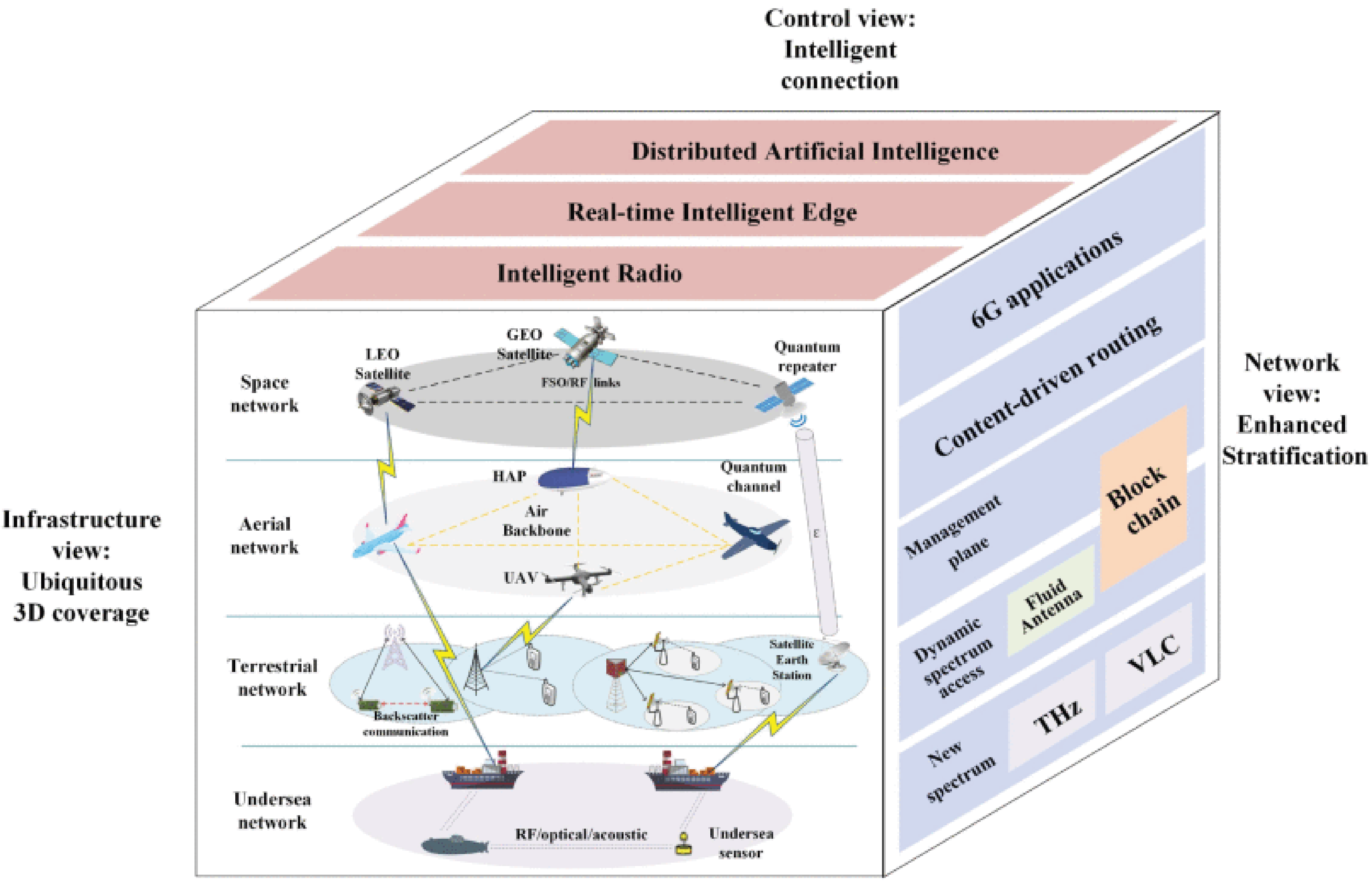
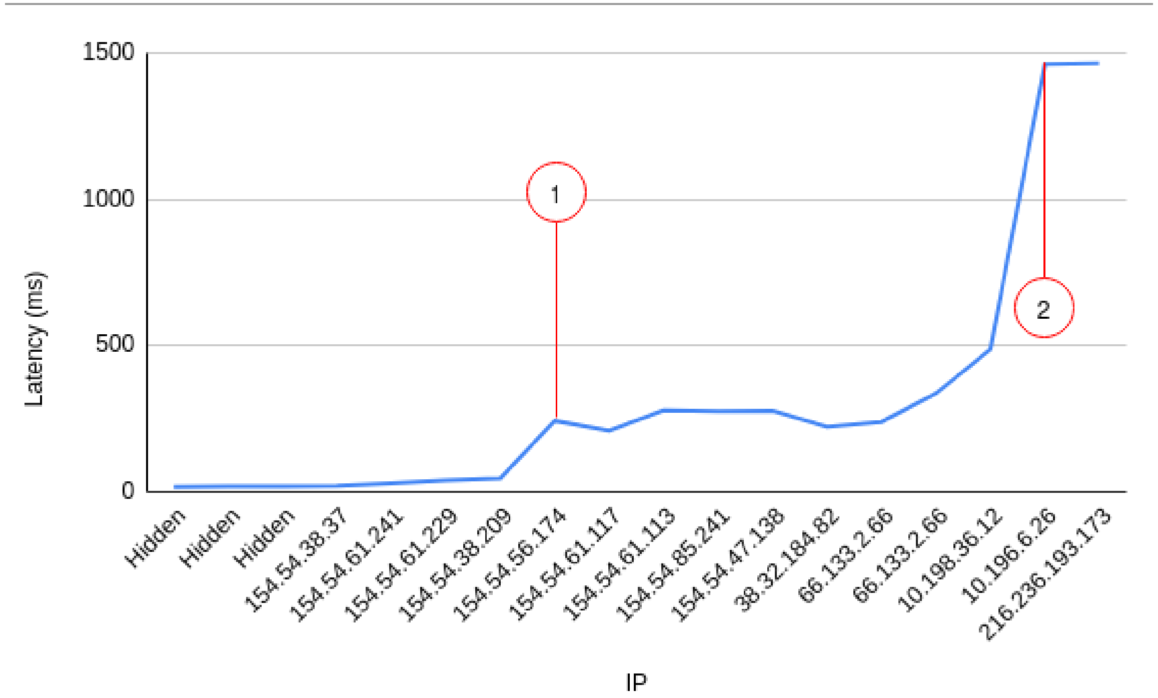
Underwater cybersecurity

Vision: 6G wireless (Huang et al.)



