Location-Based Symmetric Key Management

Bálint Z. Téglásy[1], Colin Boyd[2], John R. Potter[3], and Sokratis Katsikas[4]

[1]NTNU Department of Engineering Cybernetics, 7491 Trondheim, Norway
[2]NTNU Department of Information Security and Communication Technology,
O.S. Bragstads plass 2a, 7491 Trondheim, Norway
[3]NTNU Department of Electronic Systems, 7491 Trondheim, Norway
[4]NTNU Department of Information Security and Communication Technology,
Mail Box 191, 2815 Gjøvik, Norway

Contact author: Bálint Z. Téglásy Postal address: NTNU Department of Engineering Cybernetics, 7491 Trondheim, Norway. Fax: +47 73 59 45 99 E-mail: teglasybalint@gmail.com

Abstract: *National and international maritime authorities regularly handle requests for licences for many kinds of marine activities. These licences authorise activities, limited in time and space. We have noted secure Automatic Identification System (AIS) solutions suitable for internet-connected assets such as ships with satellite connections. Underwater, where an increased level of commercial activity is developing in addition to preexisting military and environmental monitoring, there is currently no security service interoperable between organisations. The advent of seabed mining, marine robotics and oil and gas value chains moved underwater necessitate security solutions that work across countries and companies. The inadequacy of security services to address emerging issues constitutes a regulatory gap. It is important to bridge this gap from a safety, accountability, and wider security perspective. Radio signals and optical wavelengths travel only short distances through seawater and the bandwidth offered by acoustic communications is much lower. Additional constraints on autonomous underwater assets, such as reduced power, further limit the viable options. We show that these constraints can be accommodated by using symmetric cryptography. We propose a security service that allows automatic checking of asset authorisation status based on large symmetric keys. Key generation can take place at a central authority according to the time and space limitations of a licence, i.e., time-stamped and geocoded. Our solution harnesses a standardised encoding of geocells. Given the geographically correct use of keys, civilian and military, public and private assets can prove their legitimisation to be at a place at a time to each other. While we have developed and described our solution for offshore underwater use, aerial and terrestrial environments could also use it if they are similarly bandwidth constrained or want to rely on quantum-resistant and computationally economic symmetric methods.*

Keywords: *Underwater, Symmetric key, Geocode, Key management*

1. INTRODUCTION

An Exclusive Economic Zone (EEZ) gives countries with sea access exclusive rights to underwater (UW) resources. In Fig. 1, we show the example of Norway. EEZs are further subdivided into production licences, fishing grounds and other geographically constrained rights depending on the economic domain. These rights are getting more valuable due to the proliferation of underwater technologies such as subsea oil and gas installations. Proposed subsea mining of metal deposits arranged in thin, but highly concentrated layers is expected to motivate the exploitation of larger areas. However, checking if these rights are respected has only been possible using above-water checks due to the difficulty of communicating UW. Our solution allows automated checks of resource-constrained UW unmanned assets such as Autonomous Underwater Vehicles (AUVs) as well.

We propose that keys are applied for, generated, distributed and used in protocols as a function of legitimate geographic locations. This can be done by subdividing the planet into geocoded cells (geocells) and generating geosecured keys with the geocode as an additional input.

We provide similar location-based benefits to earlier work of Choi et al. [2], but without assuming base stations, because we hold those unrealistic in an international maritime environment. In addition, the opportunity to authorise several geocells, e.g. those along a route, allows for mobile devices to be secured, which has not been foreseen previously.

2. REQUIREMENTS FOR KEY MANAGEMENT IN UNDERWATER COMMUNICATIONS

The requirements for key management should be driven by realistic assumptions for information available on the participating devices. There are not many variables that UW civilian devices can be trusted to have since they are heavily resource-constrained. Time is a commonly used variable in UW applications for enabling security, and it has been used in Venilia [3] (as an input to epochs), our previous proposal for the authentication of UW assets, and the Phorcys Cryptographic Interoperability Specification [4]. We require the devices to have a maximum drift of three seconds per month. We believe commercial quartz technology delivers this even on the most resource-constrained devices.

