ADAMANT

Real-Time Detection of Man-in-the-Middle Attacks in Industrial Control Systems Using Network Traffic Analysis

ELECOMP Capstone Design Project 2025-2026

Sponsoring Company:

Dependable Cyber-Physical System Lab (DeCPS) at the University of Rhode Island CYPHER Center

2 East Alumni Avenue,

The Fascitelli Center for Advance Engineering Room 470

https://web.uri.edu/decps/

https://web.uri.edu/cypher/

Company Overview:

At the DeCPS Lab (Dependable Cyber-Physical Systems Lab) at the University of Rhode Island CYPHER center, we are dedicated to enhancing the resilience, security, and dependability of Cyber-Physical Systems (CPS) and the Internet of Things (IoT) through cutting-edge networking and system-level innovations.

Our interdisciplinary research lies at the intersection of computer science, computer engineering, and electrical engineering. Core areas of focus include cybersecurity, intrusion detection systems (IDS), CPS, IoT, and software-defined networking (SDN). We actively explore the integration of deep learning, blockchain-based fault tolerance, and other emerging technologies to improve the robustness and intelligence of CPS and IoT infrastructures.

By combining theoretical foundations with practical implementations, our work aims to address critical challenges in next-generation connected systems and foster resilient, intelligent, and secure digital ecosystems.

Technical Director(s):

Dr. Hui Lin
Associate professor
huilin@uri.edu
https://www.linkedin.com/in/hui-hugo-lin-68012b12/

Meem Tasfia Zaman
Graduate research assistant
meemtasfia.zaman@uri.edu
https://www.linkedin.com/in/meem-tasfia-zaman/

Jake Nicynski
Graduate research assistant
jake_nicynski@uri.edu
https://www.linkedin.com/in/jake-nicynski/

Zack Notarianni
Graduate research assistant
zack.notarianni@uri.edu
https://www.linkedin.com/in/zachary-notarianni-26931a275/

Project Motivation:

Industrial control systems like power grids present a unique cyber-physical infrastructure to collect measurement data and perform control operations to ensure continuous stability. Integrating conventional analog physical processes and off-the-shelf computing and network technology increases operational efficiency while presenting a new challenge to maintaining resilience. In recent decades, the increasing adoption of renewable energy sources (RES) relies on various intelligent electronic devices (IED) and invert-based resources (IBR) to couple physical processes.

From traditional power systems to recent smart grids, communications networks are critical in sharing information in this domain. Even though they use similar technology to the public Internet, industrial control communications networks serve unique applications, i.e., sharing information related to physical processes and delivering control commands to maintain their stability. The features add new ingredients to infrastructure and network protocols used by smart grids, which malicious actors can leverage to launch cyber attacks that aim to disrupt smart grids'

physical processes. Unlike cyber attacks targeting general-purpose computing environments, cyber attacks targeting critical industrial control systems introduce unrecoverable consequences, including power outage, economic losses, and even human casualties.

In this capstone project, students will use network traffic analysis to develop a real-time detection method for man-in-the-middle attacks on industrial control systems. This project aims to provide students with hands-on experiences on (i) configuring, deploying, and operating real IED devices used in a wide range of industrial control systems, (ii) ethical hacking technology used by information technology (IT) company, and (iii) state-of-the-art network analysis adopted in cyber security operations. This capstone project is partially sponsored by awards from NSF, DOE, and ONR DOD, in alignment with research performed at DeCPS lab in URI CYPHER center.

Anticipated Best Outcome:

The anticipated best outcome (ABO) of this project is a fully functional detection prototype of implemented man-in-the-middle attacks in industrial control system (ICS), whose overall infrastructure is presented in Figure 1.

ABO1: A fully functional ICS including cyber-physical infrastructures.

Objective: Enables students to obtain a fundamental understanding of cyber-physical interactions in today's ICSs.

