumes that an eavesdropper (Eve) who swims in the vicinity is aware of the key generation algorithm and she tries to generate the same key from her intercepted signals.

In this study group, we aim to generate a key based on the following four steps [20, 21]:

1. **Feature extraction**: Alice and Bob exchange JANUS signals to estimate some pre-agreed parameters (e.g., the travel time of the signal). The key idea is that these features are expected to be unique between the two nodes but they will seem random to Eve who swims in the vicinity.
2. **Quantization**: the estimated channel parameters are quantized and represented by a bit vector;
3. **Reconciliation**: Bob and Alice try to correct any differences between their bit vectors. Classical error correction codes such as Reed-Solomon could be used. This procedure involves the exchange of parity bits from Alice to Bob (by using JANUS);
4. **Privacy Amplification**: Alice and Bob are supposed to have the same bit vectors. In order to reduce the amount the information leaked to Eve during reconciliation, a hash function is used. The benefit of using a hash function is that, even if Eve has the knowledge about the hash function, and possess a bit sequence with only one bit that is distinct from the reconciled bits of Alice and Bob, Eve will generate a complete different key.

After Alice and Bob generate the common key, they could use it to encrypt their data based on any symmetric crypto-system such as the AES or the TUBCipher. The main questions to be answered are the key generation rate (per signal transmission) and Eve's effort to break the key other than doing a brute force attack.

5. Phorcys family of waveforms

Phorcys is a novel protocol stack for highly adaptable and secure underwater acoustic communications. By utilising a common "Gorgon" baseband processing, with tunable channel, bandwidth, Direct-Sequence Spread-Spectrum (DSSS) and M-ary Orthogonal Signalling (MOS) parameters, Phorcys allows users to define their own balance between bitrate and resilience for any underwater environment.

Phorcys has been developed as a "secure-by-design" open standard (pending publication), itself inheriting foundations from other security professionals by building on AES, SHA and other established security protocols. Open standards – which reject the fragility of security by obscurity - are vital for enabling international interoperability, and the natural open competition for compliant products support users to receive better implementations.

The security of Phorcys manifests as both Communications Security (COMSEC) - the protection of data by encryption - and Transmission Security (TRANSEC), obfuscation of the waveform, where confidentiality, integrity and authentication are all provided by a pre-placed key. This is accomplished by using only lightweight processing overhead; no contextual security data is added to the packet, which otherwise reduces the available message payload. The Physical layer of Phorcys can be described as below:

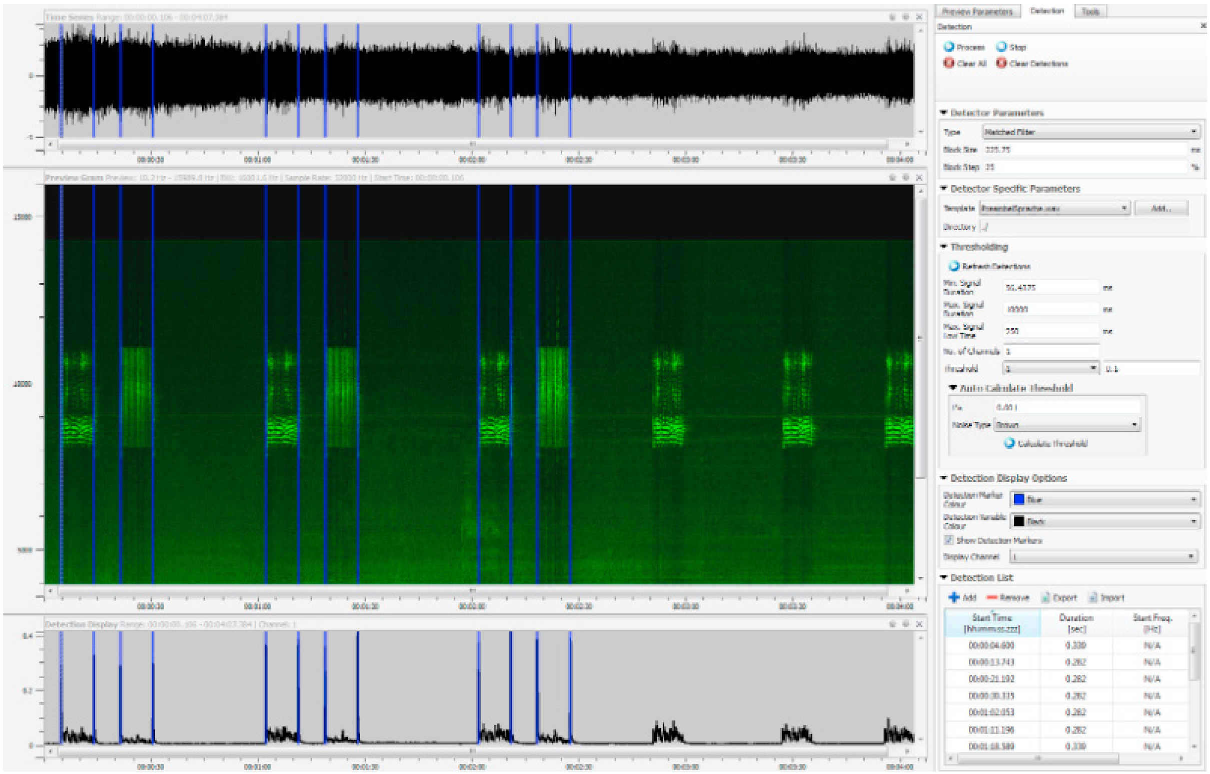
1. Encryption: Data from higher layers (including Link layer) is encrypted according to its payload size. "Short" packets are encrypted using a substitution table, with block mixing achieved with by combining the lightweight SipHash with the substitution table in an unbalanced Feistel network [22]. "Long" packets use "wrapped" AES [23]. Wrapping and block mixing both ensure that a change to any plaintext in any block affects all blocks in the packet (not just subsequent blocks, as is the case in traditional block cipher modes of operation), making any semantic cryptanalysis more difficult to accomplish.
2. Inner Modulation: The bitstream is organised into symbols, which are mapped to chips derived from rows of a Hadamard matrix. This mapping is obscured by the key.
3. Outer Spreading: The chips are spread using a non-linear combination of Linear-Feedback Shift Registers (LFSRs), which improves packet detection performance by decorrelating the packet with multipath components of itself. These codes are derived from the key and have optimal correlation properties; meaning Phorcys is easy to detect in noisy environments for someone who knows the key, and difficult to detect for everyone else because the packet looks like noise.

