Authenticated Encryption for Janus-Based Acoustic Underwater Communication

Branislav Petrović, Bálint Zoltán Téglásy, Sokratis Katsikas

19.10.2022

Introduction

- Wireless underwater communication networks are rapidly increasing in quantity
- Janus – the most established physical-layer, acoustic standard
  - No security mechanisms
  - Confidentiality and integrity of data must be ensured
- Attacks are similar as in radio-based communication
  - Three main categories
    - Eavesdropping
    - Routing attacks
    - Data tampering
  - Authenticated encryption counteracts these
- Main challenges for providing security features:
  - Low data rate
  - High packet loss compared to air interfaces

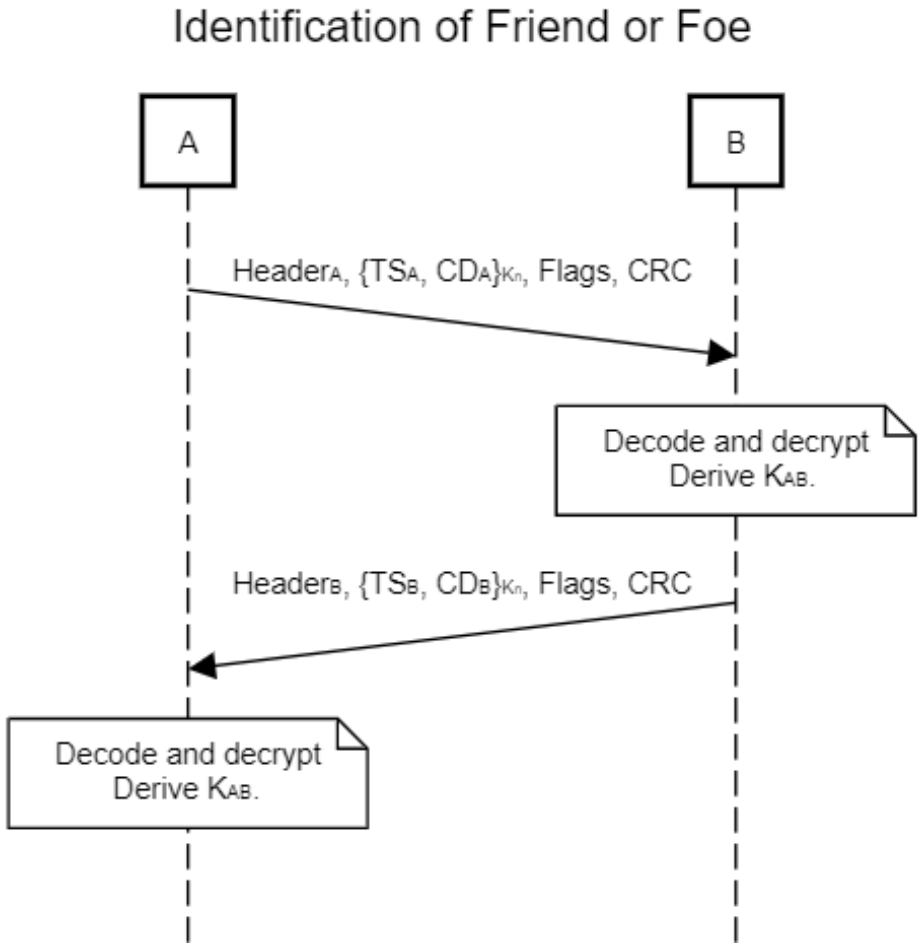
Janus Properties

- 80 bps, 10 km range
- 64-bit baseline packet
  - 34-bit Application Data Block (ADB)
  - Up to 10 min. additional cargo reservation (48 kb)
- Several baseline packets → less efficiency
- Cargo → channel reservation