Can maritime assets be found?

- No way to know unless a central authority says which assets are maritime
- Traceroute hops can be an indication
- This could be done linked to the MMSI (by International Telecommunication Union)



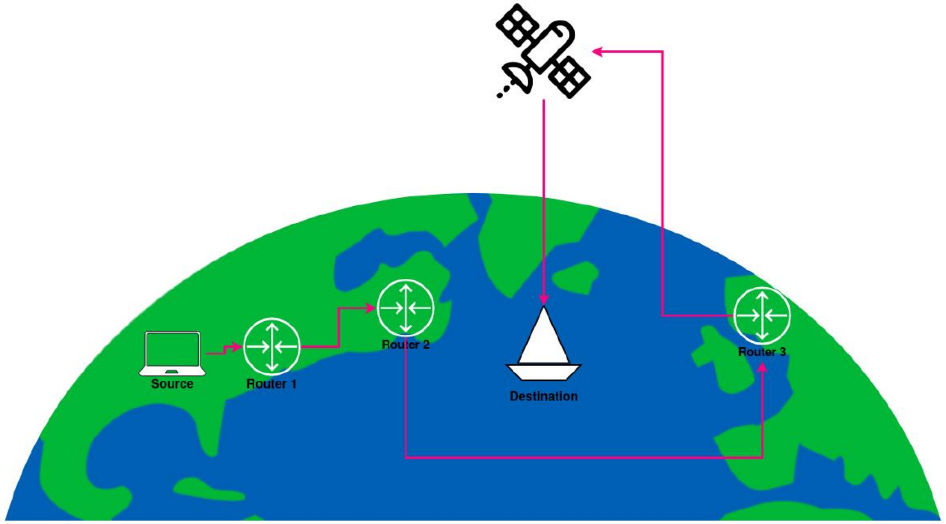


Figure 5: Visualization of internet latency. Map from http://getdrawings.com/earth-cartoon-drawing

What is authentication? Why do we need it?

1. Authentication = shorthand for ***proof of identity***.
2. Without proven identities, there can be no talk of security, especially at sea (ref. below)
3. Without getting into (too specific, often proprietary) technology, there are three ways of proving identity (*who*):
   1. Something You *Know* (information) <- *this is what puts the cyber to the security!*
   2. Something You *Have* (house/car key, *employee card, USB dongle*)
   3. Something You *Are* (visual, biometrics, photonic radars, Physically Unclonable Functions)

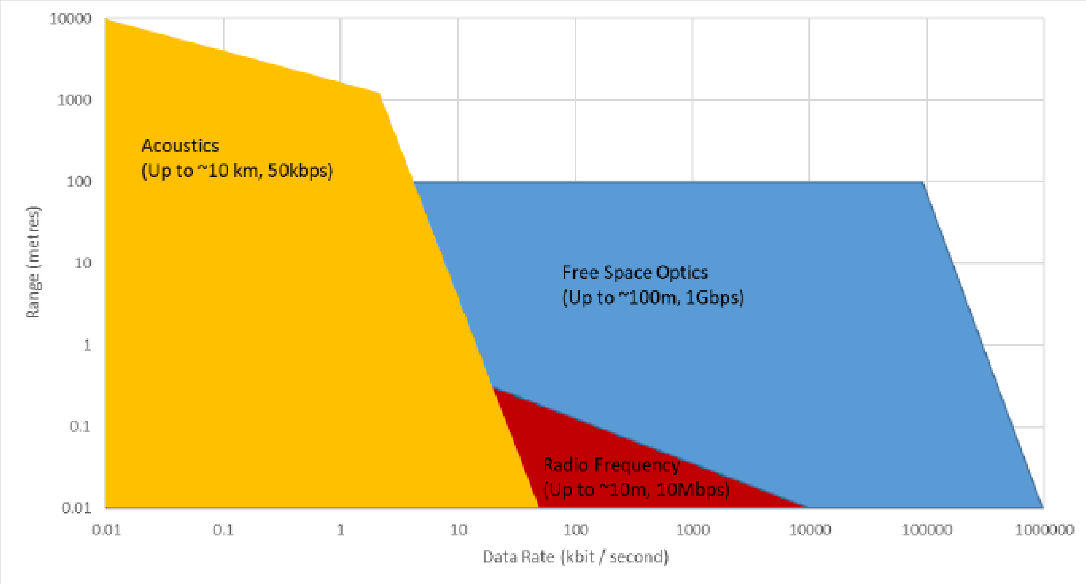
2. ^ Christopher Hodapp; Alice Von Kannon (4 February 2011). *Conspiracy Theories and Secret Societies For Dummies*. John Wiley & Sons. pp. 137–. ISBN 978-1-118-05202-0.
3. ^ Politakis (24 October 2018). *Modern Aspects Of The Laws Of Naval Warfare And Maritime Neutrality*. Taylor & Francis. pp. 281–. ISBN 978-1-136-88577-8.
4. ^ Faye Kert (30 September 2015). *Privateering: Patriots and Profits in the War of 1812*. JHU Press. pp. 62–. ISBN 978-1-4214-1747-9.
5. ^ Donald R. Hickey; Connie D. Clark (8 October 2015). *The Routledge Handbook of the War of 1812*. Routledge. pp. 64–. ISBN 978-1-317-70198-9.

Functional Specification of an IFF/Authentication: What do we need?

