

# Senior Design Project in Electrical Engineering



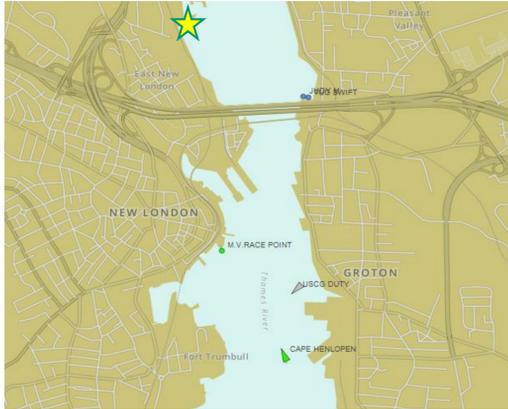
# IEEE 1609 Influenced AIS

Project Leads: 1/c Jordan Lee, 1/c John Hall

Advisors: LCDR Joseph Benin, LCDR Chris Armstrong

Sponsor: C3CEN (Liaison: LT Brock Eckel)

## AIS Spoofing Example



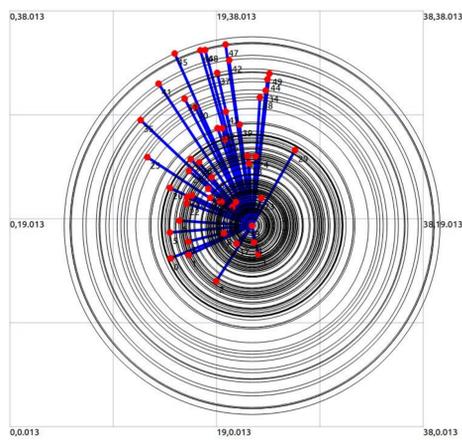
Using our AIS testing platform we were able to generate fake AIS contacts that were reported by numerous internet-based AIS tracking programs as well as the Coast Guard's National AIS and Watchkeeper programs.

## Project Plan

The project parameters and objectives are as follows:

- Develop protocol that allowed for data authentication, confidentiality, integrity, authorization and privacy.
- Demonstrate using C# simulation
  - Broadcast Safety/Navigation Information
  - Request and Transmit Amplified and Full Vessel Information
  - Retrieve Pseudonym from Shore-Side Unit
  - Implement four examples of common spoofing techniques
- Develop NS3 simulation
  - Broadcast Safety/Navigation information.
  - Allow for inter-vessel communication.

## Network Simulation Design



In order to model the macro-behavior of our new protocol in an ideal network, we developed a simulation in NS3. The simulation had the following characteristics:

- Networks were tested consisting of up to 100 vessels and as few as 5.
- All vessels were constantly moving in a random pattern.
- All vessels broadcast their safety information every two seconds
- Directed messages were sent between specific vessels every other second.
- Any vessel that received an amplified information message was then programmed to respond back with a second message, terminating the connection.

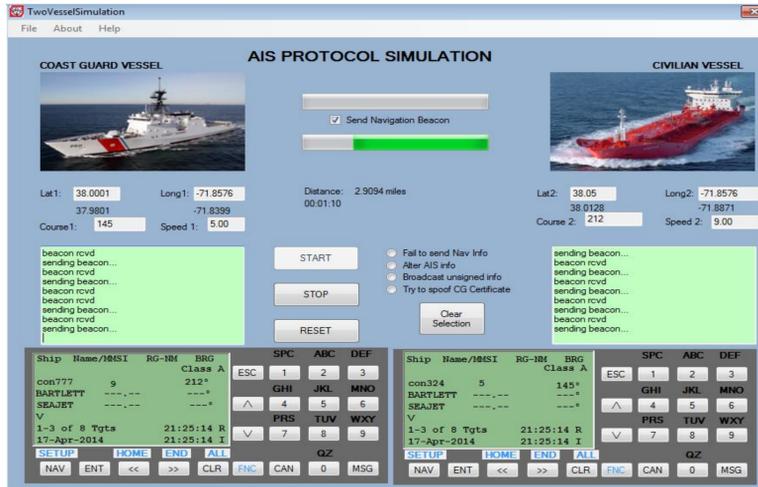
## Project Background

The Automatic Identification System (AIS) is a tracking scheme designed to prevent the collision of vessels at sea. Periodically vessels broadcast their name, position and navigational data to all ships within range. This is used by the maritime fleet to develop a comprehensive view of their surroundings.

Unfortunately, this system is almost entirely unsecure. There are no inherent methods for data validation or authentication. Already, this system has been manipulated by several parties for nefarious purposes and this trend is growing. The purpose of our project is to apply the security methods developed for autonomous vehicular networks to the maritime community.

