Security Improvements for the Automatic Identification System

M.S. Thesis Defense

Robert E. Litts

Department of Electrical and Computer Engineering

April 1st, 2021

OLD DOMINION
UNIVERSITY

Outline

The Need for Vessel Monitoring

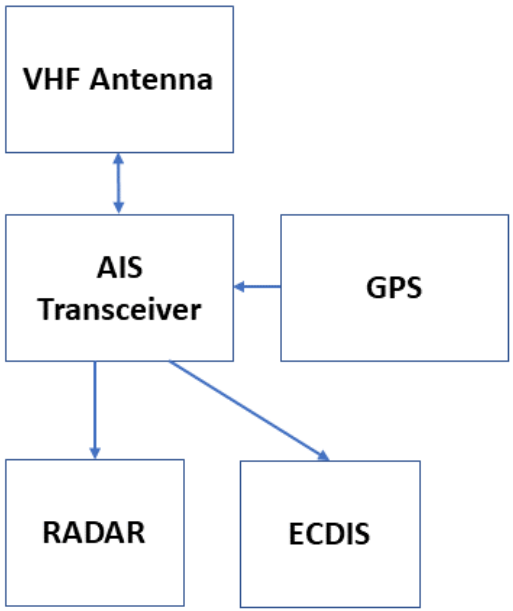
- In 1989, the tanker vessel Exxon Valdez spilled 11 million gallons of oil into Alaska's Prince William Sound
- 1990 Oil Pollution Act (OPA), required the U.S. Coast Guard to improve vessel tracking and monitoring services within ports and harbors
- International Telecommunication Union (ITU)/International Maritime Organization (IMO) wanted a standardized protocol for worldwide usage

Exxon Valdez Oil Spill

The Creation of AIS

- In the late 1990s, the Automatic Identification System (AIS) was created as a situational awareness and collision avoidance tool to provide Vessel Traffic Services (VTS) with improved clarity in harbors and improve navigational safety onbord vessels.
- AIS was created in a pre-9/11 world when cybersecurity was not a requirement, so the system operates completely free within the maritime Very High Frequency (VHF) band.
- Assumption that all users would operate with respect and would not attempt to use this tool for nefarious purposes.
- In the early 2000s, AIS became mandatory onboard the vast majority of commercial vessels and gave them a complete electronic picture of all surrounding vessels regardless of the weather, sea state or visibility, which commonly cause RADAR deterioration.
- Today, the availability of small, inexpensive AIS transceivers means that almost every vessel on the ocean operates with AIS.

AIS Configuration



Existing Requirements

- IMO Safety of Life at Sea (SOLAS) agreement adopted following 1914 sinking of the Titanic
- SOLAS chapter V AIS Requirements: Vessels $\geq 300GT$ on international voyages, cargo ships of $\geq 500GT$ not engaged on international voyages, all passenger ships.
- SOLAS Chapter V 18.9 requires an annual test by an approved surveyor or testing facility which verifies the correct programming of static information and on-air RF testing.
- U.S. CFR 33 requires vessels accurately broadcast a properly assigned maritime mobile service identity (MMSI) number, upkeep data and update system.
- No U.S. regulations which require AIS inspection in U.S. navigable waters

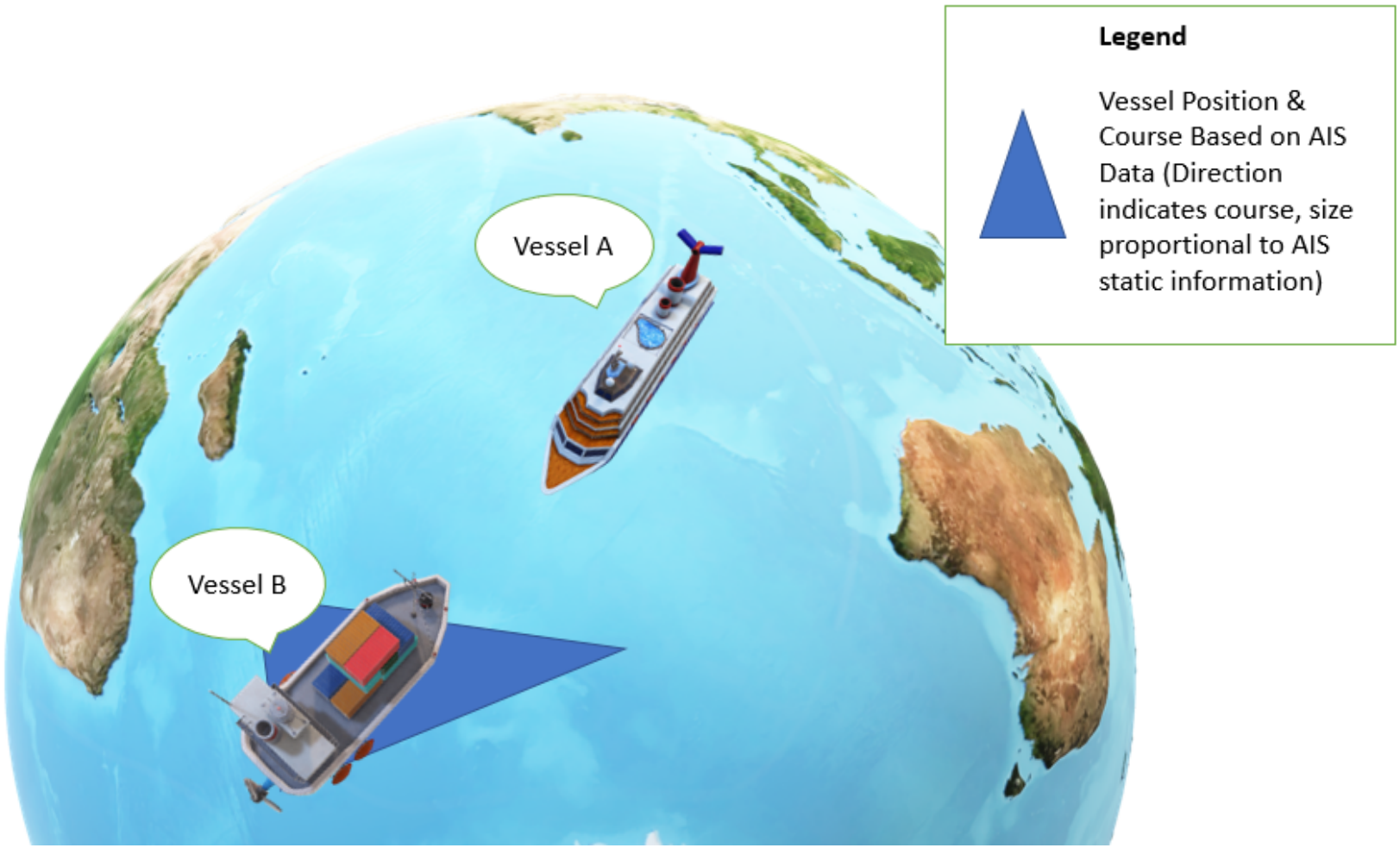
Lack of Security By Design

- The U.S. Coast Guard Navigation Center (NAVCEN) states: "AIS by design, is an open, non-proprietary, unencrypted, unprotected radio system, intended to operate on non-secure VHF-FM channels. So technically it can be spoofed - **so trust, but, verify**"
- Directs users to submit a problem report if they encounter AIS related errors
- A recent collision between two towing vessels improperly displaying their static AIS data on the Mississippi River prompted the USCG to release a Marine Safety Alert titled "AIS – Accurate Broadcasts Don't Happen Automatically".
- In 2018, members from the U.S. Coast Guard Research and Development Center (RDC), some of whom were involved in the initial creation of AIS in the nineties, stated that we must begin an international discussion on the requirements of "AIS 2.0" which should take into consideration national cybersecurity objectives.