1. We need something that fits our
   a) Operational needs (=> fast, reliable => lightweight)
   b) Threat assumptions (the false positive/negative rates will be influenced by them, balance with safety/availability goals needs to be struck)
   c) Need for future flexibility => keyed system
2. Something that, based on the above, can be standardized/codified
   a) Possibly adaptations of already standardized technologies
      a) Automatic Identification System (AIS) used by Vessel Traffic Services (VTS) for surface ships
      b) Automatic dependent surveillance–broadcast (ADS–B) for aircraft
      c) What does AMOS already have? What/how is YARA Birkeland going to use?
   b) Underwater communication is likely to be challenging => protocol tailored to the signal language/physical layer used (if not tethered). Options proposed:
      a) WiFi-like => strongly limited range (1-5 m?)
      b) Acoustic => ultralight-weight due to bandwidth concerns, will need sonar engineer on board the project
      c) Fancy, e.g. airborne laser through water https://patents.google.com/patent/US5038406A/en

A Standardizable Authentication Method for Wireless Underwater Communication

- Part of a wider collaboration with Equinor/Vidar Hepsø
- Offers a unique advantage in space (close to NTNU marine facilities) and time (standardization effort for underwater comm. ongoing) and organisational environment (related ITK activities)
- New physical layer changes protocol stack when compared to established authentication methods
- Likely involves more practical work for proofs of concept
  - This could be done in the framework of B.Sc. and M.Sc. Projects, theses under my supervision



Like the previous slide, but tabular representation

TABLE I
PHYSICAL LAYERS FOR UNDERWATER COMMUNICATION

Modality	**State-of-the-art**	**Bandwidth**	**Range**
Electromagnetic	2,4 GHz WiFi [9]	11 Mbps	15 cm[a]
Free space optical	NRZ-OOK 520 nm [10]	500 Mbps	100 m
Acoustic	JANUS standard [11]	80 bps	10 km

[a] [9] indicates that packet loss rises above 15 cm.

TABLE II

THE DIGITAL ACOUSTIC COMMUNICATION PROTOCOL STACK TODAY

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

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

The only open standard for underwater comm., digital representation

TABLE III
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 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	Application Data Block (ADB)	34 bits of payload. Our proposal: 29 bit timestamp, 3 bit clock accuracy descriptor, 2 cleartext flags.
57-64	8-bit Checksum	JANUS defined: 8-bit CRC run on the previous 56 bits with $p(x) = x^8 + x^2 + x^1 + 1, init = 0$

<table>
<tr><th>Bit</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th><th>32</th><th>33</th><th>34</th><th>35</th><th>36</th><th>37</th><th>38</th><th>39</th><th>40</th><th>41</th><th>42</th><th>43</th><th>44</th><th>45</th><th>46</th><th>47</th><th>48</th><th>49</th><th>50</th><th>51</th><th>52</th><th>53</th><th>54</th><th>55</th><th>56</th><th>57</th><th>58</th><th>59</th><th>60</th><th>61</th><th>62</th><th>63</th><th>64</th></tr>
<tr><td>Baseline JANUS</td><td colspan="4">Version</td><td colspan="4">Flags</td><td colspan="8">Class user ID</td><td colspan="6">Application Type</td><td colspan="34">Application Data Block</td><td colspan="8">CRC</td></tr>
<tr><td>Auth Challenge</td><td colspan="4">Version</td><td colspan="4">Flags</td><td colspan="8">Class user ID</td><td colspan="6">Application Type</td><td colspan="7">year</td><td colspan="4">month</td><td colspan="5">day</td><td colspan="5">hours</td><td colspan="6">minutes</td><td colspan="5">seconds</td><td colspan="2">spare</td><td colspan="8">CRC</td></tr>
<tr><td>Auth Response</td><td colspan="4">Version</td><td colspan="4">Flags</td><td colspan="8">Class user ID</td><td colspan="6">Application Type</td><td colspan="32">ciphertext</td><td colspan="2">spare</td><td colspan="8">CRC</td></tr>
</table>

About the spare bits at 55 and 56:

- I plan to use the 55th for acknowledgement (ACK in the TCP world)
- The 56th for response request (close to SYN in TCP)
- I plan not to encrypt these

From simplistic to still simple enough: iterations 1 and 2

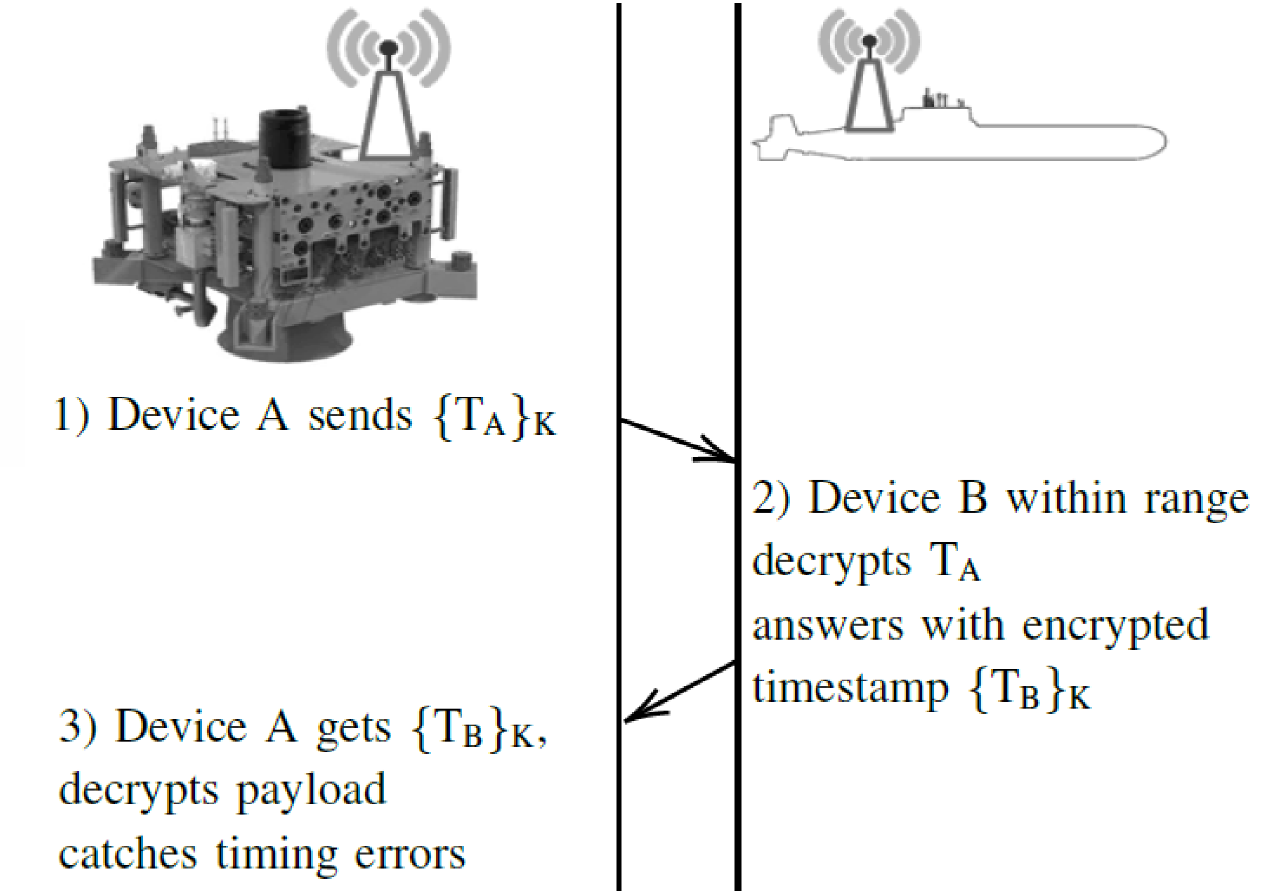


Fig. 1. An illustration of the challenge $\{T_A\}_k$ and response $\{T_B\}_k$.