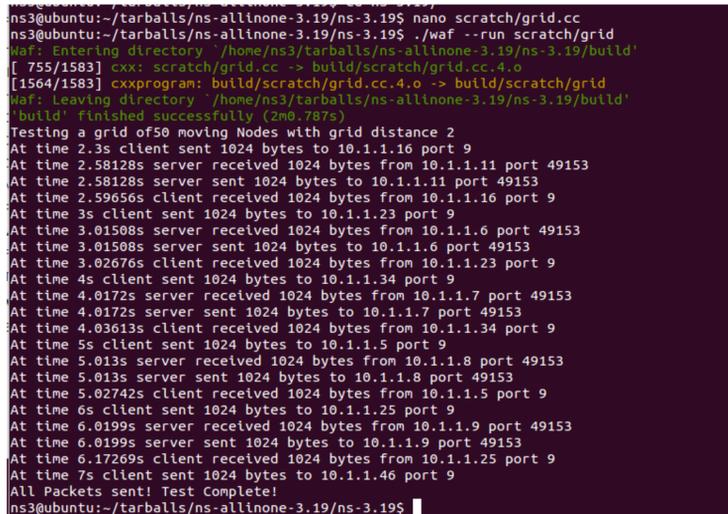
The IEEE 1609 Family of Standards dictates the data format used between cars as they engage in autonomous communication. This system uses assigned pseudonyms to maintain anonymity between cars while still preserving the integrity of their transmissions. We sought to apply these same principals as we constructed our new protocol. We then developed simulations of our new protocol in action to demonstrate their efficacy and security.

## C# Simulation of New Protocol



This simulation, constructed in c#, demonstrates how packets of AIS data will be transmitted between vessels. It also demonstrates how spoofing can be countered by simulating four instances of common spoofing scenarios and demonstrating how our protocol would mitigate them.

## NS3 Simulation of New Protocol



This simulation, constructed in NS3, demonstrates how packets of AIS data will be transmitted between vessels on a network level. It shows the client vessel sending a transmission to the receiving vessel which then responds with a second message. This occurs between multiple vessels over the course of half a minute. At the same time, the vessels are continuously updating the fleet with their navigational data.

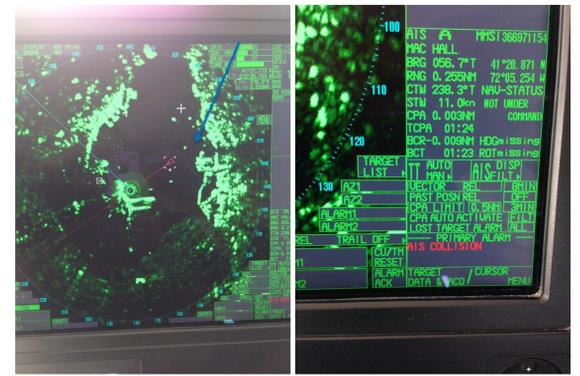
## Results

Our C# Simulation proves that the new protocol can be applied in such a way that a user would experience no degradation of service. Using the new protocol, however, provides the user with more robust security.

Our NS3 simulation proved that the inherent design behind our protocol is sound and that its network implementation is possible.

In aggregate, these simulations prove that our protocol is an effective solution to the security problems brought about by the vulnerabilities inherent in AIS.

## Radar from Bridge of Spoofed Coast Guard Vessel



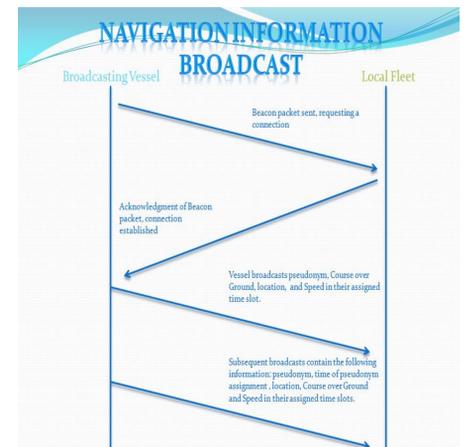
We conducted a field test of our ability to spoof AIS data using our AIS testing platform. We were successfully able to generate a fake contact that was detected by the USCGC Chinook in New London and caused the sounding of an alarm.

## Project Goals

The project goals are as follows:

- Develop a holistic understanding of the current version of AIS and the IEEE 1609 family of standards.
- Perform a vulnerability and security analysis on the current version of AIS.
- Develop a new AIS protocol that utilizes the security features of IEEE 1609 to address any identified deficiencies.
- Develop a C# simulation of the new AIS protocol that displays information a typical user would require.
- Develop a NS3 simulation of the network created by the new AIS protocol.

## Example of an AIS Data Stream



## Full Vessel Information Packet