Description: if successful, the master node, which is implemented as a Raspberry RI 5 machine, can use network communications to control the outstation node, which is an intelligent electronic relay from Schweitzer Engineering Laboratories SEL) (the model: SEL 751A). The network-based

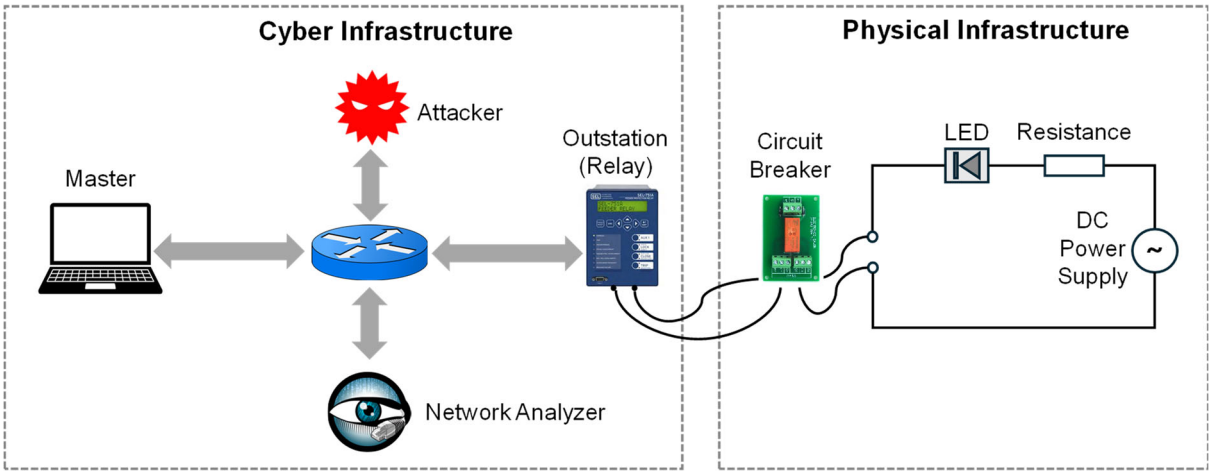


Figure 1. ADAMANT Overview: a detection prototype of implemented man-in-the-middle attack in industrial control systems.

control commands from the master node can change the DC voltage levels from the pins of the SEL 751A, which connect to activation pins of the circuit breaker. These activation pins can control the connectivity of a DC electrical circuit. Consequently, this ABO allows us to control physical circuits through communication networks.

ABO2: A fully functional man-in-the-middle attack through compromising ARP caches in network nodes.

Objective: Enables students to grasp the basic knowledge of cyber attacks in communication networks.

Description: If successful, the attacker can use another Raspberry PI machine connected to the same network router building the ICS systems to issue network commands to compromise ARP caches in master and outstation nodes and perform a man-in-the-middle attack.

ABO3: A fully functional detection module that can detect the implemented man-in-the-middle attacks through network traffic analysis.

Objective: Enables students to obtain in-depth knowledge of network traffic analysis, e.g., deep-packet inspection.

Description: If successful, the network analyzer implemented in the third Raspberry PI machine to monitor network traffic going through the cyber infrastructure of the ICS. The students define and implement their own detection logic based on the extracted network traffic.

The final outcome will be presented at the URI Capstone Design Summit. In addition, the prototype can be presented at the DOD ONR Integrate Product Team (IPT) annual meeting in July 2026.

Activities that go beyond the ABOs may include:

- Leveraging an advanced network traffic analysis tool like Zeek to detect man-in-the-middle attacks
- Measure the network-level performance, e.g., throughput and latency, that is affected by attacks and detections

Project Details:

The objective of this project is to demonstrate the potential vulnerability in intelligent electronic devices commonly used in industrial control systems and state-of-the-art cyber defense prototype through non-intrusive network traffic analysis. The objectives are initiated in three ABOs:

- ABO1: A fully functional ICS including cyber-physical infrastructures
- ABO2: A fully functional man-in-the-middle attack through compromising ARP caches in network nodes
- ABO3: A fully functional detection module that can detect the implemented man-in-the-middle attacks through network traffic analysis