AIS Vulnerabilities

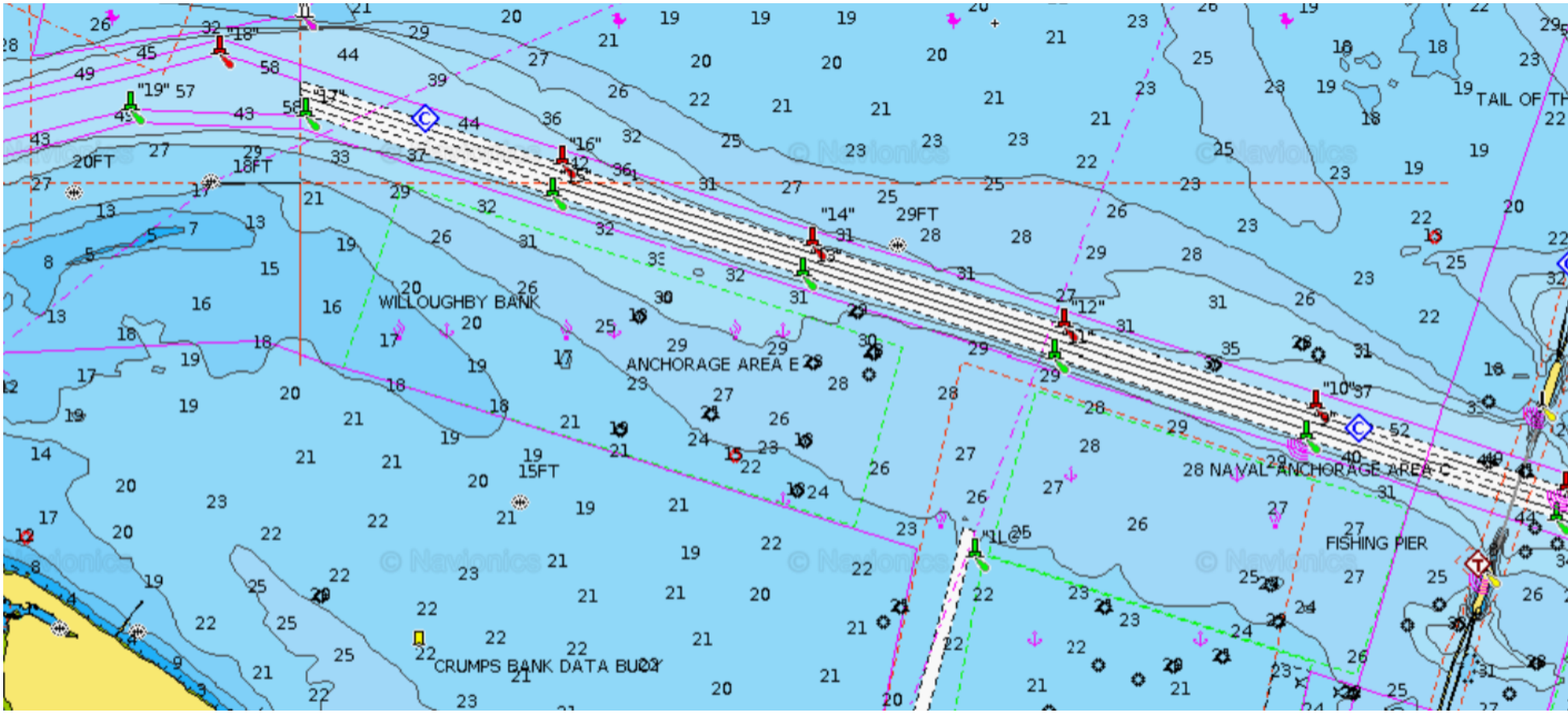
- **Spoofing (Ship, ATON, SART)** – Assigning static and dynamic AIS information to a fake ship, buoy, SAR target
- **Collision Spoofing** – Set off alarms using their first identified threat (ship spoofing) by placing a fictitious vessel on a collision course with another real vessel
- **Weather Forecasting** – Using binary messages to convey false weather alerts
- **Hijacking** – Modifying a real user's AIS static or dynamic information to falsify the vessel's location
- **Availability or Frequency Disruption** – Impersonating maritime authority using existing AIS messages to disable all AIS communications within a large geographic area or force frequency shift (persists after reboot)
- **Timing Attack** – Overload the SOTDMA algorithm

Problem Scenario 1



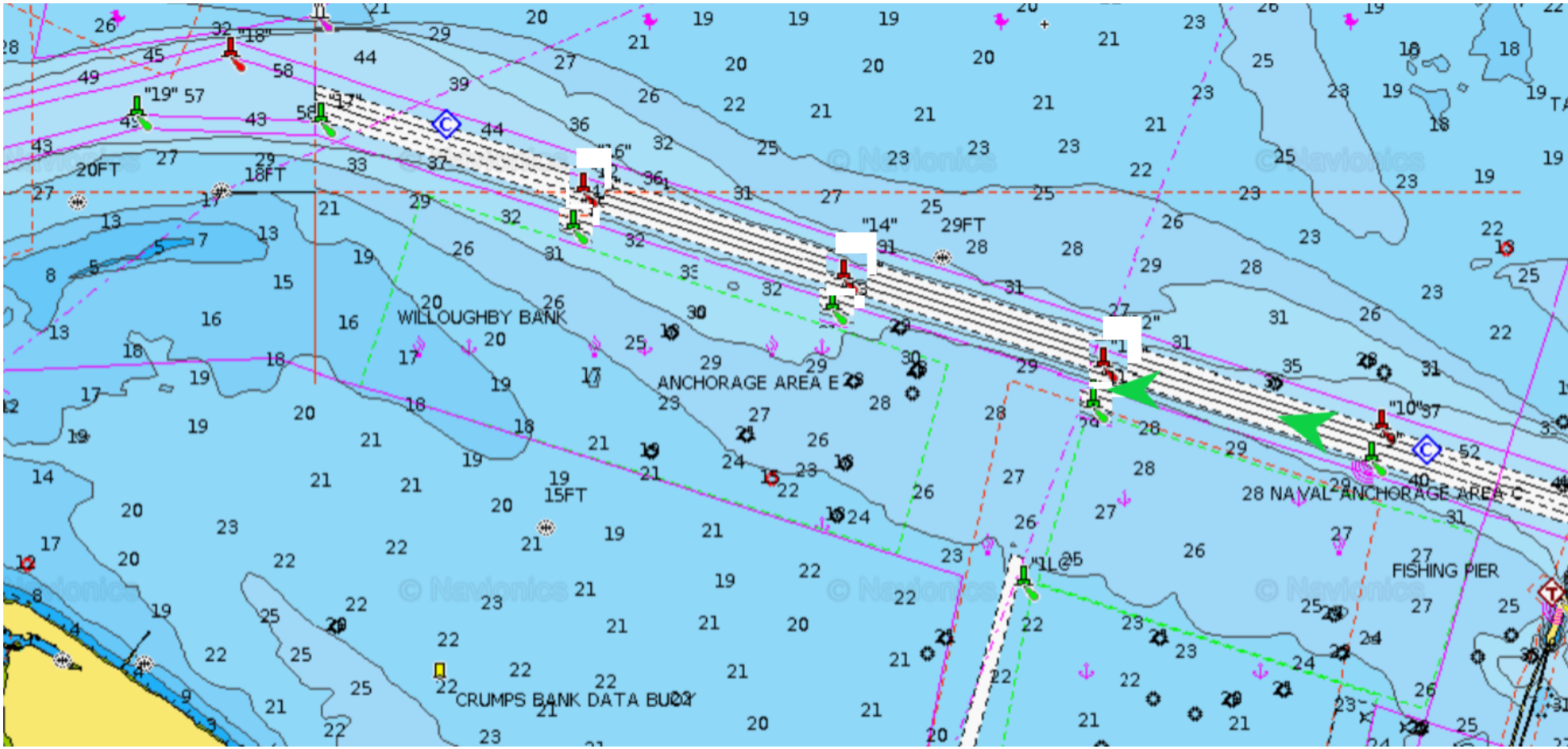
- Vessel's may be transmitting false or incorrect data, leading to confusion and potentially collisions