Key Ingredient: Ultra-lightweight block ciphers

TABLE IV
ENCRYPTION ALGORITHMS WITH BLOCK SIZES ≤ 34 BITS

Cipher	RC5	Skipjack	Speck	Katan32	Hummingbird-2
Cryptanalysis available?	Yes (for 64 bit variant)	Yes (for 64 bit variant)	Yes	Yes	Yes
Minimum block size [bits]	32	32	32	32	16
Maximum key size [bits]	2040	80	64 (for 32 bit variant)	80	128
Needs initialization vector?	No	No	No	No	Yes
Software optimised	Yes	No	Yes	No	No

From simplistic to still simple enough: iteration 3

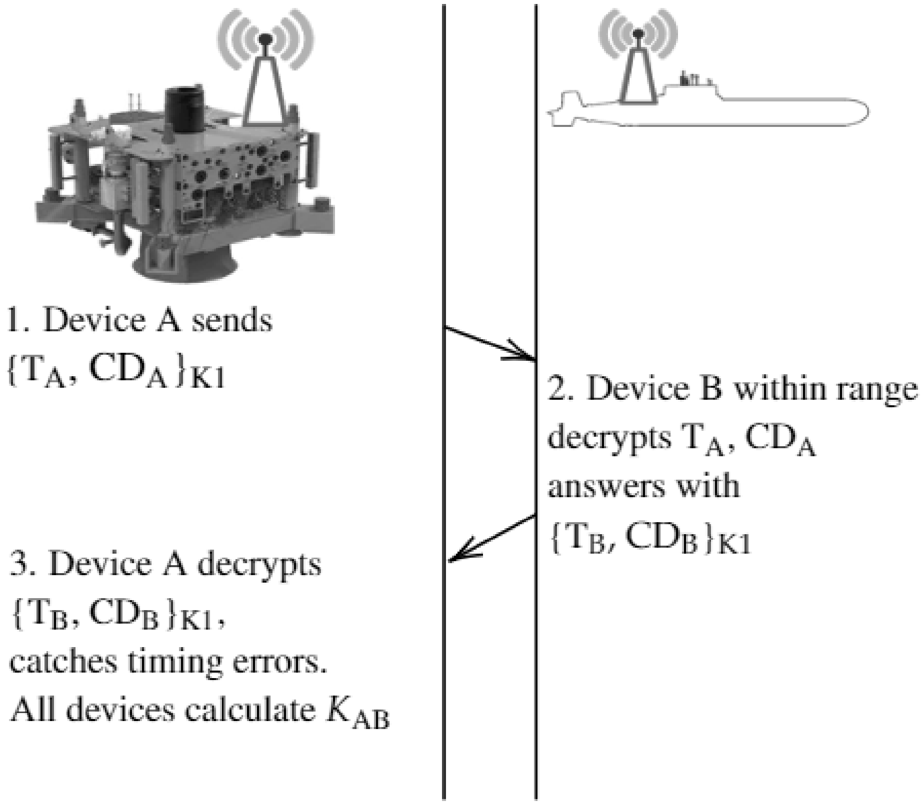


Figure 1. An illustration of the authentication challenge $\{T_A, CD_A\}_{K_1}$ and the response $\{T_B, CD_B\}_{K_1}$.

This is a bilateral (relational) session design. Is this good enough?