A further element of scalability, Phorcys inherits the concept of an epoch from Venilia. In Phorcys, the epoch changes how frequently spreading codes, mappings and encryption keys change, resetting any cryptographic knowledge determined by an eavesdropper; determining a spreading code in one epoch does not support any crypto-attack in the next. Phorcys uses derivations of the pre-shared key rather than the key itself, so this key does not need to change each epoch. This does not imply a tight time-synchronisation between two devices; epochs can be of order minutes, hours, days or even longer and the time-synchronisation requirements scale linearly in roughly equal order of magnitude.

Phorcys supports networks of up to 128 addresses with specific protocols in development for mesh and linear network topologies. Short and long packets have both been successfully received from in-service platforms with further trials planned.

6. Hybrid Underwater Acoustic Communication

It has been known since 1935 that human voice can be transmitted underwater. Nowadays, every NATO submarine must be equipped with an analogue underwater telephone (UT). Yet, this communication is openly audible and hence not secure. Mostly depending on the human decoder, this fault-tolerant communication is an alternative to digital communication using chat or short message service in very bad sonar environments. With the voice of the person, additional metadata is transmitted. Work package 5 of IST-174 deals with the combination of voice with a digital pre- and a postamble, similar to the NASA quindar tones (Fig. 5).



Type: Matched Filter
Block Size: 225.75 ms
Block Step: 25 %
Template: PreambelSprache.wav
Directory: ../
Min. Signal Duration: 56.4375 ms
Max. Signal Duration: 10000 ms
Max. Signal Low Time: 250 ms
No. of Channels: 1
Threshold: 1 0.1
Pfa: 0.001
Noise Type: Brown
Detection Marker Colour: 🟦 Blue
Detection Variable Colour: ■ Black
☑ Show Detection Markers
Display Channel: 1

Start Time [hh:mm:ss.zzz]	Duration [sec]	Start Freq. [Hz]
00:00:04.600	0.339	N/A
00:00:13.743	0.282	N/A
00:00:21.102	0.282	N/A
00:00:30.115	0.282	N/A
00:01:02.053	0.282	N/A
00:01:11.196	0.282	N/A
00:01:18.589	0.339	N/A