Problem Scenario 2



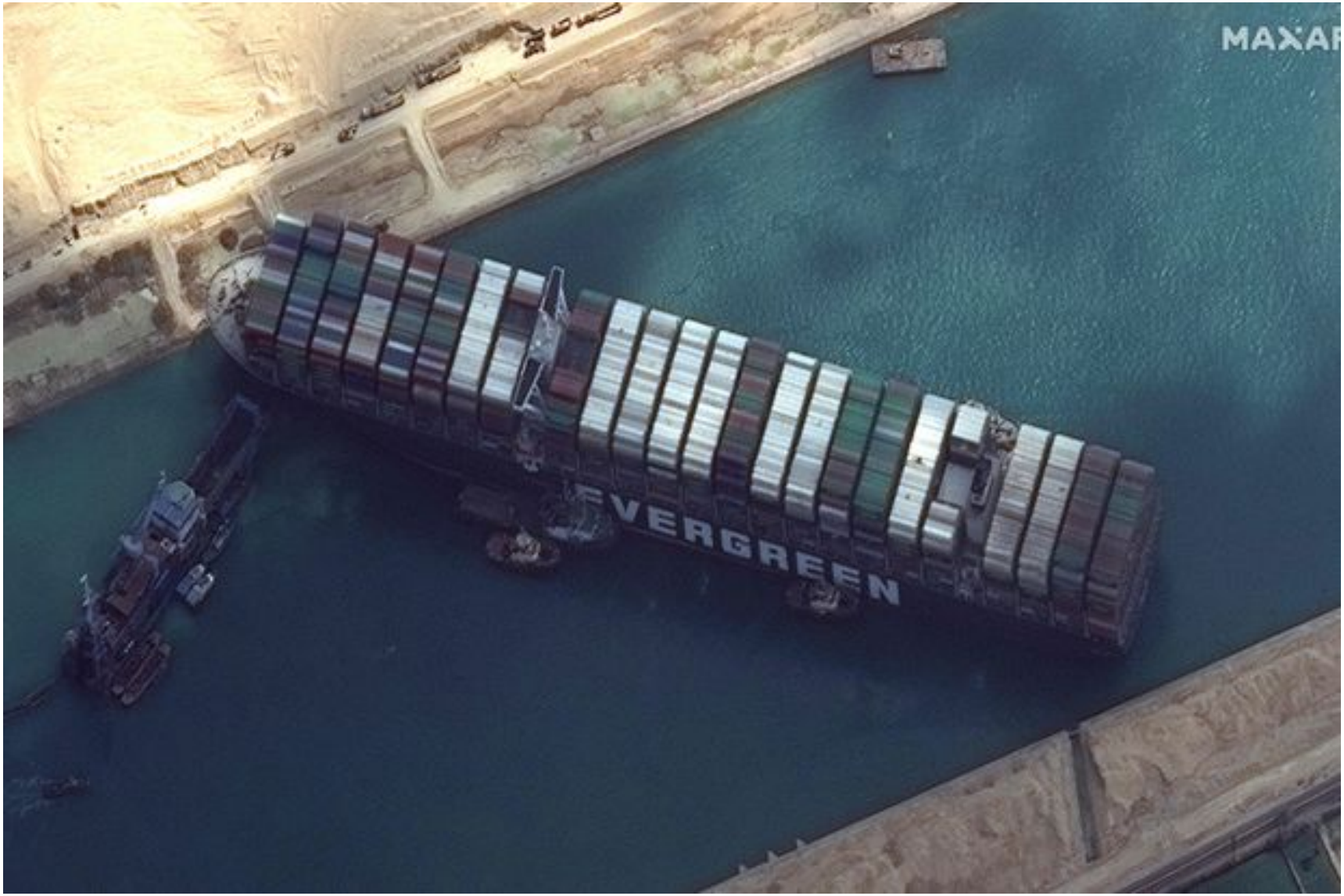
- Aids-to-navigation (ATON) can be spoofed, making harbors inaccessible

Problem Scenario 2



- Aids-to-navigation (ATON) can be spoofed, making harbors inaccessible

M/V EVER GIVEN: March 23rd, 2021



Motivation for Thesis

- The reliability of AIS currently hinges upon good faith of its users
- Well-documented vulnerabilities that can easily be exploited by an adversary armed with a simple software-defined radio (SDR) and a VHF antenna which could potentially cripple a major harbor.
- Several commercial and government products provide encrypted AIS transmissions for smaller subsets of vessels for use in law enforcement and other fleet activities where confidentiality is required.
- Vessel data can be spoofed (false targets) and hijacked (information changed en-route to destination)
- Messages lack a time stamp and are therefore vulnerable to replay attacks using legitimate data

Goal

Evaluate a feasible method to bring AIS up to the twenty-first century cybersecurity standards & eliminate three of the major vulnerabilities:

- Lack of source authentication
- Lack of message integrity
- Lack of time stamp

Contributions

Contribution 1: Built a Software Defined Radio (SDR) implementation of AIS which provides a robust test platform for system analysis.

Contribution 2: Designed an authentication protocol for securing AIS, based on the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol which enables receivers of multicast communications to authenticate the source and integrity of received data packets.

- Unlike the alternative approaches, can authenticate messages without the use of an a priori shared secret key, no need to conduct key exchanges over several messages, requires significantly less overhead.
- Provides authentication, integrity, and time stamp

AIS Technical Overview

- A system which automatically and continually broadcasts a ship's dynamic and static information to all other stations in range
- Can receive and process the same information from others in a self-organized manner.
- Access to the VHF data link (VDL) should be accommodated through time division multiple access (TDMA).
- Capable of transmitting safety related messages on request.
- 161.975MHz (AIS 1, default channel 1, 2087) and 162.025MHz (AIS 2, default channel 2, 2088), 25kHZ Bandwidth

Transmission Schedule

Class A shipborne mobile equipment reporting intervals[2]

Ship's dynamic conditions	Nominal reporting interval
Ship at anchor or moored and not moving faster than 3 knots	3 min[(1)]
Ship at anchor or moored and moving faster than 3 knots	10 s[(1)]
Ship 0-14 knots	10 s[(1)]
Ship 0-14 knots and changing course	3 1/3 s[(1)]
Ship 14-23 knots	6 s[(1)]
Ship 14-23 knots and changing course	2 s
Ship >23 knots	2 s
Ship >23 knots and changing course	2 s

(1) When a mobile station determines that it is the semaphore (see § 3.1.1.4, Annex 2), the reporting interval should decrease to 2 s (see § 3.1.3.3.2, Annex 2).

- Reporting Interval (RI): Dynamic information (position/course/speed) transmits at a variable rate based on ship's navigation status, speed, and course changes.
- Every 6 minutes: Transmit static information (such as name, MMSI, call-sign, length); also when data has been changed or upon request.
- ATON report every 3 minutes
- Reporting Rate (RR): $RR = \frac{60}{RI}$, (2-30 reports per minute)

Analysis of AIS Using OSI Model

AIS Layers 1-4

Transport Layer

- Convert data into transmission packets of correct size
- Sequencing data packets
- Interface to higher layers

Network Layer

- Message priority management
- Congestion resolution
- Distribution between channels

Link Layer

- UTC Coordination for TDMA
- Synchronization using SOTDMA

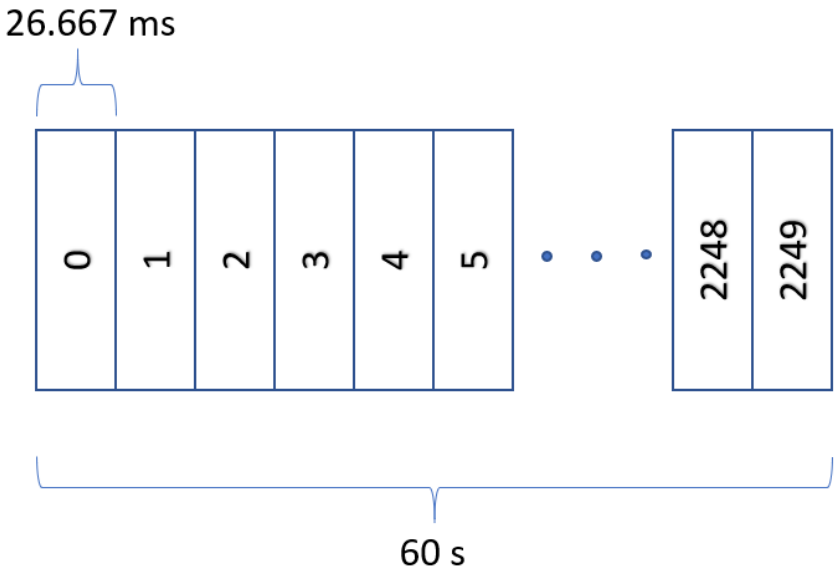
Physical Layer

- Transfer bit stream using NRZI encoding
- Convert digital NRZI encoded packet to analog GMSK signal

Link Layer

- Data from the VHF channel is accessed using TDMA with a common time reference synchronized every 2 seconds for a mobile user and every 3.33 seconds for a base station.
- Users either have direct access to coordinated universal time (UTC) by setting a synchronization state to UTC direct, while other stations who cannot should synchronize their time off of nearby stations with the proper synchronization state set.
- Users cannot achieve indirect synchronization more than one user removed from UTC direct to avoid timing errors.