From simplistic to still simple enough: the problem with iteration 3

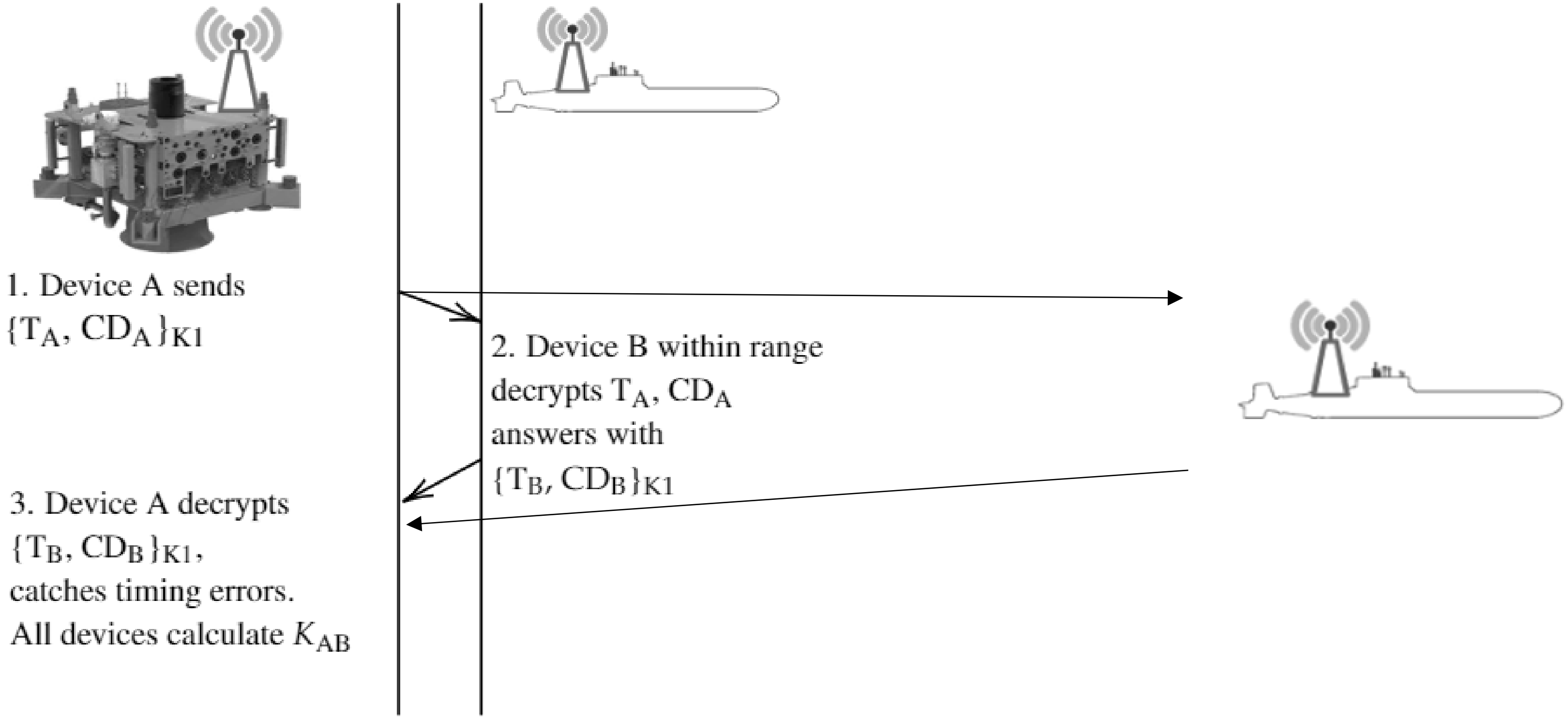
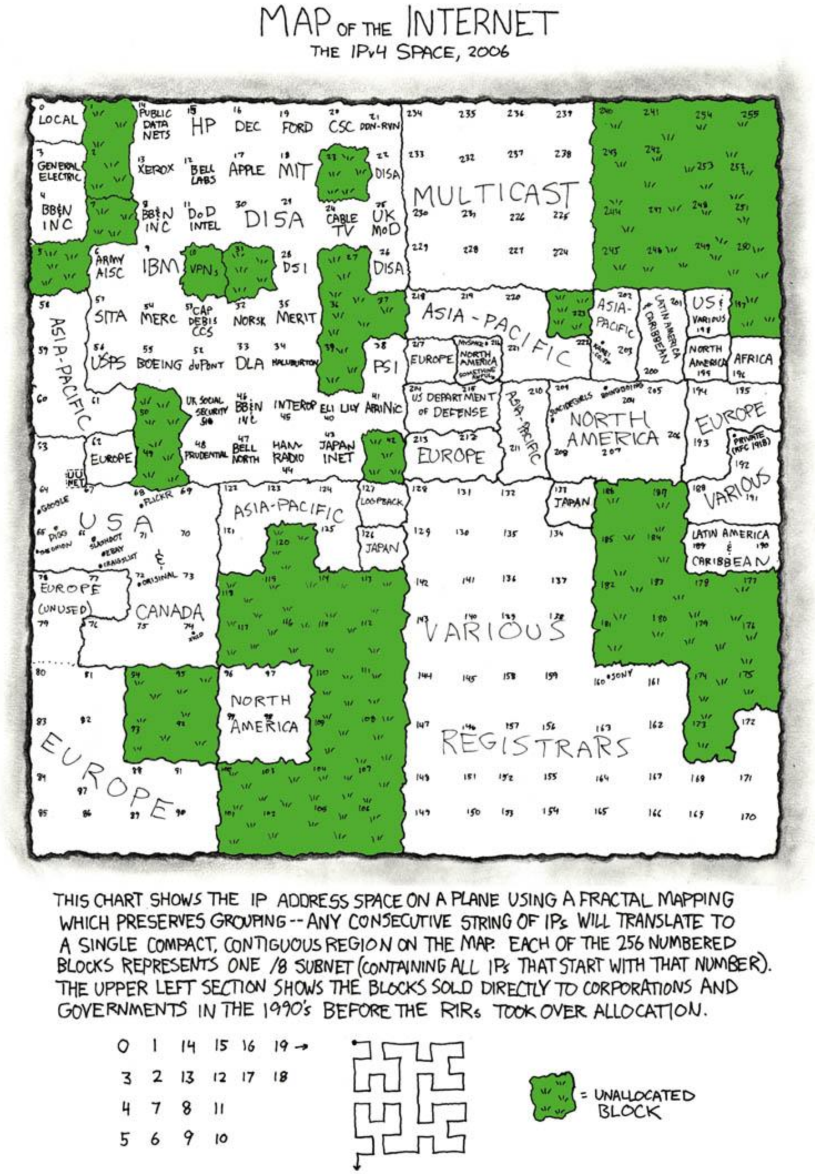


Figure 1. An illustration of the authentication challenge $\{T_A, CD_A\}_{K_1}$ and the response $\{T_B, CD_B\}_{K_1}$.

Device A has no way of knowing if it just calculated K_AB or K_AC! No unique identifier has been communicated.

Options for unique identifiers, no. 1: IP address.



Options for unique identifiers, no. 2: IMO number.

A unique identifier for *certain* ships:
1) typically larger than 12 m
2) At most 1000000 worldwide
Supervised by the International Maritime Organization (IMO)

Options for unique identifiers, no. 3: MMSI.

Maritime Mobile Service Identifier (MMSI)

supervised by the International Telecommunication Union (ITU)

From simplistic to still simple enough: iteration 4 (final?)