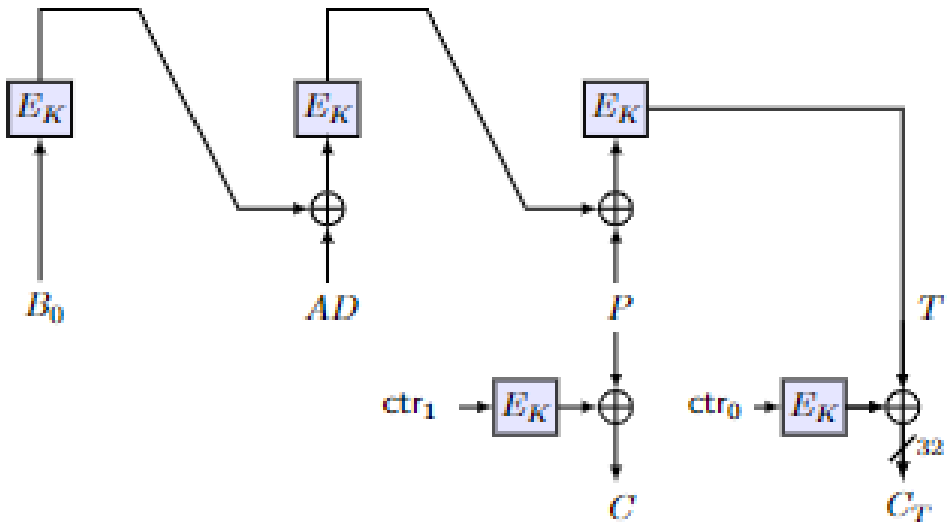
Version number	Mobility flag	Schedule flag	Tx/Rx	Forward capability	Class user i.d.	Application type	Repeat	Reservation time	Application data block	CRC	Optional cargo
4	1	1	1	1	8	6	1	7	26	8	$n \leq 48000$

First Authentication Protocol

- Authentication based on timestamps
  - TS, CD, F are exchanged
- Encryption with $RC5 - 32/12\ /16$
  - Pre-shared long-term key K_n
- Timestamps are checked for validity and used for ranging
- Session key K_{AB} is derived from $MMSI_A, TS_A, CD_A$ and $MMSI_B, TS_B, CD_B$
  - Each new K_{AB} is unique due to timestamp
- K_{AB} is stored in a lookup table of all other K_ns and MMSIs