Link Layer: TDMA Frame



- One minute blocks of time divided into $2,250$ slots (indexed $0 - 2249$)
- Frames are coordinated with UTC to start/stop with each UTC minute.
- Each slot is allocated $26.667ms$ for transmission.
- Users may begin transmitting Radio Frequency (RF) power at the start of a slot and must conclude within the allocated slots for transmission.

Link Layer: Data Packet

Ramp Up 8 bits	Training Sequence 24 bits	Start Flag 8 bits "011111110"	Data 168 bits	FCS 16 bits	End Flag 8 bits "011111110"	Buffer 24 bits

- Data transmitted in 256 bit packet
- Ramp up: Used between start of RF power and 80% RF power
- Buffer: Allows for differentiation between messages from delay, sub-divided into the following:
  - item Bit stuffing – 4 bits
  - Distance delay – 14 bits correcting for propagation delay of over 120NM (maximum possible is 235.9 nautical miles)
  - Synchronization jitter – 6 bits used to preserve integrity of TDMA
- Stations are allowed to occupy a maximum of 5 consecutive slots for continuous transmission; only required to send a single set of overhead messages surrounding the data at the beginning/end of the transmission.

Link Layer: Access to Data Link

<table>
<tr><td colspan="5">SOTDMA Data
168 bits</td></tr>
<tr><td>Msg ID
6 bits</td><td>User ID
30 bits</td><td>Data
113 bits</td><td colspan="2">Communication State
19 bits</td></tr>
<tr><td colspan="3"></td><td>Sync State
2 bits</td><td>Slot time-out
3 bits</td><td>Sub message
14 bits</td></tr>
</table>

- SOTDMA is the primary access scheme; used mainly for repetitive, autonomous messages. To enter VDL, an AIS device will:
- Monitor the VDL link for 1 minute to determine a dynamic directory & generate a frame map
- Start network entry phase, wait for a nominal transmission slot (NTS) which is randomly selected among potential candidate slots within the selection interval using ITDMA to pre-designate a slot.
- At NTS, the device (if Class A mobile) will transmit a special position report & select next NTS using the SOTDMA access scheme

Symmetric (Secret) Key Cryptography

$$m = K_A[K_A(m)] \tag{1}$$

- The same key (called a key pair) used for both encryption and decryption.
- K_A is an encryption key used by "Alice" to seal the contents of the message
- If the key is given to "Bob", he can use K_A to decrypt the message.
- Secret key must remain secret; key must be transmitted securely.
- Users can physically exchange keys, but this limits the scope of the encryption mechanism
- If the key is compromised, all messages between users should assume to be clear.
- No authentication

Asymmetric (Public) Key Cryptography

$$K_B^+(m) \rightarrow K_B^-[K_B^+(m)] = m \tag{2}$$

$$m = K_B^-[K_B^+(m)] = K_B^+[K_B^-(m)] \tag{3}$$

- Alice's Private Key: K_A^-
- Alice's Public Key: K_A^+ (CA binds public key to Alice)
- Bob's Private Key: K_B^-
- Bob's Public Key: K_B^+ (CA binds public key to Bob)
- Alice and Bob can exchange a plaintext message without the need to exchange a secret key.
- Key pairs are generated in such a manner that one of the keys is the the only possible method to decode a message encrypted with the other.

Digital Signatures

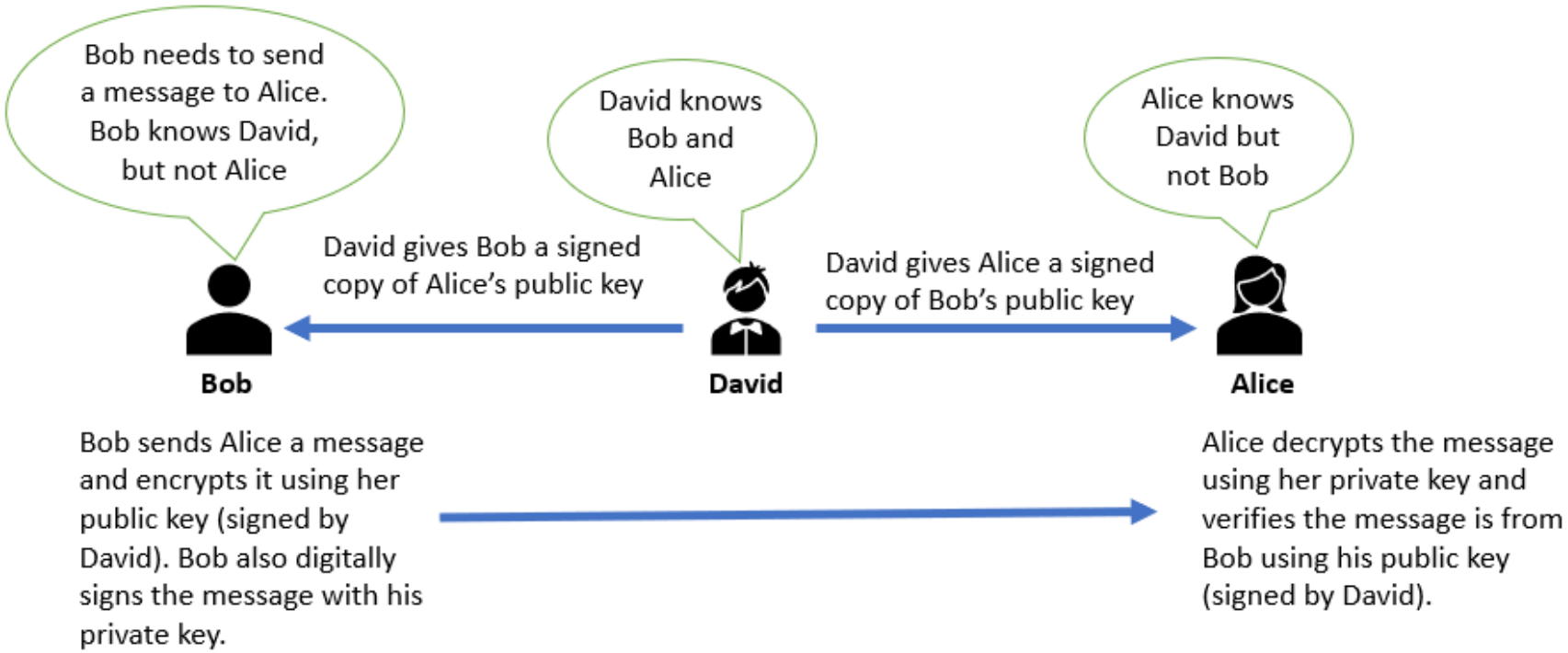
$$K_A^-(m) \rightarrow K_A^+[K_A^-(m)] = m \tag{4}$$

- Digital signatures require 3-5 orders of magnitude more processing power than symmetric key cryptography.
- Hashed message authentication code (HMAC) can be used to reduce computation when signing long messages
- Entire message and secret key is sent through a hash function, provides a one-way, fixed size fingerprint of the message which cannot be reversed.
- Attach to the original message.
- Receiver computes hash of plain text message and secret key, compares the results to HMAC.
- If they are identical, verifies message authenticity and integrity
- Difficult to scale HMAC (due to private key)

Identity Based Encryption

- PKI where public keys are generated based on other publicly available, unique information (name or e-mail address).
- Users only have one interaction with the trusted third party to obtain their private key
- Public keys can be generated on an as-needed basis by users.