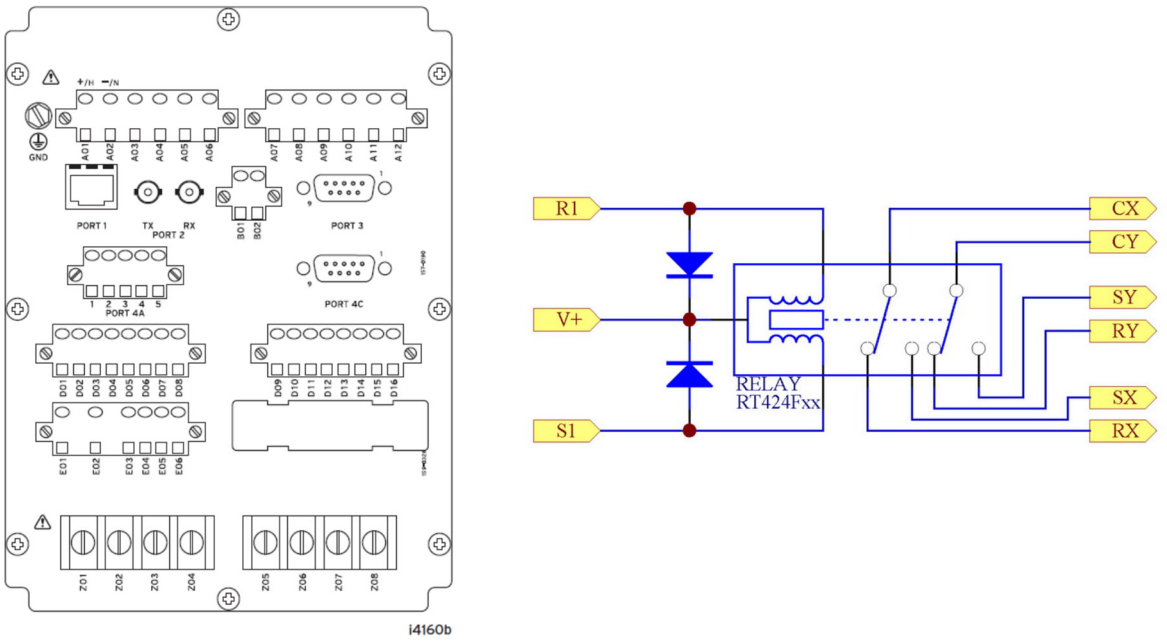
ABO1: A fully functional ICS including cyber-physical infrastructures

The cyber infrastructure is a communication network including two nodes exchanging information based on the standard DNP3 protocol: a master node implemented in a Raspberry PI and an outstation node implemented by an intelligent electronic relay from Schweitzer Engineering Laboratories (the model: SEL 751A). The physical infrastructure is an electrical circuit, whose connectivity is controlled by a magnetic breaker (the model: MD-D262) or SEL751A directly. The cyber and physical infrastructures are coupled by wiring connectivity between GPIO pins in the SEL 751A relay and the magnetic breaker, as shown in Figure 1.

Hardware/Electrical Tasks

The hardware/electrical tasks focused on the implementation of the physical infrastructure of the ICS:

- Connect the SEL 751A relay and MD-D262 circuit breaker to an example DC electrical circuit.
- Study the configuration software, e.g., ACSELERATOR, that is used to configure and control SEL 751A



(a) Rear panel of SEL 751A (b) Electrical schematic of MD-D262 breaker

Figure 2. Example electrical schematic of intelligent electronic devices used in ADAMANT's physical infrastructure.

relay.

- Using the instructional manual of SEL 751A and MD-D262 to implement local control that can activate the connectivity of the electrical circuit (example electrical schematic of those devices are presented in Figure 2).
- Perform initial demonstration of the control of the electrical circuit.

Firmware/Software/Computer Tasks

The computer tasks focused on the implementation of the cyber infrastructure of the ICS:

- Study the fundamental functionality of the DNP3 protocol and simulate network communication based on the DNP3 protocol through the opensource library, e.g., PyDNP3. The high-level network structure of the DNP3 protocol is presented in Figure 3 (the details can be referred to the protocol specification).
- Implement the Master node based on the PyDNP3 to successfully communicate to the SEL 751A relay.
- Successfully demonstrate that the Master node can remotely control the SEL751A relay and MD-D262 circuit breaker.