Proposal 1: CCM



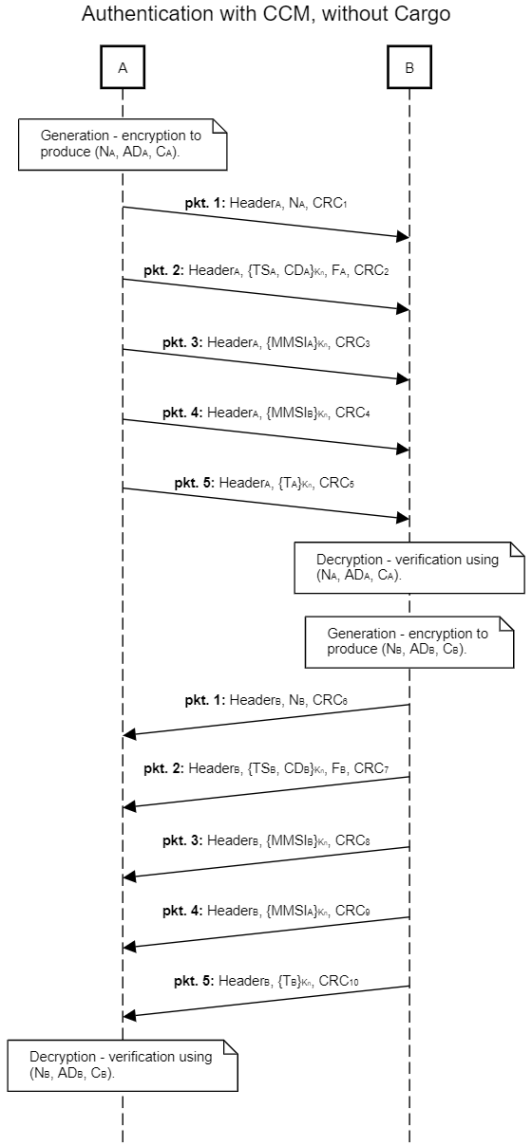
$B_0 = \text{Flags}_1||N||\text{Q}$

$\text{ctr}_i = \text{Flags}_2||N||i$

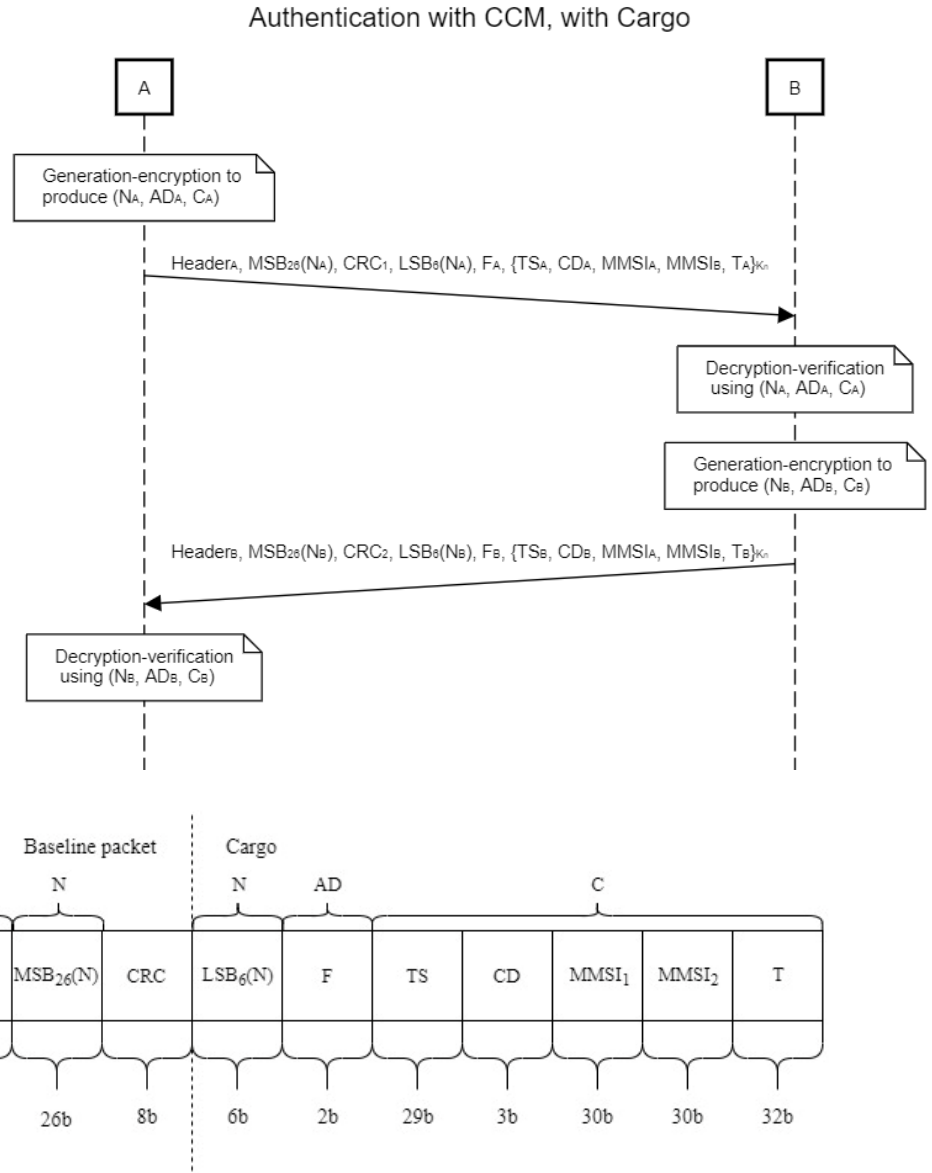
- Input:
  - Nonce N (32 b, expanded to 64 b upon reception)
  - Associated data AD (24 b without cargo, 32 b with cargo)
    - Consists of Janus header and F
  - Payload P (92 b)
    - Consists of TS, CD, and MMSIs of sender and receiver
- Output:
  - MAC tag T (32 b)
  - $C = AES(P||T, K)$
- (N, AD, C) are transmitted with Janus
- Relies on formatting and counter generation functions