PGP Web of Trust



Related Work

- [27]: Security review using SDR, validated vulnerabilities, proposed X.509 PKI and anomaly detection software
- [28]: SecureAIS - software-only encryption/authentication using ECQV/ECDH implicit certificates, less data than X.509; symmetric key & requires key exchange
- [29]: IEEE 1609 influenced system with 3-tiers of users with varying levels of data exchanged, including encryption
- [30]: IBE scheme using MMSI as public key
- [31]: USCG Encrypted AIS (EAIS), symmetric key AIS system in use by US Govt; uses binary message 6/8 to encapsulate packets, encrypt with AES
- [33]: Protected AIS (pAIS) - Proof-of-concept PKI system for AIS within current ITU standard, protect string (8-bit checksum over message, digitally signed with time stamp), legacy receivers ignore protect string

Related Work - Aviation and MANET

- [34]: ADS-B - Time Difference of Arrival (TDOA) using antennas at known locations, spread spectrum, frequency hopping, TESLA and $\mu TESLA$
- [22]: NASA research on blockchain using IBM Hyperledger Fabric
- [42]: MANET - Self-organized PKI and chain of trust, significant overhead requirements
- [43]: PGP-like trust establishment with certificate-less IBE to reduce overhead from [42], significant technical changes to AIS standard for implementation

SDR Background

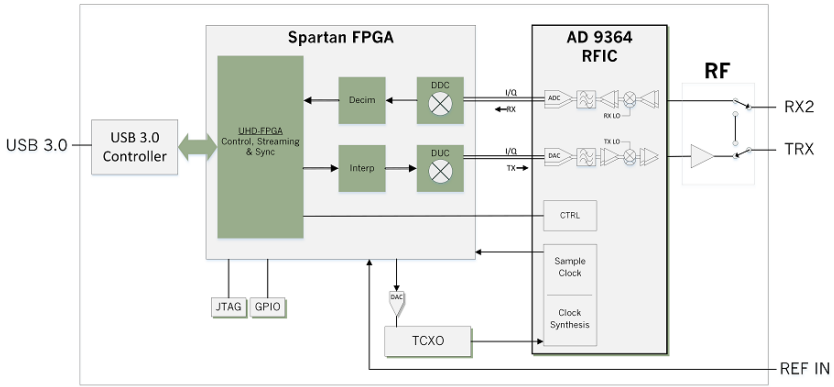


Figure: B200 Mini

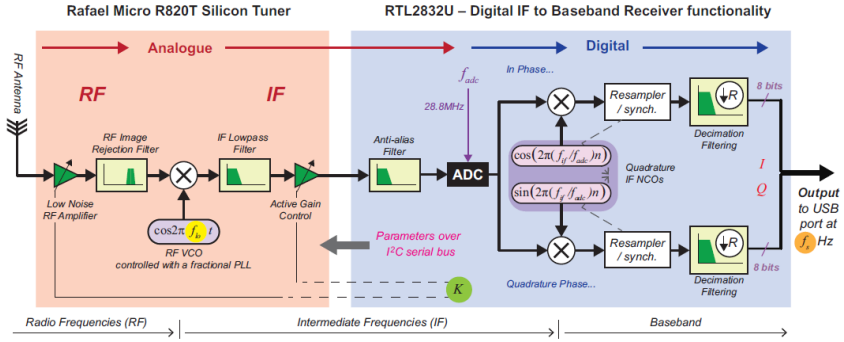
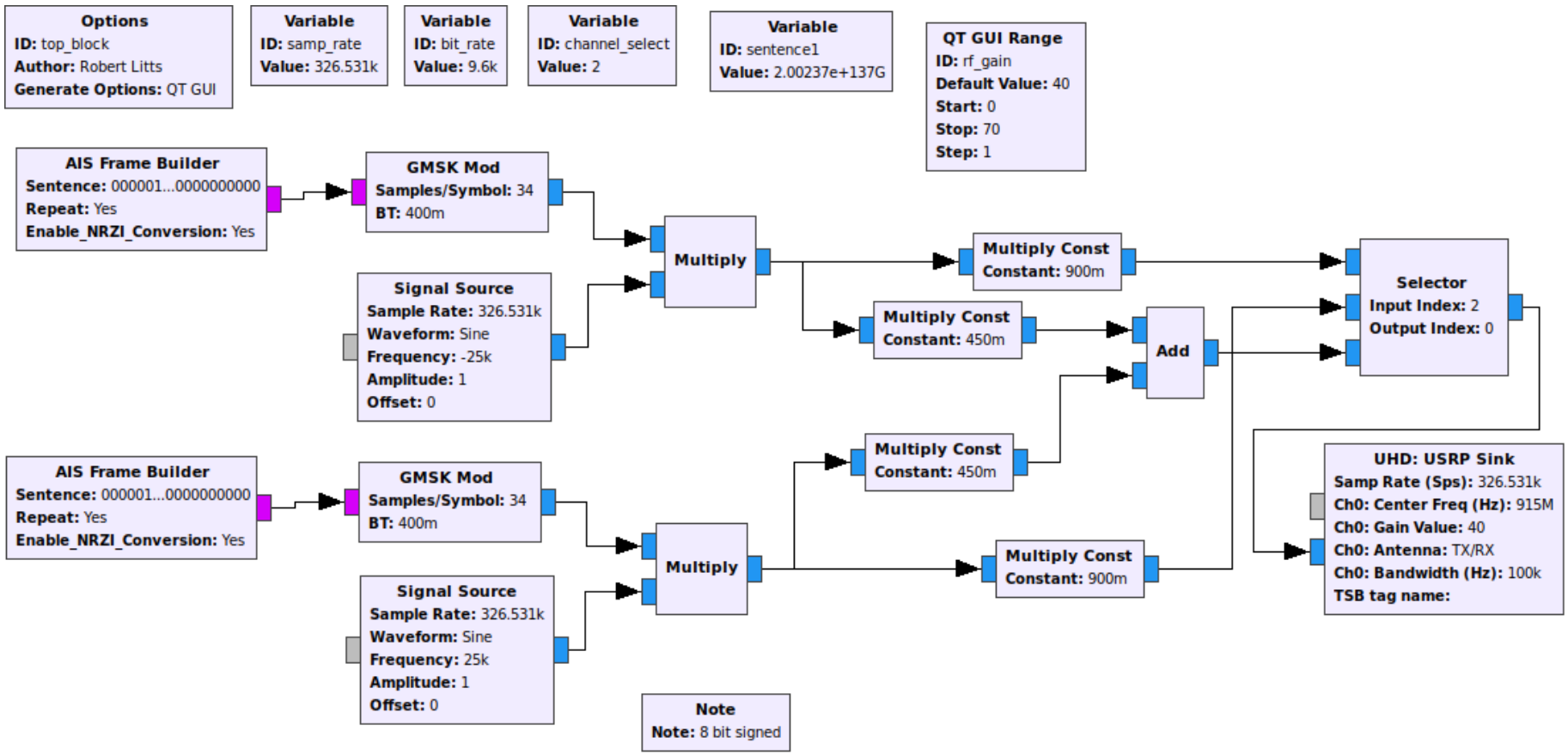