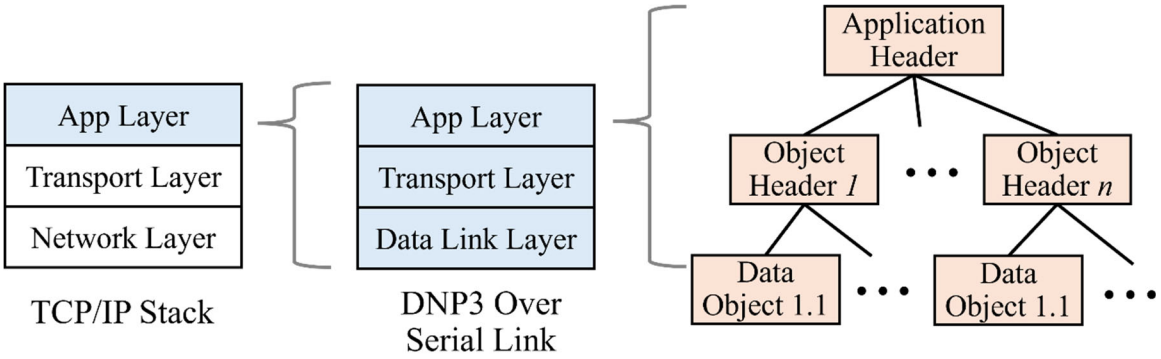


Figure 3. The network structure of the DNP3 protocol built over the TCP protocol.

ABO2: A fully functional man-in-the-middle attack through compromising ARP caches in network nodes

On top of this ICS setup, an attack machine is implemented on a different Raspberry PI machine to successfully perform a man-in-the-middle attack by poisoning the ARP cache in both master and outstation nodes. If the attack is implemented successfully, the attack machine intercepts the communication between the master nodes and the SEL 751A relay. In other words, the attack machine communicates with master nodes pretending to be the outstation node (i.e., the SEL 751A relay) while the attack machine communicates with the outstation node pretending to be the master node.

Firmware/Software/Computer Tasks

Below is general, high-level information that can help students to understand the Address

Resolution Protocol (ARP) and how ARP cache poisoning (often used in "man-in-the-middle" attacks) is typically carried out. **Please note that** *this information is for educational and legitimate testing purposes only (e.g., in a controlled lab environment with explicit permission). Using these techniques on campus networks without authorization is unethical and illegal in many jurisdictions.*

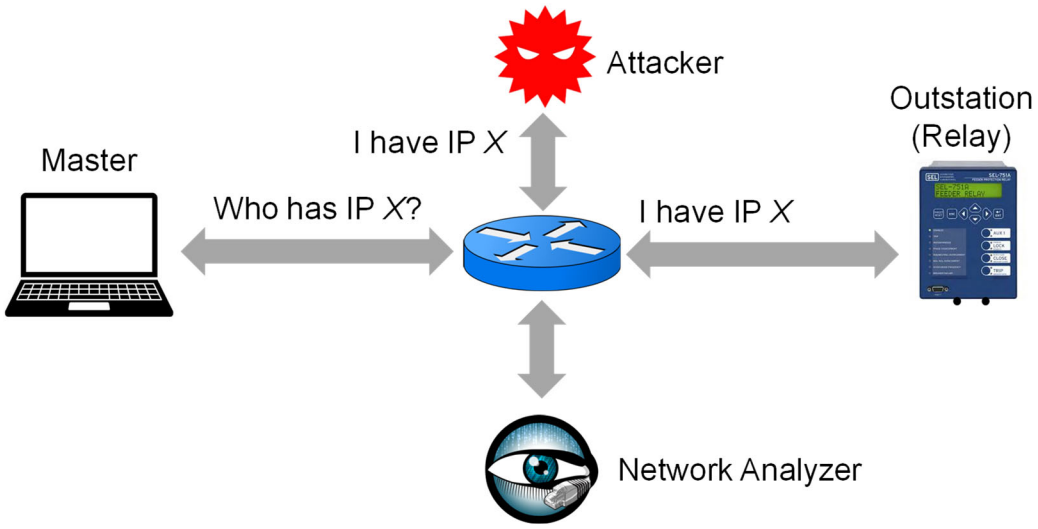


Figure 4. Illustration of the ARP cache poisoning attack and its detection.