CCM in the Authentication Protocol

Without Cargo



With Cargo

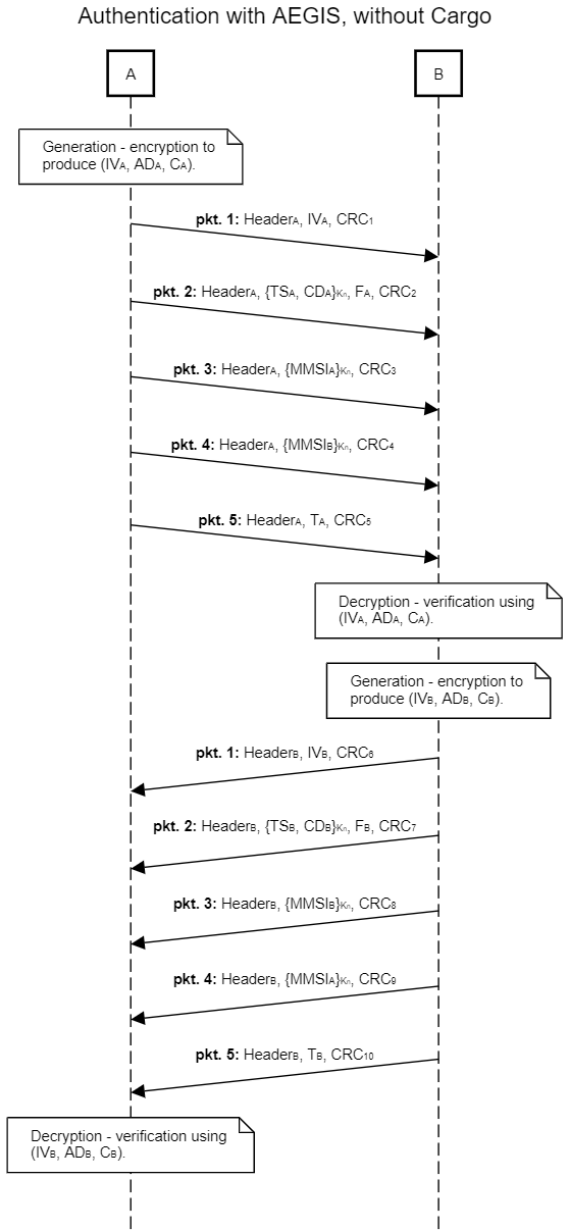


Proposal 2: AEGIS-256

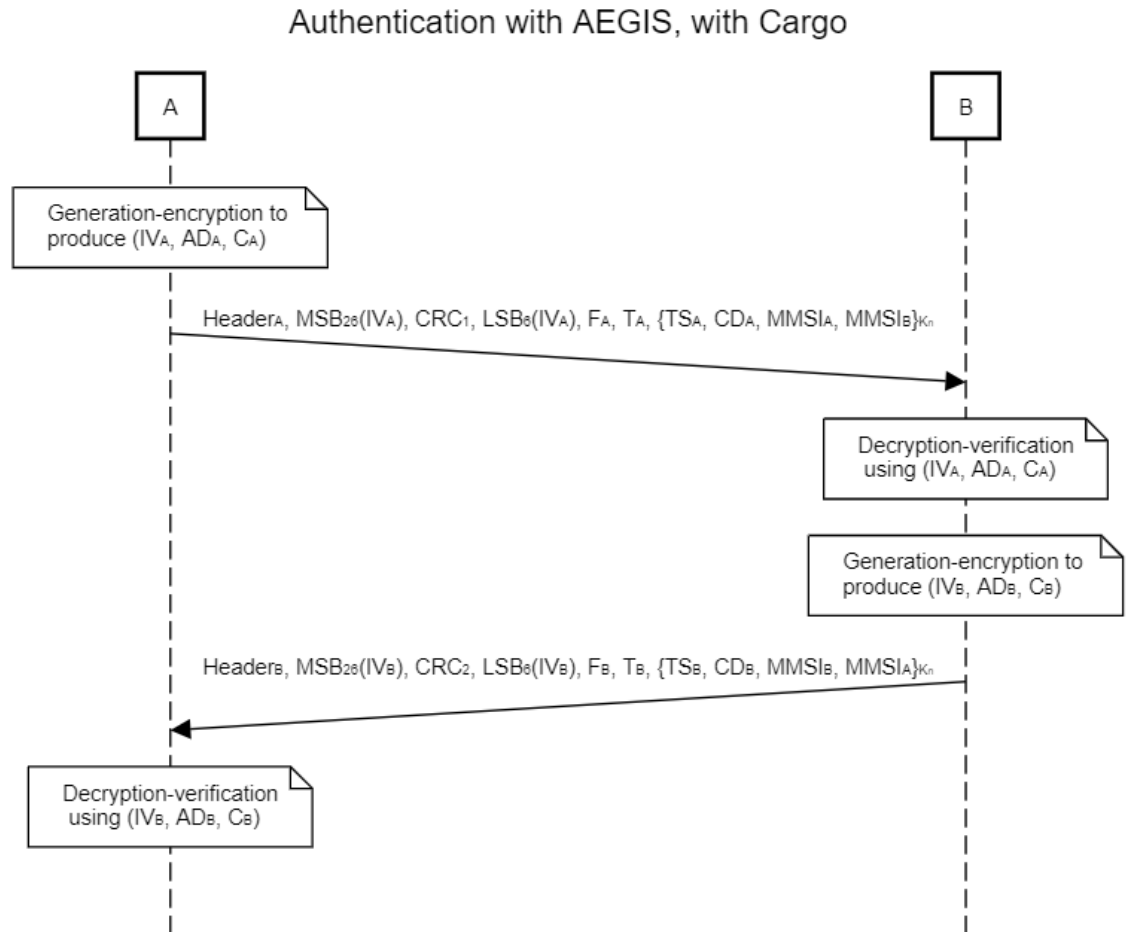
- State update
  - 6 AES rounds
  - Runs for every 16-byte plaintext block
- Initialization
  - K and IV are loaded into the state
- Processing of AD
  - AD is used to update the state
- Encryption
  - Plaintext blocks are XORed with state blocks
- Finalization
  - T is constructed from the state
- Input:
  - K (256 b)
  - IV (32 b, expanded to 256 b upon reception)
  - AD (24 b without cargo, 32 b with cargo)
  - P (92 b)
- (IV, AD, C, T) are transmitted with Janus