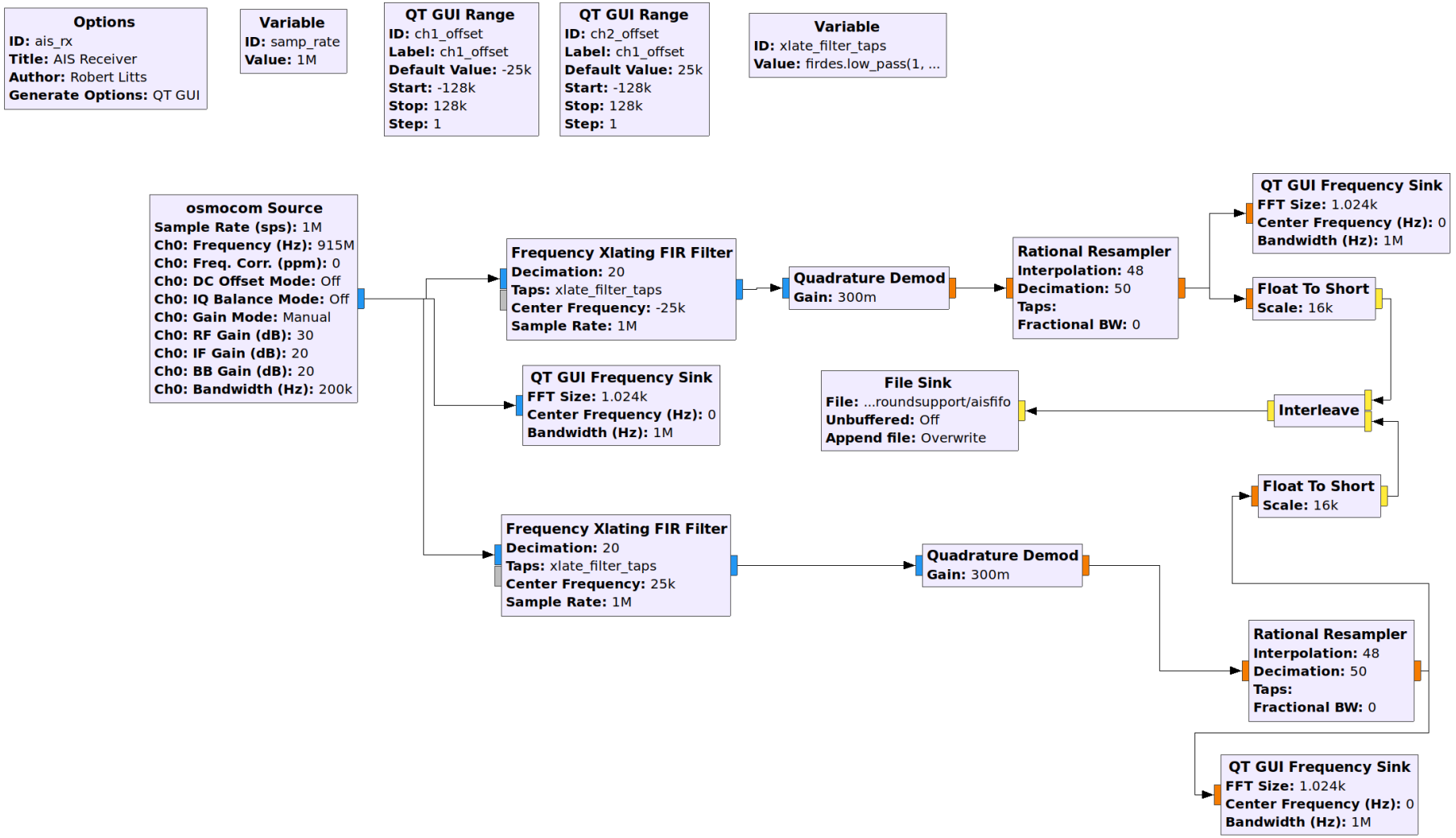
Figure: RTL-2832

- First theorized by Joseph Mitola in the early 1990s
- Allows for physical layer hardware components of a radio system to be implemented using software
- Highly customizable and reconfigurable system
- GNU Radio Companion software