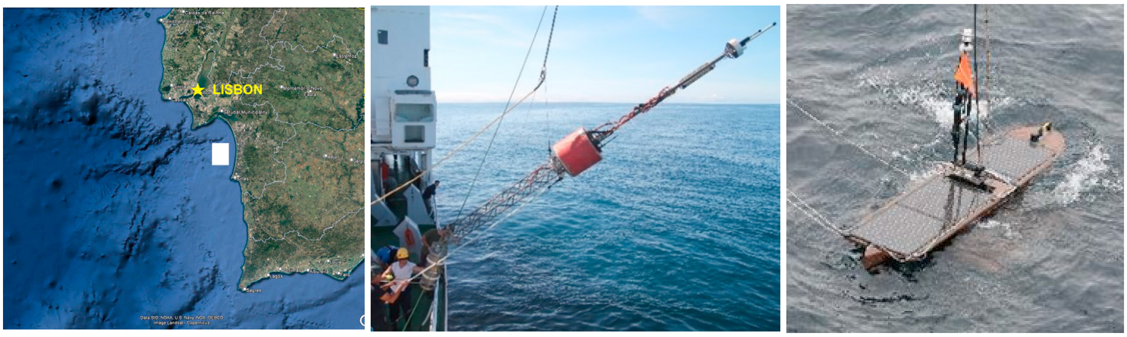
Fig. 5: Six openly audible and three scrambled underwater voice transmission received in a fjord environment in 2016, with and without digital labels for automatic processing inside the UT [24].

With these optional digital labels, the standard underwater telephone is able to recognize messages automatically (like an answering machine), to decode the content, en-/decrypt of open/scrambled voice or can help with speech enhancement. There are various forms of old-fashioned voice scrambling which offer various levels of security; all of them need a defined start- and end-trigger of the voice transmission. If this point is omitted, analogue voice encryption techniques normally do not require more bandwidth than unencrypted speech. This analogue encryption therefore has a strategic advantage over digital crypto solutions underwater. The start-trigger signal is a 48-bit MFSK label with a length of one second. This signal duration results in no intersymbol interference, and hence, it is easy to demodulate. Label flag, application type, operative 6-bit address and a 34-bit application payload, similar to the JANUS bit allocation table, are forming the digital message before and after the voice transmission. As an alternative, the pre- and post-amble could contain the Venilia encryption solution for the scramble initial vector (IV).

Since interoperability in NATO nations is important, this work could be an optional extension for the STANAG 1475 (Material Interoperability Requirements for Submarine Escape and Rescue). Although the standard UT can ignore these digital labels, a next-generation UT equipped with hybrid communications could use the new functionality. For this reason, the patent DE102016009279A1 will be suspended for all NATO productions of UTs and modems to foster hybrid interoperability.

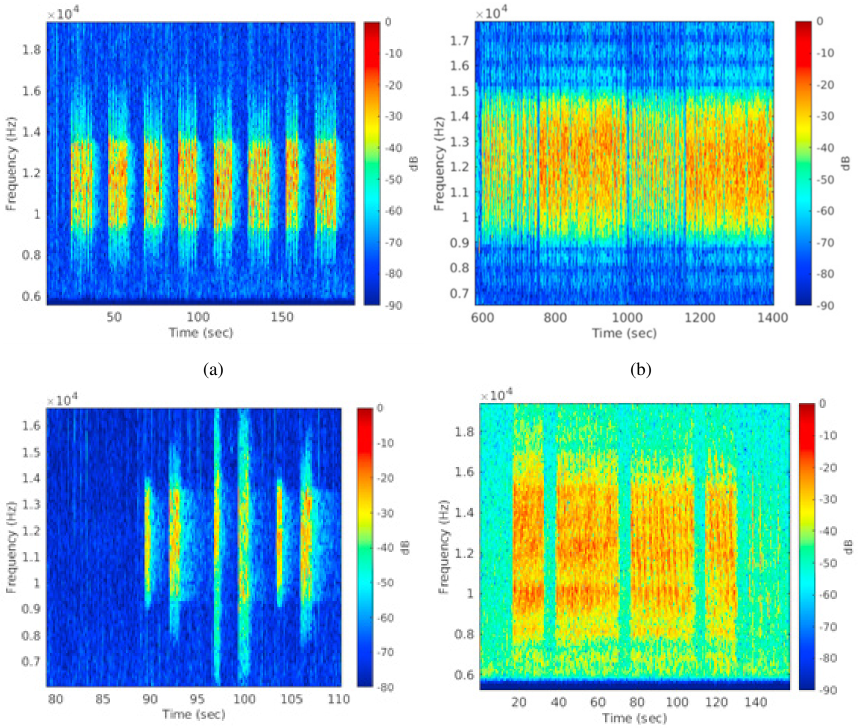
7. Experimental activities

The RTG leveraged on the Robotics Experimentation and Prototyping - Maritime Unmanned System 2021 (REP-MUS-21) sea trial to acquire a rich acoustic dataset for the purposes of the IST-174 study group. The REP-MUS-21 was held in September 2021 in the Atlantic Ocean off the coast of Portugal, close to Sesimbra. The trial was co-organized by CMRE, the University of Porto and the Portuguese Navy. The objective of the sea trial was to foster the collaboration of government, academia and industry to develop and test novel hardware and software



(a) (b) (c)

Fig. 6: (a) REP-MUS-21 area of operations; (b) Gateway buoy; (c) Wave Glider SV3.



