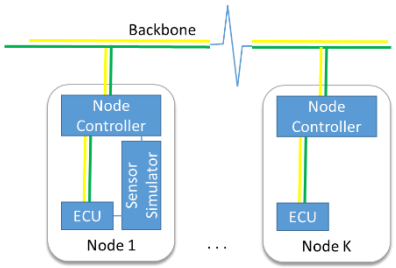
Toward a Test Bed for Heavy Vehicle Cyber Security Experimentation

Challenge:

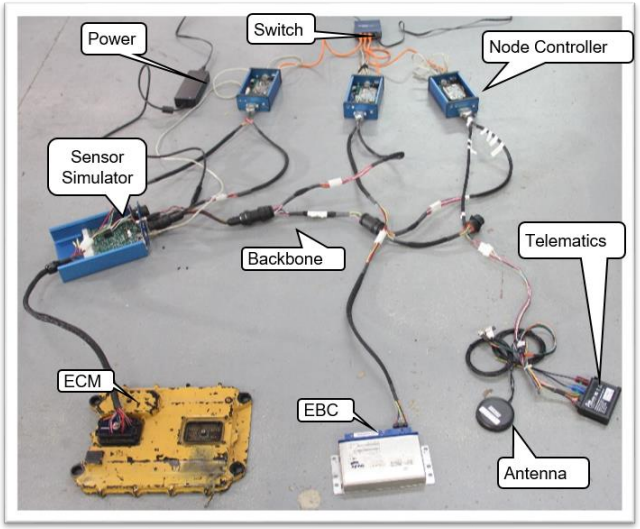
- Access to heavy vehicles for cyber security research is difficult and expensive
  - How can remote access to heavy vehicle systems be enabled for researchers?
- Test theories related to security in a safe and controlled environment
  - How are experiments configured and simulated so that their results are meaningful?
- Bluetooth has been shown to have multiple vulnerabilities
  - Can truck telematics units using Bluetooth be attacked allowing entrance into the CAN?

Solution:

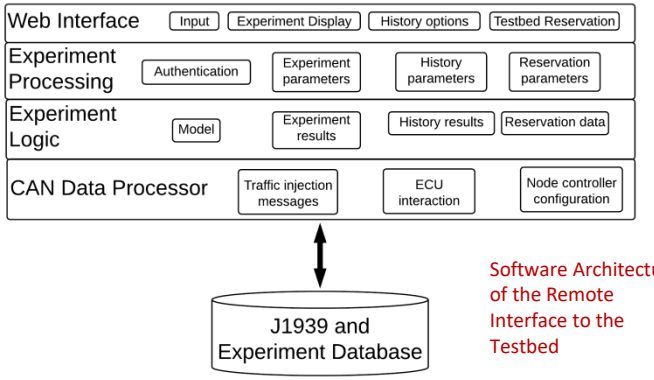
- Create a Heavy Vehicle Test Bed to emulate vehicle sensors and communications
- Create an interface to the test bed to enable remote experimentation
- Research Bluetooth vulnerabilities and their potential presence as attack vectors in telematics units



Testbed concept arrangement with node controllers separating each module from the backbone



Physical layout of a basic testbed



Software Architecture of the Remote Interface to the Testbed

Scientific Impact:

- The test bed and the results of the research, including the potential to extend the test bed with other components, can impact cyber security analysis for other industries that use CAN, such as building automation, medical devices, and manufacturing.

Broader Impact:

- The remote test can be a resource for broad experimentation.
- Experimentation parameters and the data collected can be shared with a community of researchers
- Accessibility and openness can advance CPS security research and also support efforts to conduct other studies in safety and reliability

NSF EAGER CNS-1619690
University of Tulsa
Rose Gamble, gamble@utulsa.edu
Jeremy Daily, jeremy-daily@utulsa.edu