ARP (Address Resolution Protocol) is used to map an IP address to a physical MAC (Media Access Control) address on a local network segment (e.g., Ethernet). As shown in Figure 4, when a device (Host *A*) wants to communicate with another device (Host B) on the same network, it generally relies on MAC address for the communication. However, the Host *A* only knows Host *B*'s IP address, which is *X*. Consequently, Host *A* broadcasts an ARP request: "Who has IP *X*? Tell Host *A*." The device with IP *X* responds with its MAC address, and Host *A* then stores this mapping (IP-to-MAC) in its ARP cache. Consequently, when Host *A* communicates with Host *B* in all following interactions, Host *A* uses the information stored in its ARP cache to obtain the corresponding MAC address and use it to target its network packets to Host *B*.

ARP does not have built-in authentication or integrity checks. It assumes that the network's responses are truthful, making it vulnerable to ARP spoofing/poisoning. When Host *A* broadcasts an ARP request: "Who has IP *X*? Tell Host *A,*" the attacker machine, which should be located in the same local area networks as victim machines, sends fake ARP "reply" messages across the network, associating the attacker's MAC address with the IP address of the victim machine, e.g., the Host *B*. Following the same procedure, when Host A attempts to communicate with Host B, it uses the stored ARP cache to obtain the attacker's MAC address and use it to targets its network packets that originally are destined to Host *B* to the attacker machine.

Key Points & Ethical Considerations

Legality: Performing ARP cache poisoning attacks on networks without explicit permission is illegal in many jurisdictions, e.g., URI campus.

Scope: Ensure you only perform such tests on networks you have authority to test (such as a lab setup).

Responsibility: Always alert system owners and follow institutional guidelines for conducting penetration testing or demonstrations in your capstone project.

By understanding these concepts, you can discuss ARP vulnerabilities and illustrate them in a controlled lab environment for your undergraduate project. Make sure to follow ethical guidelines and obtain permission before conducting any tests on real or shared networks.

ABO3: A fully functional detection module that can detect the implemented man-in-the-middle attacks through network traffic analysis

A detection machine, implemented on a third Raspberry Pi machine, relies on state-of-the-art network analysis tools, such as Wireshark, to detect and display the attack procedure, providing information for the system administrator to inform future mitigation measures.

Firmware/Software/Computer Tasks

ARP cache poisoning attacks are common attacks that have been well studied for decades. Many state-of-the-art Security Information and Event Management (SIEM) tools load detection mechanisms by default. In this project, we can implement two detection methods based on network traffic analysis.

- Detect the ARP cache poisoning attacks by identifying multiple ARP responses including different IP-MAC mappings. This is a direct indication of ARP cache poisoning attacks.
- Detect the man-in-the-middle attacks even after ARP cache poisoning attacks become successful. To intercept and modify the network traffic between the master node and the outstation node, the attacker's machine needs to be involved, inevitably introducing additional latency. Consequently, we can continuously monitor the round-trip time between the master node and the outstation node and raise alerts if there are significant changes in the round-trip time.

Hardware/Electrical Tasks

An anomaly in the ICS can also be reflected in the runtime states of the electrical circuit and computer hardware. Consequently, we can implement a web-based dashboard to continuously monitor ICS's runtime states.

- The explicit display of runtime states of ARP cache in both Master and Outstation nodes.

- Build a digital twin of the electrical circuit in an electrical circuit simulation and display its runtime states.

Composition of Team:

2-3 Computer Engineers and 1-2 Electrical Engineers.

Skills Required:

Computer Engineering Skills Required:

- Network programming
- Embedded systems programming
- Familiar with computer networks
- Familiar with basic operating systems and computer architecture
- Python

Electrical Engineering Skills Required:

- Electrical circuit prototype
- Electrical circuit simulation
- Web programming
- Familiar with basic operating systems