(a) (b) (c) (d)

Fig. 7: Spectrograms of various received signals during REP-MUS-21 sea trial. In all plots the colormap is in dB scale. (a) Venilia signals; (b) Phorcys signals; (c) JANUS and BPSK signals; (d) Linear frequency sweep signals.

solutions for the employment of unmanned systems (air, surface and sub-surface) in maritime operations. The white box (of about 64 km^2) in Fig. 6(a) shows the area of operations. The water column depth of the area ranged between 100 m and 150 m. Six days, i.e., September 12th, 14th, 16th, 24th, 25th and 26th were dedicated, among many other activities, to transmitting/recording acoustic signals for the IST-174 study group. The communication nodes were two surface gateway buoys (Fig. 6(c)) with transmit/receive capability and a Wave Glider (Fig. 6(d)) with receive capability. The gateway buoys were deployed about 1 km apart and they were drifting around their mooring positions. One buoy had the acoustic sensors at about 78 m of depth while the second one had the sensors at about 74 m of depth. The Wave Glider could propel itself and its hydrophone was submerged at 34 m depth. The topology of the three-node network was time-varying and from GPS logs it was found that the maximum achieved range and speed was 3 km and 0.57 m/s, respectively. The operational band was approximately 8-15 kHz.

The following figures show excerpts of the received waveforms. Fig. 7(a) shows eight Venilia-type of signals. The collected data will be used to test the Venilia receiver and perform TUBcipher cryptanalysis and spoofing attacks. Fig. 7(b) shows a suite of Phorcys signals with different bit rates and message sizes. The collected dataset will be used to quantify the trade-off of receiver complexity vs. message detection probability vs. low-probability of intercept (LPI) communications. Fig. 7(c) shows JANUS and BPSK modulated channel probes that are received on the Wave Glider. In this scenario, the Wave Glider played the role of Eve while the two buoys acted as Alice and Bob (their recordings are not shown for brevity). The collected dataset will be used to validate the PLS crypto-key generation concept. Fig. 7(d) shows a suite of linear frequency sweep signals. These signals will be used for acoustic channel characterization in terms of multipath and Doppler spread.

Another experimental activity conducted at REP-MUS-21 was the usage of AES-GCM to encrypt JANUS cargo data. Two different configurations were explored, one where the same payload was transmitted over time and another one varying the payload, considering also different message sizes (up to 60 Bytes). The collected data will be used to address the capability of the attacker to extract useful information from the encrypted messages.

8. Conclusion and Future Work

This paper described the different research activities currently undertaken within the IST-174 RTG. Using the collected dataset from the REP-MUS-21 sea trial, the group will investigate: cryptanalysis of TUBCipher and AES-GCM when applied in the underwater domain; assessment of PLS in term of key generation efficiency and security attacks; receiver performance of Phorcys signals. We expect our findings from the analysis of this comprehensive dataset to foster standardization of various security aspects of underwater acoustic communications.

Acknowledgment

The authors would like to thank the Portuguese Navy and Captains and crews of the NRV Alliance and RV PLANET for the excellent support during the REP-MUS-21 sea trial. The authors are indebted to Stephane Blouin (DRDC), Roald Otnes (FFI), Henry Dol (TNO), partners of IST-174, for reviewing this paper and providing useful comments.

References

[1] J. Heidemann, M. Stojanovic, and M. Zorzi, “Underwater sensor networks: applications, advances and challenges.” *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, vol. 370, no. 1958, pp. 158–75, 2012.

[2] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, “Toward the Development of Secure Underwater Acoustic Networks,” *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[3] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, “Jamming-Resistant Multi-path Routing for Reliable Intruder Detection in Underwater Networks,” in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*, ser. WUWNet’11, Seattle, Washington, USA, December 1–2 2011.

[4] A. Signori, F. Chiariotti, F. Campagnaro, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, “A geometry-based game theoretical model of blind and reactive underwater jamming,” *IEEE Transactions on Wireless Communications*, 2021.