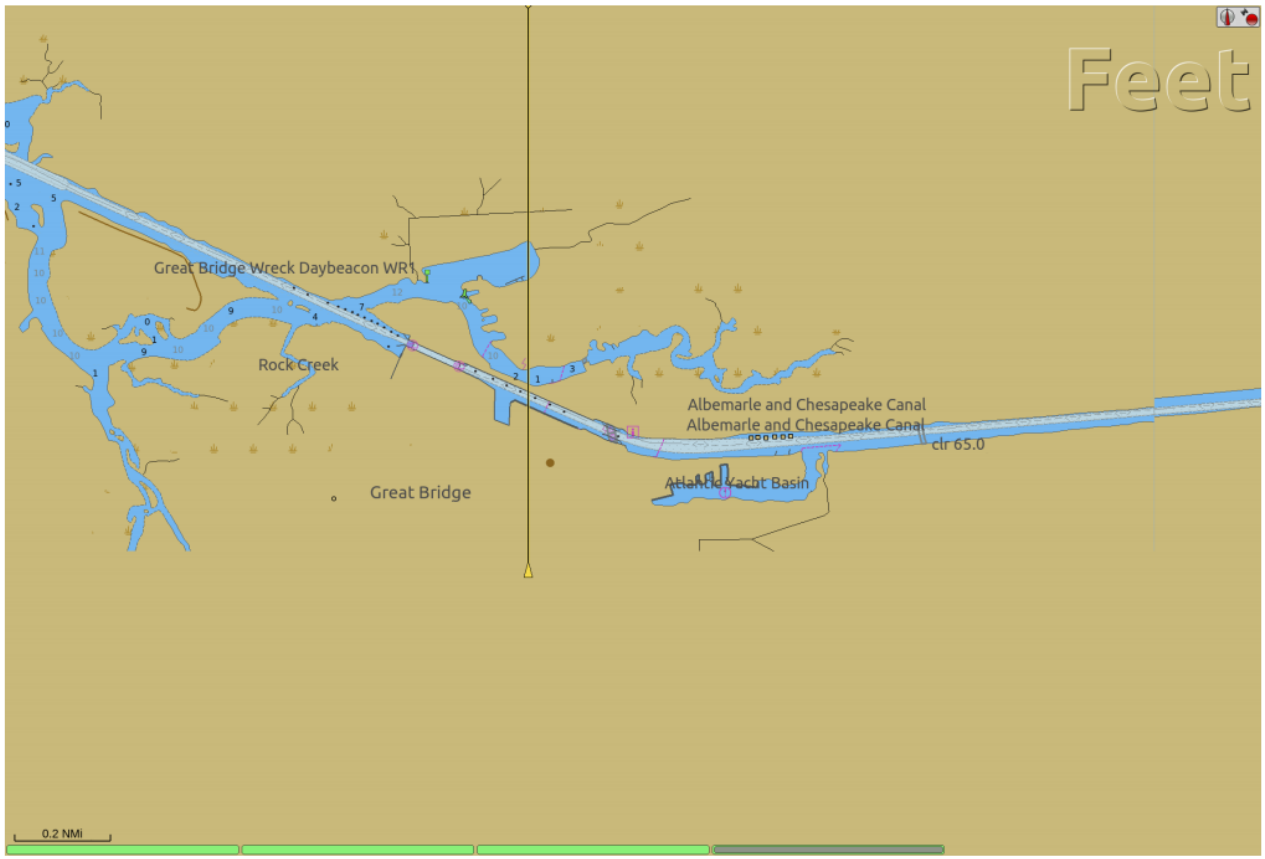
AIS Transmitter



AIS Receiver

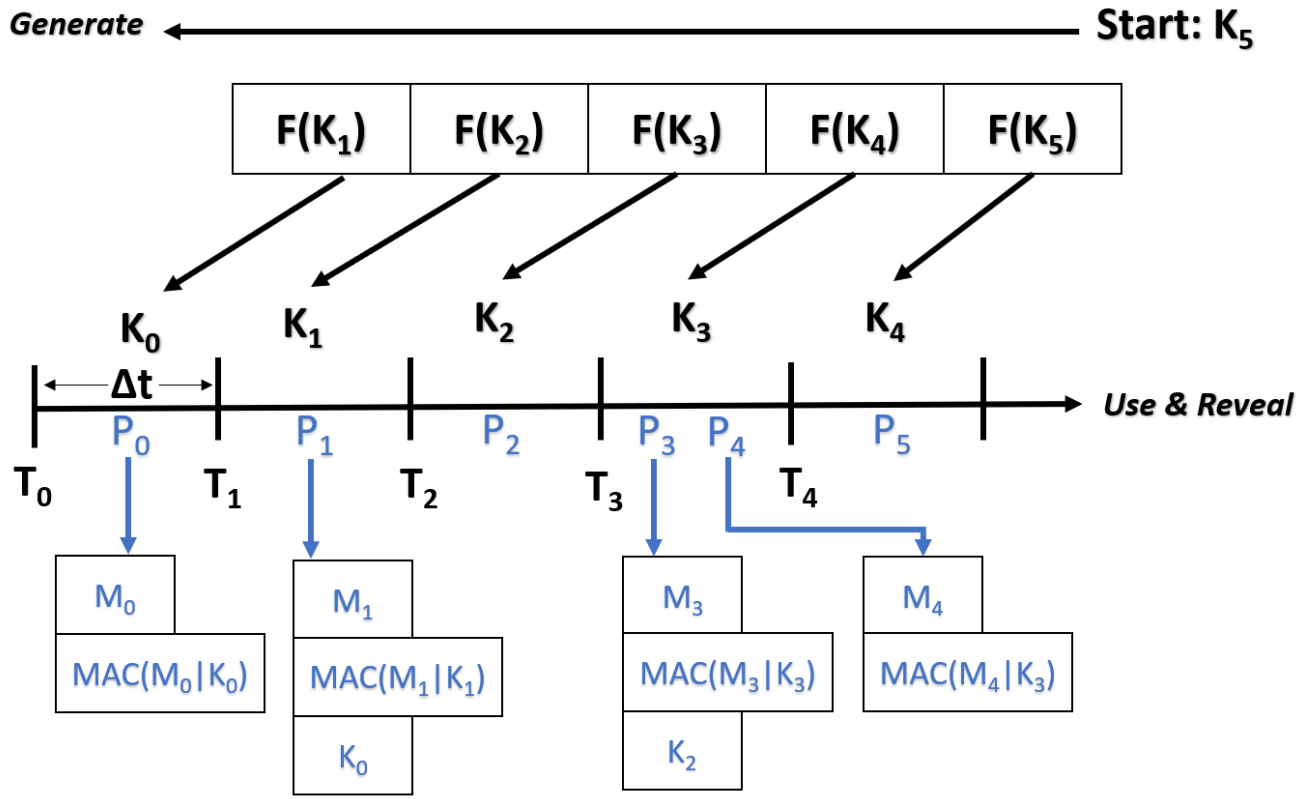


Processing AIS Data



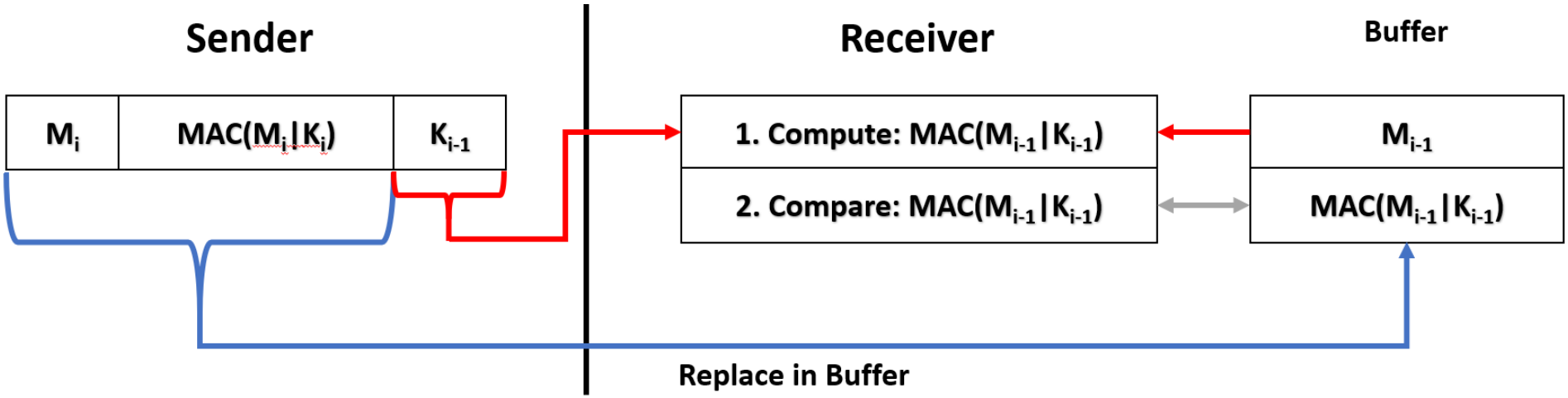
- AIS data stream is sent to named Unix pipe
- GNU AIS program reads the data from named Unix pipe, processes, sends to virtual serial port
- OpenCPN Chart Plotter reads data from virtual serial port

Timed Efficient Stream Loss-Tolerant Authentication Protocol



- Loose time synchronization of users
- PRF: F such that $F(k) = x$, such that given x, k cannot be back-computed and F cannot be distinguished; $F(k)$ will always produce the output x .

TESLA Protocol: Sender Broadcast & Receiver Verification

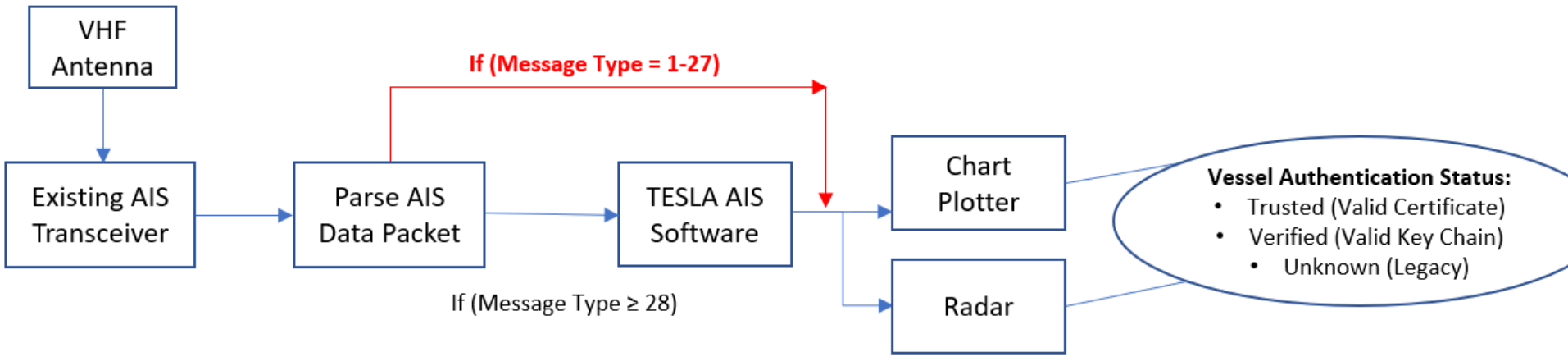


- Broadcast Δt, T_0, as well as the first key in the key chain commitment.
- Receiver must verify that the message was not sent after $T_0 + i * \Delta t$.

TESLA Protocol: Sender Setup

- Choose a random value, K_n to begin a PRF chain of length n.
- Compute initial commitment: $K_{n-1} = F(K_n)$
- Produce remaining keys using F of every value in a chain.
- Loss Tolerance: $K_{n-1} = F(K_n)$, each K is produced recursively using F, then any receiver who receives any K_n value is able to produce all prior key commitments.
- Receiver will be unable to forward-compute any other keys
- Determine Δt, for which each of the K_n will be released,
- T_0, the sender releases first key, K_{n-1}
- Release K_{n-2} at $T_1 = T_0 + \Delta t$, until all keys are released.
- Receiver can derive prior keys using the PRF to validate prior messages.
- Establishes a sound link that all messages came from same source, does NOT authenticate who that source is
- Some form of PKI authentication must occur on at least 1 key chain commitment

Implementation Overview

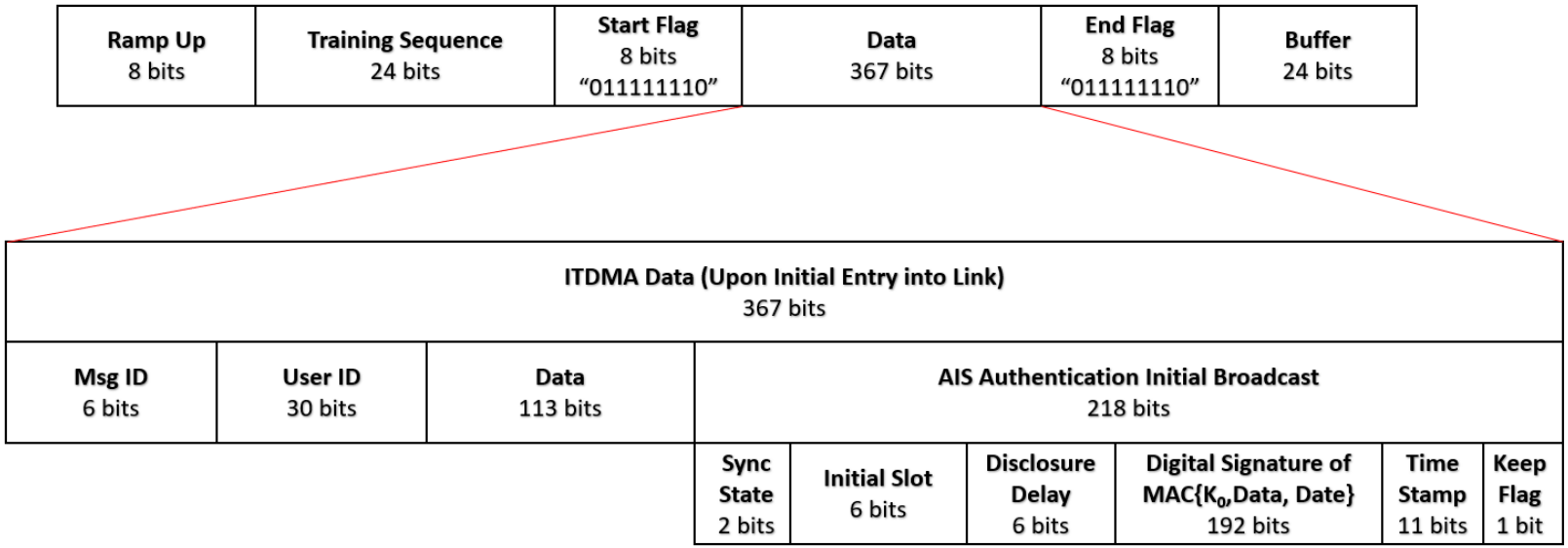


- Embed HMAC containing TESLA-generated key onto AIS messages
- Broadcast key values in subsequent messages
- Periodically provide digital signature to authenticate sender
- Add time stamp to messages
- Can be implemented by adding a software update to the existing AIS software