In addition to time, we believe it is reasonable to assume that wireless UW devices have some idea of where they are because they would be lost otherwise. Positioning is not as trivial as with the Global Positioning System (GPS) technology readily available for all non-UW mobile devices, but doable with the help of aided inertial navigation systems (INS), where the aid to the inertial gyroscopes typically comes from Kálmán-filtered Doppler Velocity Log bottom trackers and kinetic vehicle models. Larger vehicles are more expensive and warrant the additional expense of higher-quality INS. Therefore we assume an error of 50 meters root mean square per hour for devices that need keys. We can, in addition, assume that points with known coordinates are available at least once a day either at the sea bottom (terrain contour matching) or floating on the surface (buoys with a known location or ships that securely transmit their location). Therefore, we require the positioning error of every participating device to have an upper limit of 1000 meters with a high probability.

In addition to the above, we require that an inter-operable challenge-response authentication indicates compliance within ten seconds over a distance of 10 km. From this requirement, it

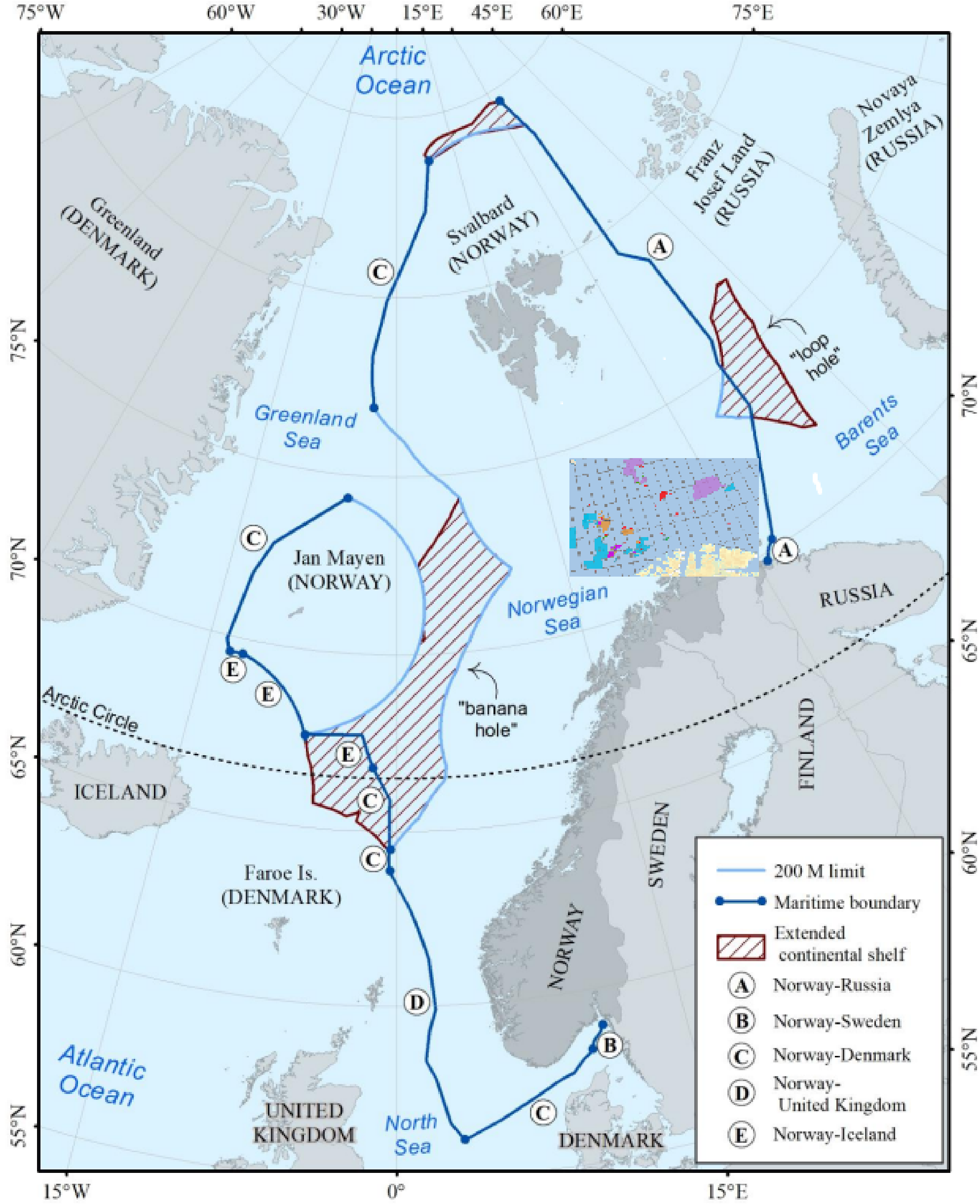

Figure 1: The internationally accepted boundaries of Norway's EEZ. Source: [1]
Coloured insert shows petroleum licences in the Norwegian part of the Barents Sea.

follows that we have to use the only open and therefore inter-operable UW communication standard JANUS, whose bandwidth does not exceed 80 bits per second. Given that it already takes around 7 seconds for sound to travel 10 km in water, the devices have no more time than to encode one JANUS baseline packet each. Such a packet is constrained in bandwidth to 34 bits of payload per second.