AEGIS in the Authentication Protocol

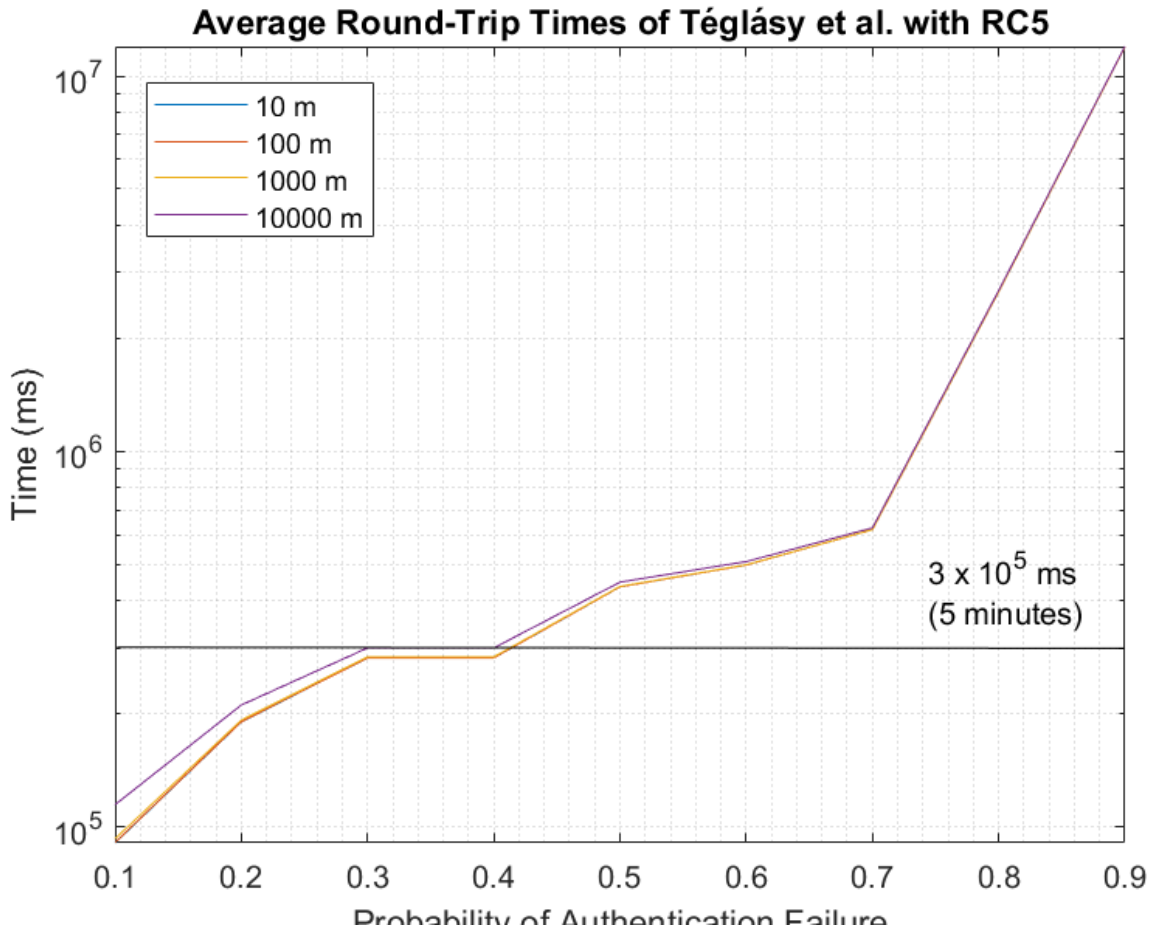
Without Cargo



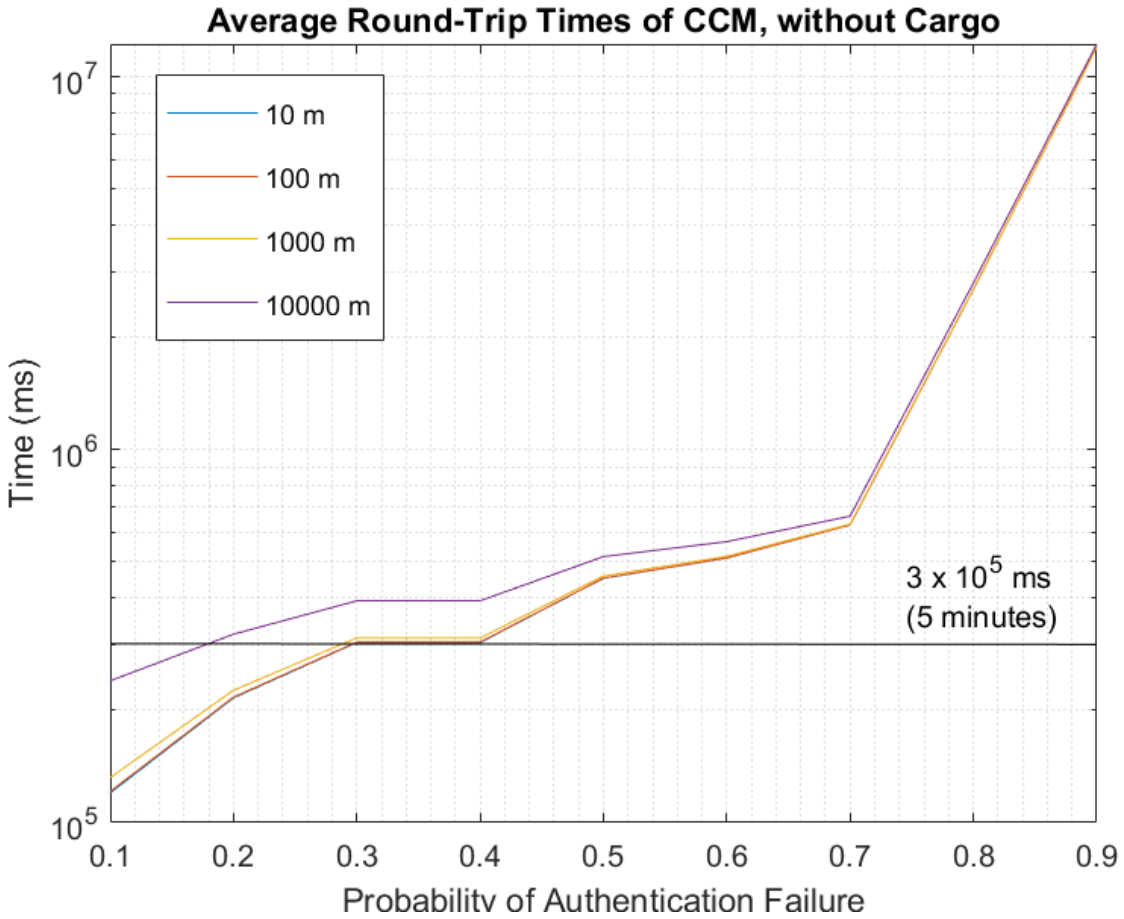
With Cargo

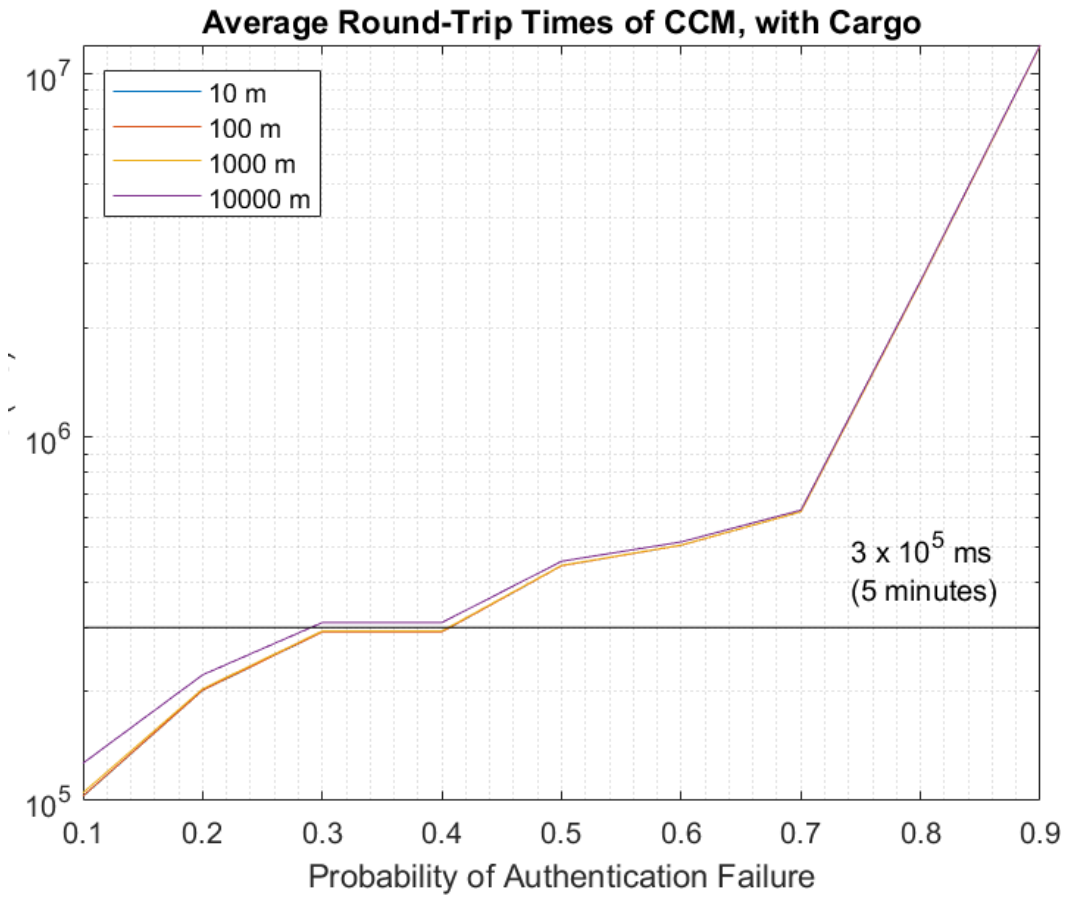


Simulation Results: Original Protocol