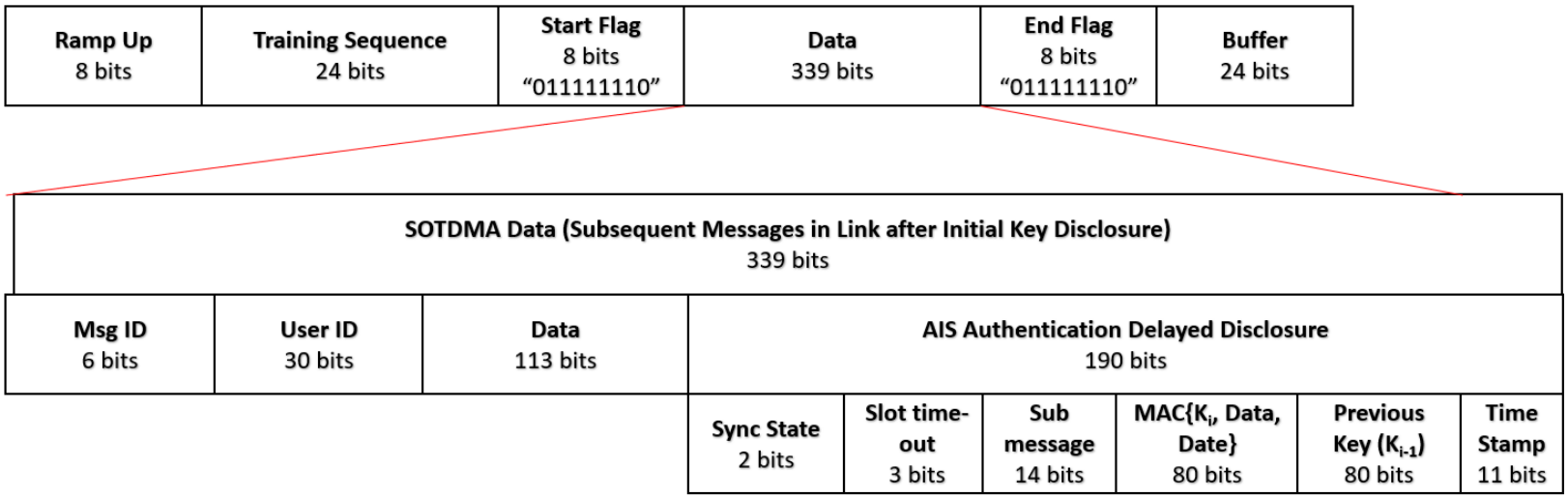
Selecting Δt

- Set $\Delta t = RI$ for all users, implied by receiver
- key disclosure occurs at each vessel's automatic position report.
- Receiver would verify that the received message was sent prior to the NTS (plus a factor of the high bound of the SI).
- Allows for more rapid message authentication at a delay equal to the reporting rate.
- Note: Length N of the authentication hash chain is not a significant factor, only requires $\log(N)$ storage and computation.
- Max RR (2 s): Require 30 keys/min or 1800 keys/hour.
- Using 10 byte keys, storage between 30 bytes and 18 kbytes of data to store. Therefore, storage is not a significant concern.
- Set $\Delta t = RI$ and the chain length, $N = (RR * 60) + 6$, where $126 \leq N \leq 1,806$ (Key chains are recomputed at most once per hour)
- Receiver validates the HMAC, confirming message integrity

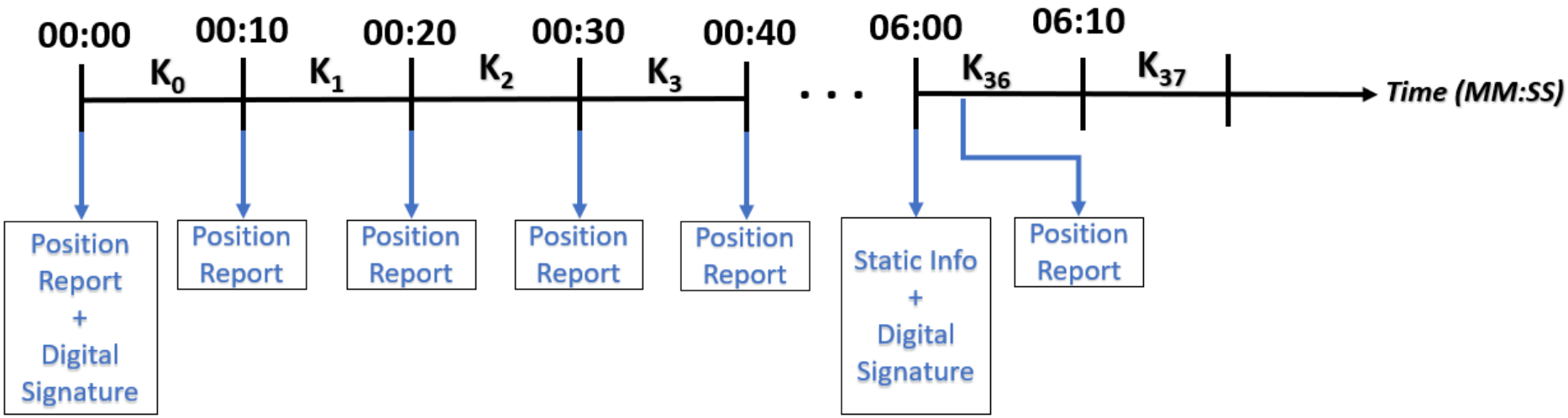
Updated ITDMA Message



Updated SOTDMA Message



AIS with Authentication System Model



The benefits of TESLA AIS system include:

- Resistant to packet loss
- Limited overhead size
- Minor updates to current packet structure
- Can be implemented as a software-only upgrade to existing AIS systems using spare, unused message types defined by ITU

Sender and Receiver Algorithms

- Algorithm 1 $\rightarrow$ AIS Transmitter: Authentication Startup
- Algorithm 2 $\rightarrow$ AIS Transmitter: Broadcasting Authentication Information
- Algorithm 3 $\rightarrow$ AIS Receiver: Authentication Verification

Comparison of AIS Security Protocols

Method	Data Overhead (bits)	Consecutive TDMA Frames	Cryptography	Security Type
Proposed Authentication Protocol (using TESLA)	203 (initial & digitally signed) 171 subsequent	1.5-2	Asymmetric	ECDSA (NIST-192)
Secure AIS w/ IDBE [30]	331, 672, or 768 (depending on security type)	3+	Asymmetric	SS, MNT
SecureAIS – Securing Pairwise Vessel Communications [28]	Not stated; 880 (estimated)	10 (5 per transceiver)	Symmetric	ECQV/ECDH
pAIS (Suggested in [33])	258	2	Asymmetric	RSA
X.509 Certificates (Suggested in [27], [28])	8000+ (estimated)	85	Asymmetric	X.509

- 76.9% – 80% less data overhead and 80% less consecutive TDMA frames than that in [28].
- 38.7% less overhead data for the initial digitally signed message and 48.3% less data for all subsequent messages than [30]
- If digitally signing all Message Type 5 (6 minutes), 42.2% less overhead than [30] and 25.9% less overhead than [33] in an hour (120 messages).

Conclusions

- AIS is an unsecure system and is vulnerable to spoofing, hijacking, and replay attacks; requires authentication, message integrity, and a dedicated time stamp to secure the system
- Presented SDR AIS transmitter and receiver which can be used as a robust test platform for AIS research
- Novel authentication algorithm for the AIS system which is based on the TESLA protocol that enables
- Authenticates users without the use of an a priori shared secret key, no startup message exchanges
- Significantly less overhead than previous solutions, backward compatible with existing hardware.
- Provides for message authentication, integrity, and resistant to replay attacks

Future Work

- Test with existing AIS transceivers
- Analyze the scaling of this system and modeling how it will react in congested waterways with many users
- Further security analysis on signature type/size
- Minimum key size that can be used while still maintaining adequate security of the hash chain
- Output to chart plotters and radar systems since the data this feature provides is ultimately a tool for the use of shipboard personnel
- Reliant upon GPS source for both timing and position data; GPS jamming and spoofing are relatively easy
- AIS message 21 (ATON Report) and message 22/23 (group assignment command) must also include verification that they originated only from a competent maritime authority

Questions?