3. DRAWBACKS OF COMMON SOLUTIONS

Due to the fundamental importance of key management in cryptographic security, different solutions are common on the internet and in enterprise settings. However, these same solutions cannot be applied under the constraints UW. This section briefly summarises existing schemes and their limitations in our scenario.

3.1. PUBLIC KEY ALGORITHMS

Public key cryptography usually requires a Public-Key Infrastructure (PKI) to ensure integrity of public keys. The requirements for a scalable PKI are not to be underestimated, and there is no ready-made solution for PKIs of IoT devices that lack an internet connection. However, we concede that PKI for IoT is possible, for example by harnessing identity-based cryptography [5]. There remain fundamental drawbacks that make all flavours of public keys less suitable for any IoT UW:

1. A public key ciphertext or ephemeral key needs to be exchanged for any two devices A and B that are seeking to establish a secure connection. These values are typically large (at least 2048 bits), and are always larger than a sufficiently large nonce encrypted with a pre-shared symmetric key (PSK), where 32 bits possible. This is an issue where bandwidth is restricted.

2. Public-key algorithms are significantly more computationally complex than symmetric ones. This is an issue in the heavily energy-constrained wireless UW environment.

3. Today’s commonly-used public-key algorithms are typically insecure in a post-quantum world, especially in cases where nation-state-backed threats are to be considered. Those public-key methods that are quantum resistant are complex to the extent that flaws have sometimes been found in them after rigorous expert review.

3.2. KERBEROS-STYLE CLIENT-SERVER ARCHITECTURES

Client-server models are unfeasible UW because, in addition to any devices A and B that are instantaneously seeking to establish trust with each other, there is unlikely to be a simultaneous connection with a trusted third party S (for server). This can change if a large network of base stations can be installed. While there are proposals in academic literature to do so, the costs for installing millions of such base stations to serve a sparsely populated UW IoT are prohibitive, and will likely stay that way for decades to come.

3.3. PSK FOR ENTIRE NETWORKS

We believe that underwater cybersecurity systems, if used at all, currently rely on PSK [6, 3, 7, 4] . The PSK binds devices to one packet-switched network, where every device is a potential opportunity for adversaries to retrieve the secret key valid for the entirety of that network. Gateways connecting two or more networks are feasible, but those then become points of vulnerability for both networks since they carry the keys for all networks they want to route packets between. This poses a scalability issue. Depending on the strength of anti-tampering and other countermeasures, large-scale UW networks become indefensible. A key shared between hundreds of devices distributed in a large area, where constant surveillance or immediate intervention is impossible, represents an extreme risk. As we will see, our proposal geographically segments networks to a point where having more than a few 10s of devices within one of the millions of network segments (corresponding to geocells) is unlikely.

4. DEFINITION OF A PROPOSED LOCATION-BASED SOLUTION

In this section, we present our proposed key management technique. We avoid public key cryptography, online servers and network-wide keys for reasons explored above. We need to use PSK but on a restricted basis. The complexity of key management increases exponentially with the increasing network size [2]. The difficulty comes from the increased chance of key ring compromise in larger networks [8]. If all devices are to communicate with each other in a network, they have to have each other's PSK. If a device holds several keys to participate in several networks, it has a key ring. An attacker can access a key ring by capturing a device, and all networks whose key has been on the ring will be compromised. It is therefore important to provide resilience to the loss of key rings. PSK are derived from geocells of the Open Location Code (OLC) system. Six characters encode a quadratic cell with a side length of approx. 5,5 km, which is deemed to be in good agreement with the range of UW digital acoustic communication.

4.1. ENTITIES

Two kinds of entities are necessary for our solution: (1) Maritime authorities generating keys for their jurisdiction, and (2) Maritime devices (with onboard information on time and location, as well as acoustic modems). The maritime authorities can be international authorities distributing keys to national authorities, or national authorities generating keys directly for their EEZ. A third kind of entity is not required per definition but is likely to be a middleman between the authority and the devices. This would be the operating organization of the maritime assets, requesting keys from the authority and distributing them to the devices.