[5] E. Souza, H. Wong, I. Cunha, A. Loureiro, L. Vieira, and L. Oliveira, “End-to-end authentication in under-water sensor networks,” in *Proceedings of the 18th IEEE International Symposium on Computers and Communications*, ser. ISCC’13, Split, Croazia, July 7–10 2013, pp. 299–304.

[6] M. Zuba, M. Fagan, Z. Shi, and J.-H. Cui, “A Resilient Pressure Routing Scheme for Underwater Acoustic Networks,” in *Proceedings of the 57th IEEE Global Communications Conference*, ser. GLOBECOM’14, Austin, TX, USA, December 8–12 2014.

[7] F. Campagnaro, D. Tronchin, A. Signori, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, “Replay-attack countermeasures for underwater acoustic networks,” in *Global Oceans 2020: Singapore – U.S. Gulf Coast*, 2020, pp. 1–9.

[8] J. Alves, T. Furfaro, K. LePage, A. Munafò, K. Pelekanakis, R. Petroccia, and G. Zappa, “Moving janus forward: A look into the future of underwater communications interoperability,” in *OCEANS 2016 MTS/IEEE Monterey*, 2016, pp. 1–6.

[9] “Janus wiki.” [Online]. Available: http://www.januswiki.org

[10] R. Petroccia, J. Alves, and G. Zappa, “JANUS-Based Services for Operationally Relevant Underwater Applications,” *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 994–1006, 2017.

[11] National Institute of Standards and Technology, “Advanced encryption standard (aes),” U.S. Department of Commerce, Washington, D.C., Tech. Rep. Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002, 2001.

[12] D. J. Bernstein, *ChaCha, a variant of Salsa20*, ser. Lecture Notes in Computer Science. Germany: Springer, 2008, pp. 84–97.

[13] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security framework for underwater acoustic sensor networks," in *Proceedings of the IEEE/MTS OCEANS 2015 Conference*, Genova, Italy, May 18–21 2015, pp. 1–9.

[14] M. J. Dworkin, "NIST SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," National Institute of Standards and Technology, Gaithersburg, MD, United States, Tech. Rep., 2007.

[15] A.-M. Hobbs and S. Holdcroft, *JANUS Class 17 "Venilia": Secure Pre-Canned Messaging*, Defence Science & Technology Laboratory, Fareham, Hampshire, Jun. 2021.

[16] International Telecommunications Union, *G.704: Synchronous Frame Structures used at 1544, 6312, 2048, 8448 and 44,736 kbit/s Hierarchical Levels*, Oct. 1998.

[17] A.-M. Hobbs and S. Holdcroft, *Tiny Underwater Block cipher (TUBcipher): 27-bit Encryption Scheme for JANUS Class 17*, Defence Science & Technology Laboratory, Fareham, Hampshire, Jun. 2021.

[18] L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw, "PRINTcipher: A Block Cipher for IC-Printing," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, S. Mangard and F.-X. Standaert, Eds., vol. 6225, 01 2010, pp. 16–32.

[19] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[20] K. Pelekanakis, S. A. Yildirim, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical Layer Security against an Informed Eavesdropper in Underwater Acoustic Channels: Feature Extraction and Quantization," in *Proceedings of the 5th IEEE OES International Conference on Underwater Communications and Networking*, ser. UComms20, 2021, pp. 1–5.

[21] G. Sklivanitis, K. Pelekanakis, S. A. Yildirim, R. Petroccia, J. Alves, and D. Pados, "Physical Layer Security against an Informed Eavesdropper in Underwater Acoustic Channels: Reconciliation and Privacy Amplification," in *Proceedings of the 5th IEEE OES International Conference on Underwater Communications and Networking*, ser. UComms20, 2021, pp. 1–5.

[22] J.-P. Aumasson and D. J. Bernstein, "SipHash: A Fast Short-Input PRF," in *Progress in Cryptology - INDOCRYPT 2012*, S. Galbraith and M. Nandi, Eds. Springer Berlin, Heidelberg, 2012, pp. 489–508.

[23] M. J. Dworkin, *Recommendation for Block Cipher Modes of Operation:Methods for Key Wrapping (SP 800-38F)*, National Institute of Standards and Technology, Dec. 2012.

[24] I. Nissen and E. Kuhnt-Matthé, "Verbesserung der sprachverständlichkeit bei analoger unterwasserkommunikation durch nutzung von digitalen anfangs- und endmarken," *DAGA*, vol. 2017, no. 223, pp. 161–163, 2017.