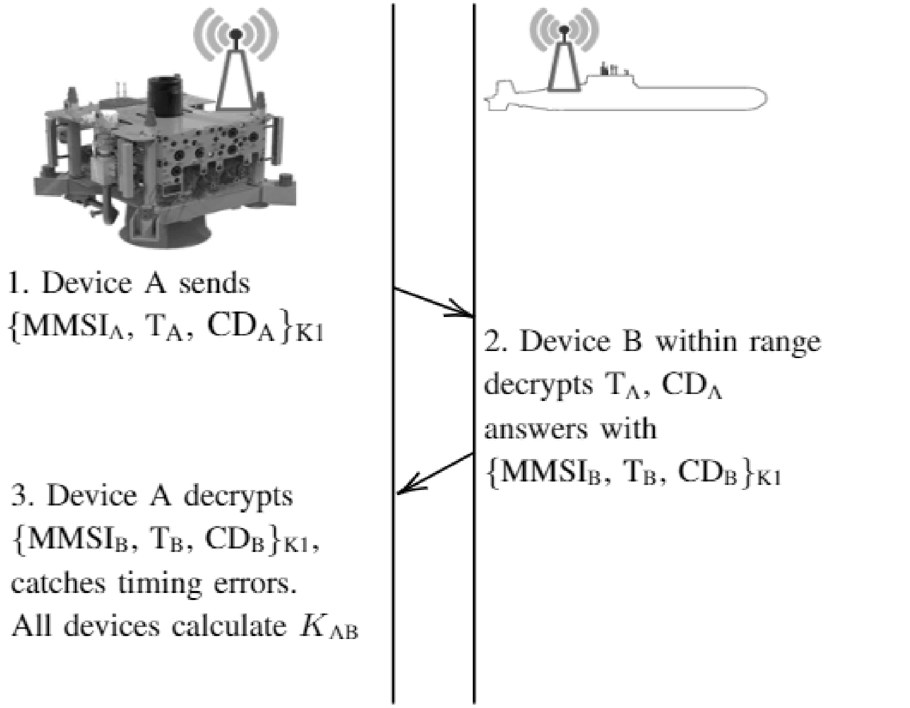


Fig. 2. An illustration of the authentication challenge $\{MMSI_A, T_A, CD_A\}_{K_1}$ and the response $\{MMSI_B, T_B, CD_B\}_{K_1}$.

Devices can collect tables containing info on other devices they've met consisting of:

- Unique ID (MMSI)
- Session key (K_ij)

Determined by HMAC that can be verified as correct («checks out») according to the onboard database of session keys

TABLE V
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}
Urgent exception	0	0	none (cleartext)

HMAC could still provide auditable message authenticity for cleartext payload

Compression of local routing data and key identification might be possible with MAC tag:

$$MMSI_B, \{payload\}_{K_{AB}}, HMAC$$

Humble beginnings for challenging IT/OT environments

TABLE V
REQUIREMENTS AND SPECIFICATIONS IN THE AUTHENTICATION OF UNDERWATER ASSETS

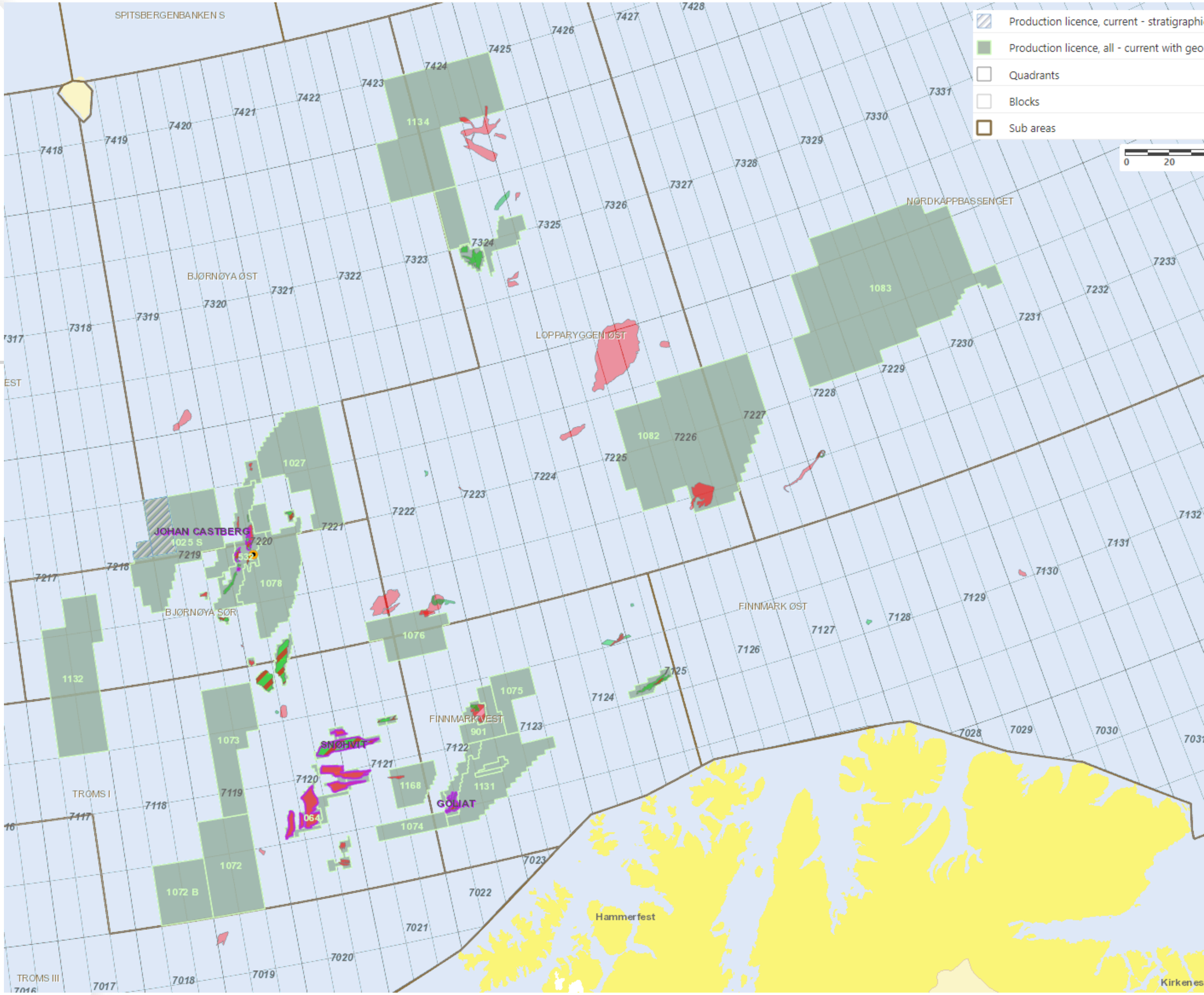
Requirement	**Specification**
Minimized number of packets	2 packets sufficient for friend ID
Fits JANUS baseline ADB	34 bits
Range at least 10 km	10+ km for 11 kHz acoustics
Key size at least 256 bits	2040 bits
Allows autonomous bilateral ranging	Through redundant timestamps