The maritime authority generates keys according to the inputs shown in Fig. 2. Note that inputs to and outputs from the centralised key generation process are protected by data diodes in order to safeguard the master key. Also in Fig. 2, the blue colour could represent the maritime devices, or a trustworthy (ensured e.g. by Transport Layer Security, TLS) operating organization acting on their behalf while they are UW.

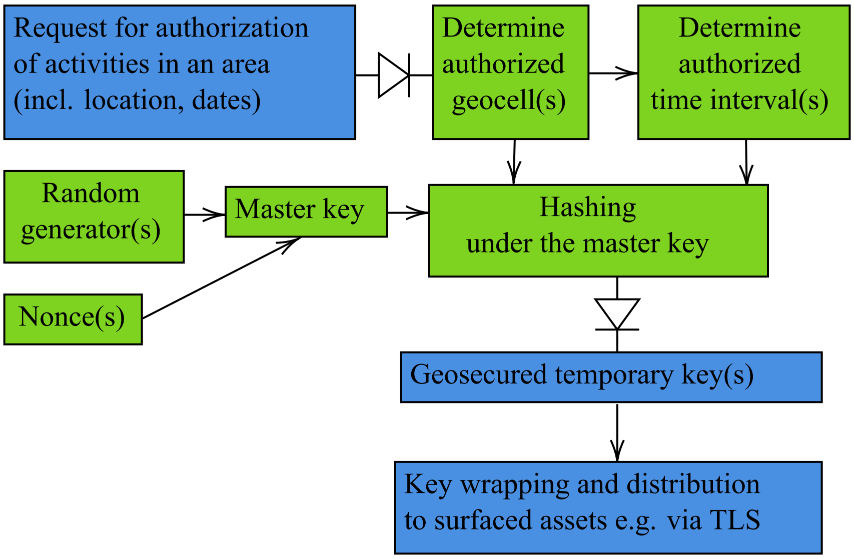
Request for authorization of activities in an area (incl. location, dates)
Determine authorized geocell(s)
Determine authorized time interval(s)
Random generator(s)
Master key
Hashing under the master key
Nonce(s)
Geosecured temporary key(s)
Key wrapping and distribution to surfaced assets e.g. via TLS

Figure 2: Internal processes of the maritime authority (green) and the maritime devices or their operating organization (blue).

4.2. KEY DERIVATION AND DISTRIBUTION

In the notation used by the relevant standard [9], the inputs and outputs of Fig. 2 are as follows:

- The master key is the key-derivation key input
- A Keccak-based message authentication code (KMAC) should be the pseudorandom function for hashing under the master key. This is to accommodate large inputs and outputs, including the keys contributing to security.
- Geocell and time interval should be used as context inputs specified by the standard
- Geocoded keys valid for a time interval will be the output.

Key distribution has to happen with the involvement of surface vessels - we hold this to be evident due to the short range and low speed of interoperable UW communication and the sparse population of UW assets. Satellite communication and public key infrastructure to ensure secure the distribution of data, including keys, should only be assumed for surfaced vessels. Compliance can be checked with the present proposal.

5. SAMPLE APPLICATION IN A PROTOCOL FOR IDENTIFICATION OF FRIEND OR FOE

Once distributed, the keys can be used by devices UW without the involvement of an authority. They can be applied in a protocol for two-pass mutual authentication as per ISO/IEC 9798-2:2019, part 2. Departures from the standardised protocol might be needed to fit the ciphertext into one JANUS baseline package. A method is illustrated in Fig. 3, where an AUV and a subsea valve assembly typical for oil and gas production are depicted as communication partners. A subsea valve assembly is shown challenging an AUV to prove its authorisation.

Key K_1 is a geosecured temporary key (see Fig. 2) that the devices choose from their key ring based on their location. After a valid response, both devices can derive a bilateral session key from the decrypted payloads, such as time stamps T_A and T_B, and clock descriptors CD_A and CD_B. This is desirable to make sessions independent of each other. This method was verified to be practical with acoustic modems.