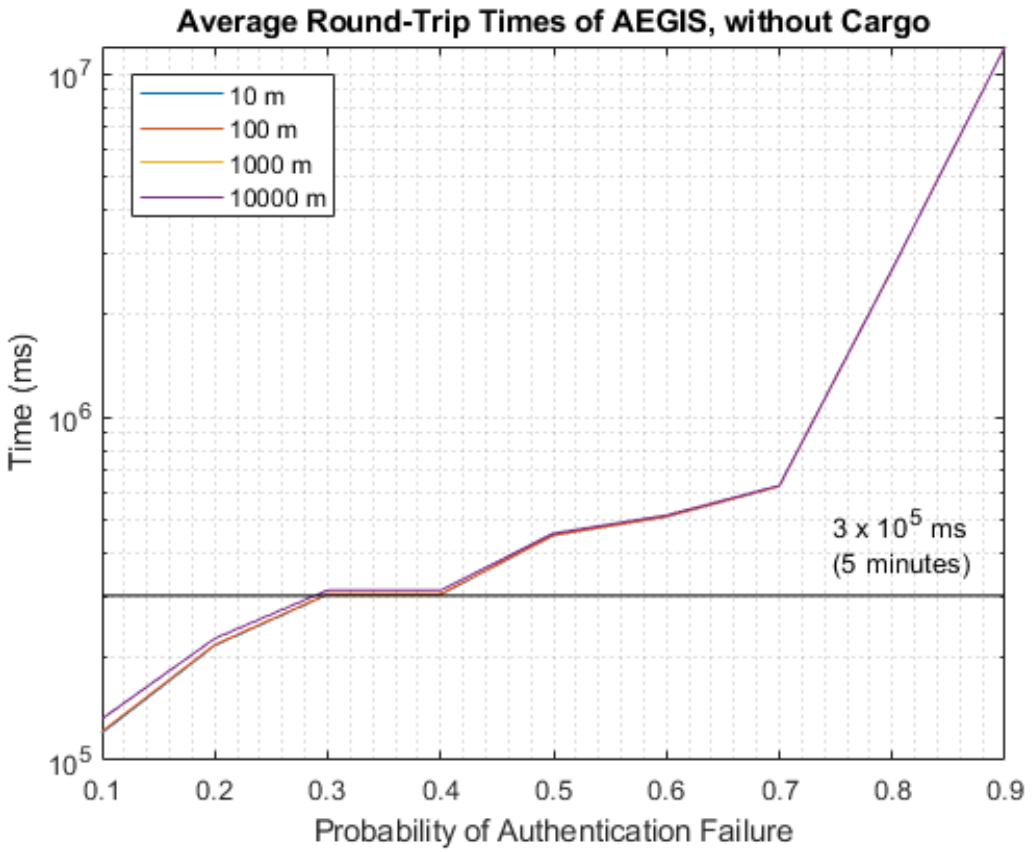


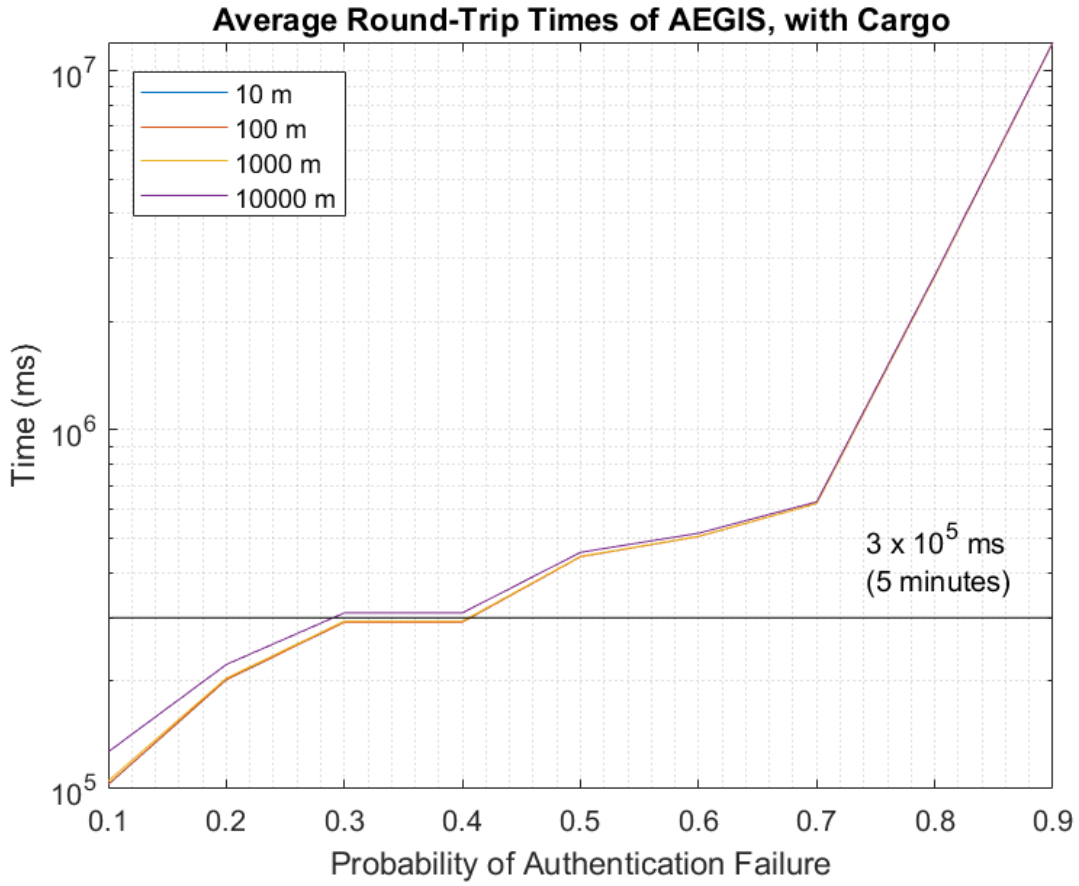
Simulation Results: CCM





Simulation Results: AEGIS-256





Conclusion

- Contributions
  - Proposed two AE schemes for providing confidentiality and integrity in wireless acoustic underwater communication using the Janus standard
    - Evolved the original protocol and kept the ranging functionality
  - Minimized communication overhead for completion within a reasonable time period in a simulation environment
    - Results indicate the possibility of practical realization
  - Provided high security against most attacks
- Future work:
  - Authenticated key exchange with forward secrecy to justify K_{AB}
  - Real-world implementation and testing