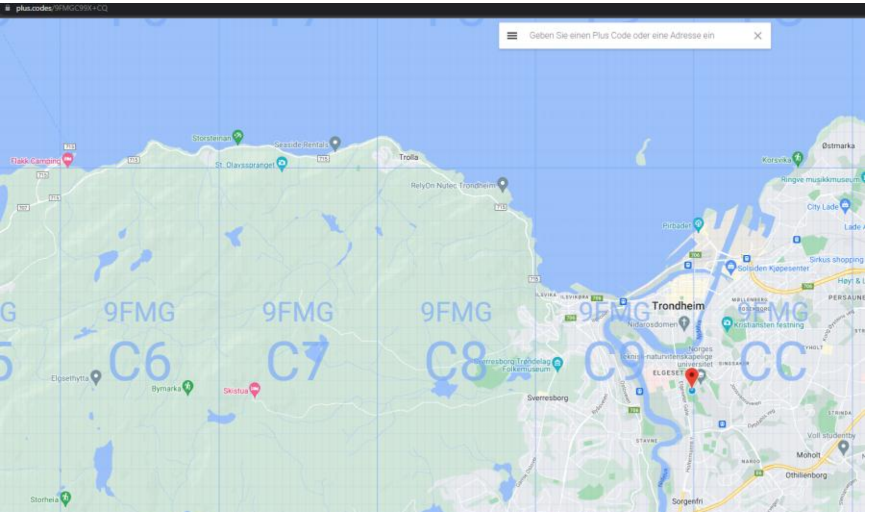
Major assumption: pre-shared key confidentiality

- Key management intensifies. Who pre-shares the keys and how?
  - Probably some kind of authority through radio connection (TLS 1.3).
- How does the authority know which key to give whom?
  - I propose a location based scheme.

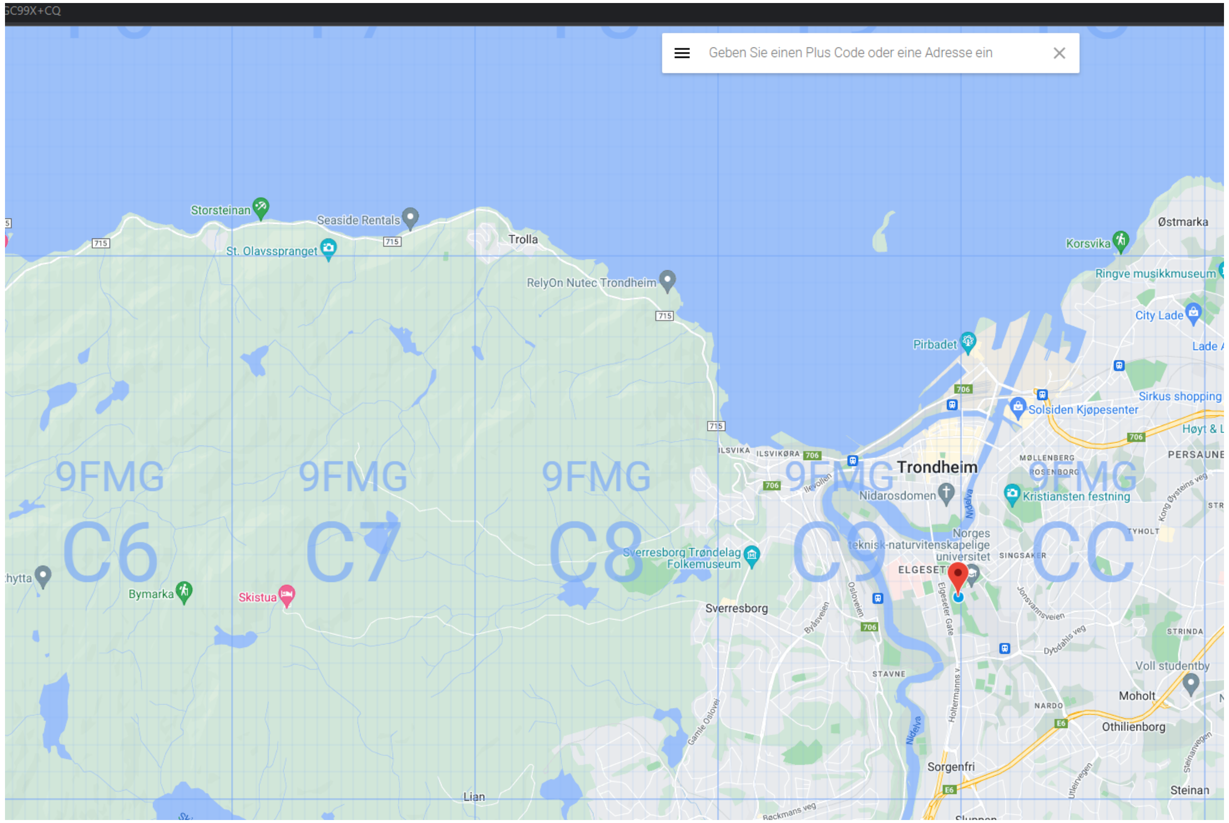
A Global, Location-Based Key Management

- Take a big (2048 bit) key
- Encrypt the (padded) geocodes with it
- Give the encrypted geocodes to license owners
- License owners authenticate everyone, call coast guard etc. if alarms sound