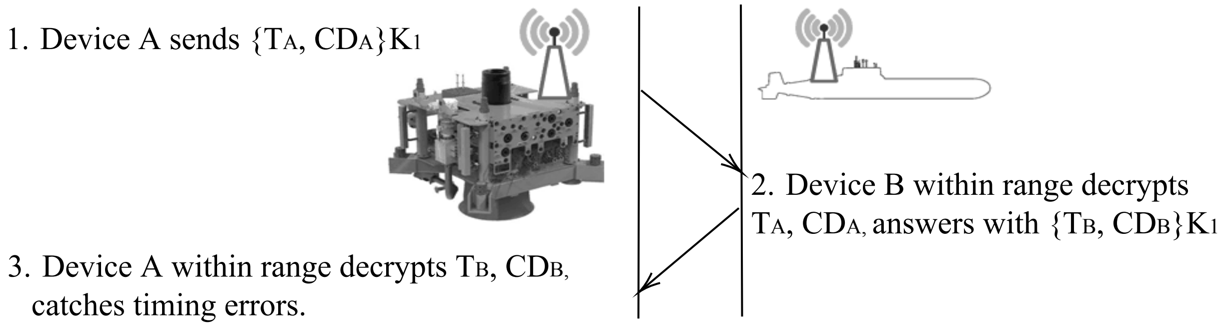
1. Device A sends {TA, CDA}K1
2. Device B within range decrypts TA, CDA, answers with {TB, CDB}K1
3. Device A within range decrypts TB, CDB, catches timing errors.

Figure 3: Illustration of a protocol using the geosecured temporary keys.

6. INFORMAL SECURITY ANALYSIS

Geocoded keys introduce resilience to PSK-secured networks. These are shown in Table 1, where we compare our solution with traditional, pseudorandom only key assignment.

Attributes	**Pseudorandom only**	**Location-based**
Number of keys assigned	One per organization (applicable worldwide)	One per geocode (across organizations)
What is to be proven with key possession	Devices belong to the same organization, where the claimed organization has to be assumed. This assumption can be strengthened through associated cleartext communication or physical layer security, but the false-to-true negatives and positives ratio is unlikely to reach levels considered secure if the system is to service more than one organization in a geographic area.	The responding device is authorised to be in its current location by the same authority as the challenging device.
Key compromise consequence	A compromised key means that the whole organization using that key has lost confidentiality and integrity until surfaced (Transport Layer Security-mediated) key renewal takes place.	Adversarial devices gain false authorisation to geocode(s) in the key ring until renewal.

Table 1: Comparison of security attributes of symmetric key generation methods.

7. THE EFFICIENCY OF STORAGE AND COMPUTATION

Computation efficiency is high due to the exclusive usage of symmetric methods once the keys are on the constrained devices. The generation of those keys by the authorities is relatively efficient due to the modern KMAC hashing methods.

Storing all geocoded keys worldwide is possible in less than 7 gigabytes of data. This feature allows federated management of any arbitrary geographic subdivision (as a collection of geocodes) without revealing the master key. Withholding the master key enables delegating the management of any collection of geocodes to another, e.g. national entity, without the danger that this national entity would fabricate keys for geocodes belonging to other entities.

8. CONCLUSION

We have presented a symmetric key management system based on locations that enables unprecedented resilience to compromised keys. Such a system would be especially useful for unmanned assets with restricted communication such as those encountered UW.

9. ACKNOWLEDGEMENTS

Boyd and Potter are supported by the Research Council of Norway, under Project No. 288545 and 309960 respectively.

REFERENCES

[1] U.S. Dept. of State Bureau of Oceans and Intl. Environmental and Scientific Affairs, "Limits in the seas no. 148: Norway maritime claims and boundaries," accessed 30/8/2022.

[2] J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, "Location-based key management strong against insider threats in wireless sensor networks," *IEEE systems journal*, vol. 11, no. 2, pp. 494–502, 2017.

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

[4] A.-M. Hobbs, J. Barnett, and A. Hamilton, "PCIS - a novel approach to security in the UW domain," in *UComms 2022 Conference*, pp. 1–4, IEEE, 2022.

[5] A. Goudosis and S. Katsikas, "Secure ais with identity-based authentication and encryption," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 14, no. 2, 2020.

[6] F.-X. Socheleau and S. Houcke, "Hiding cyclostationarity with dispersive filters for covert underwater acoustic communications," in *UComms 2022 Conference*, pp. 1–5, 2022.

[7] B. Z. Téglásy, E. Wengle, J. Potter, and S. Katsikas, "Authentication of Underwater Assets," *arXiv*, pp. 1–27, 2020.

[8] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key predistribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 948–959, 2013.

[9] L. Chen *et al.*, *Recommendation for key derivation using pseudorandom functions*. US Department of Commerce, National Institute of Standards and Technology, 2008.