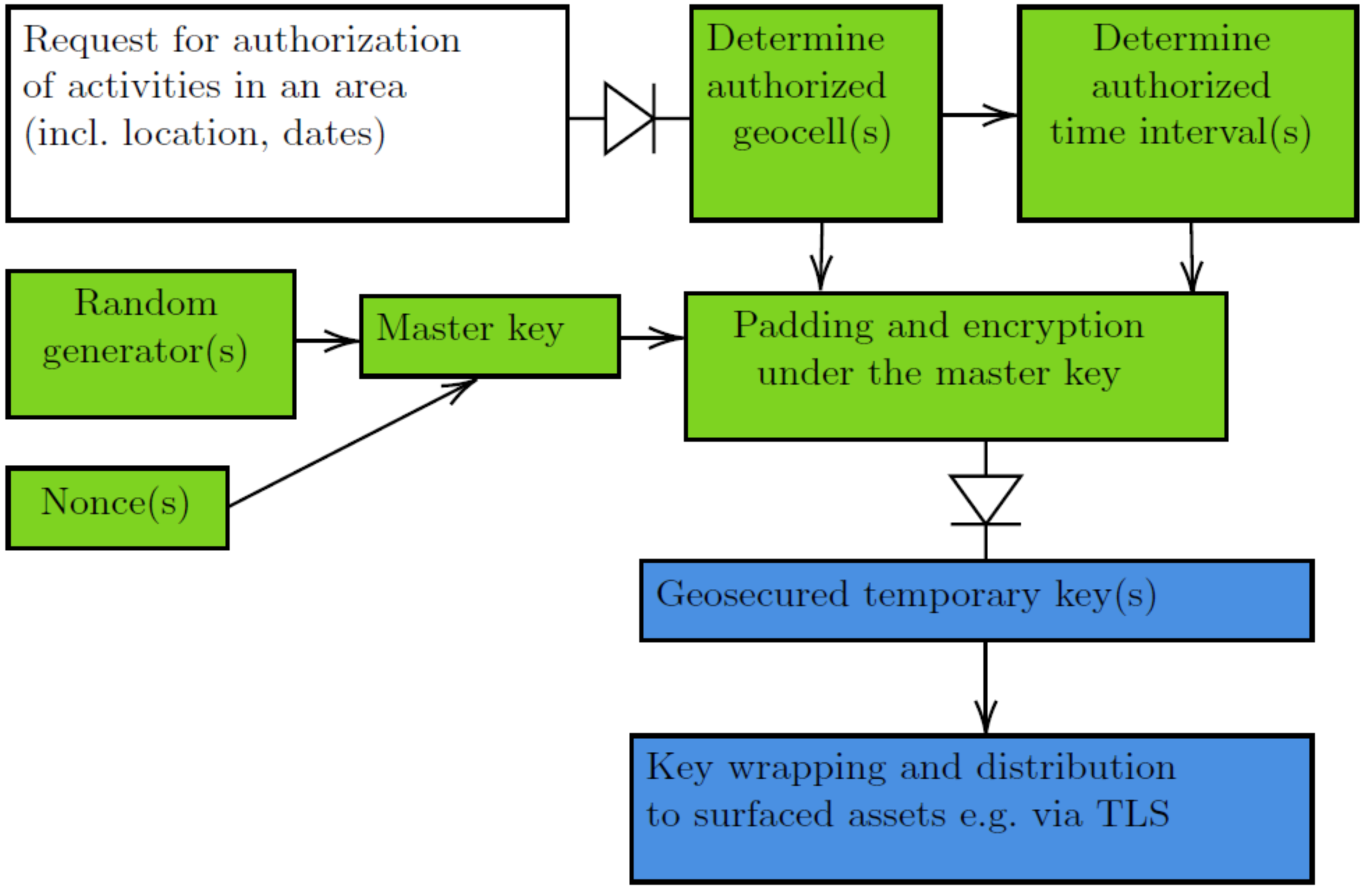


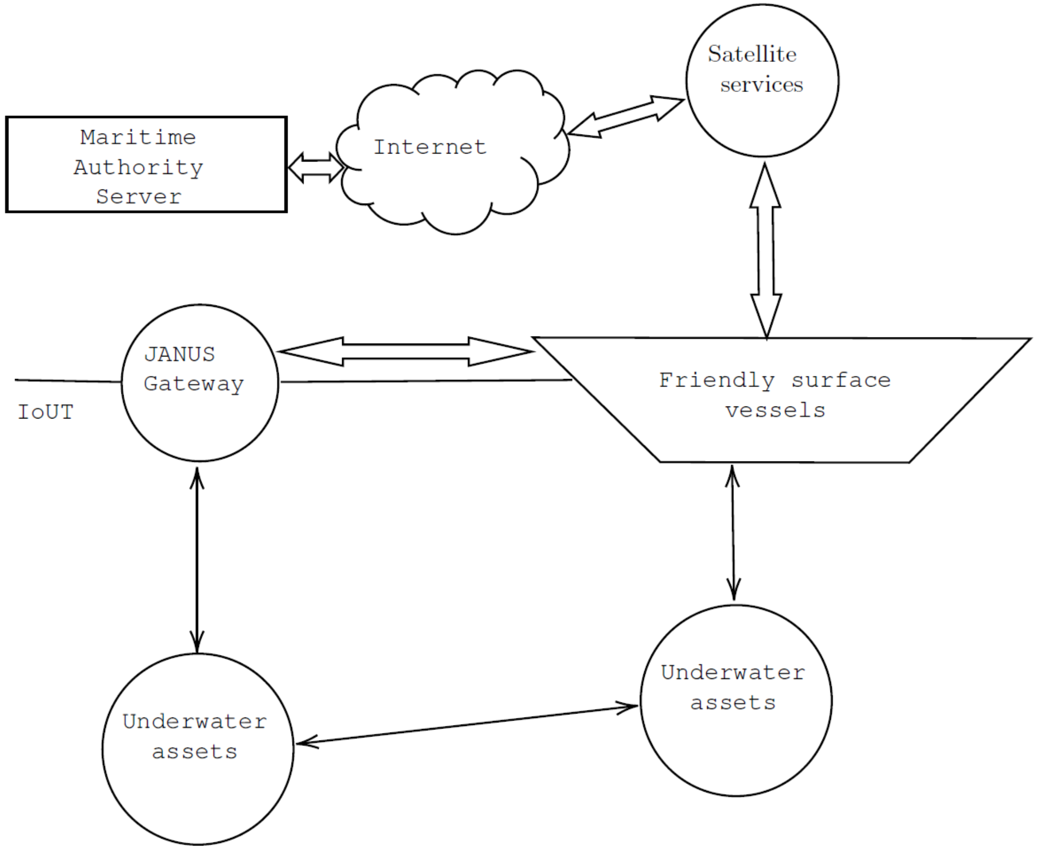


Tiling (tessellation) according to the Open Location Code (OLC) system (AKA plus.codes)



Key generation & distribution





Testing: til leaks, noise-to-signal do us part!

Positioning in society

- Secure acoustic digital/underwater comms are currently **still primarily** a military interest.
- DUV was founded with the immediate goal to participate in European calls for public-private partnerships
- The Standards Essential Patent (SEP) model famed for Nokia allow civilian commercialization of **protocols**

Welcome to the Cyber Physical Security Bar

Please place your orders:

1. What is security
2. Who needs security
3. Challenges of security in the offshore environment
4. Security solutions offshore
5. Authentication
6. Compliance-based regulation
7. Have it your way?

-> balint@d-uv.com