ICS/SCADA Device Recognition: A Hybrid Communication-Patterns and Passive-Fingerprinting Approach*

Alaa Al Ghazo[1,2], Ratnesh Kumar[2]

[1]Dept. Electrical and Computer Engineering
University of Hartford, West Hartford, CT 06117

[2] Dept. Electrical And Computer Engineering
Iowa State University, Ames, IA 50010

Abstract

The Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are the backbones for monitoring and supervising factories, power grids, water distribution systems, nuclear plants, and other critical infrastructures. These systems are installed by third party contractors, maintained by site engineers, and operate for a long time. This makes tracing the documentation of the systems' changes and updates challenging since some of their components' information (type, manufacturer, model, etc.) may not be up-to-date, leading to possibly unaccounted security vulnerabilities in the systems. Device recognition is useful first step in vulnerability identification and defense augmentation, but due to the lack of full traceability in case of legacy ICS/SCADA systems, the typical device recognition based on document inspection is not applicable. In this paper, we propose a hybrid approach involving the mix of communication-patterns and passive-fingerprinting to identify the unknown devices' types, manufacturers, and models. The algorithm uses the ICS/SCADA devices's communication-patterns to recognize the control hierarchy levels of the devices. In conjunction, certain distinguishable features in the communication-packets are used to recognize the device manufacturer, and model. We have implemented this hybrid approach in Python, and tested on traffic data from a water treatment SCADA testbed in Singapore (iTrust).

Background

- Homeland security ICS common vulnerability report (2010): many ICS network diagrams /documentation are not up-to-date (do not match the actual systems)
- CRISALIS Report on device fingerprinting (2013): Existing network discovery and fingerprinting tools have a high error rate when applied to ICS/SCADA systems
- **Active fingerprinting** attempts to identify the devices on the network by actively requesting information from the devices
- **Passive fingerprinting** uses a network sniffer to capture traffic already generated by the system devices, and analyzes this traffic to identify the devices.

Contribution

1) To the best of our knowledge, for the first time, a hybrid communication-pattern and passive-fingerprinting
approach is proposed to identify the ICS/SCADA devices' type, manufacturer, and model.
2) To the best of our knowledge, for the first time, the ICS/SCADA communication-pattern is used to identify the device control hierarchy level, and next to determine the device type.
3) The paper identified a set of features in the communication packets that can be used to distinguish among the devices based on their control hierarchy level, while not relying on the availability of special packets such as the SYN packets.
4) We present a software implementation, and its validation

Devices Recognition Hybrid Approach

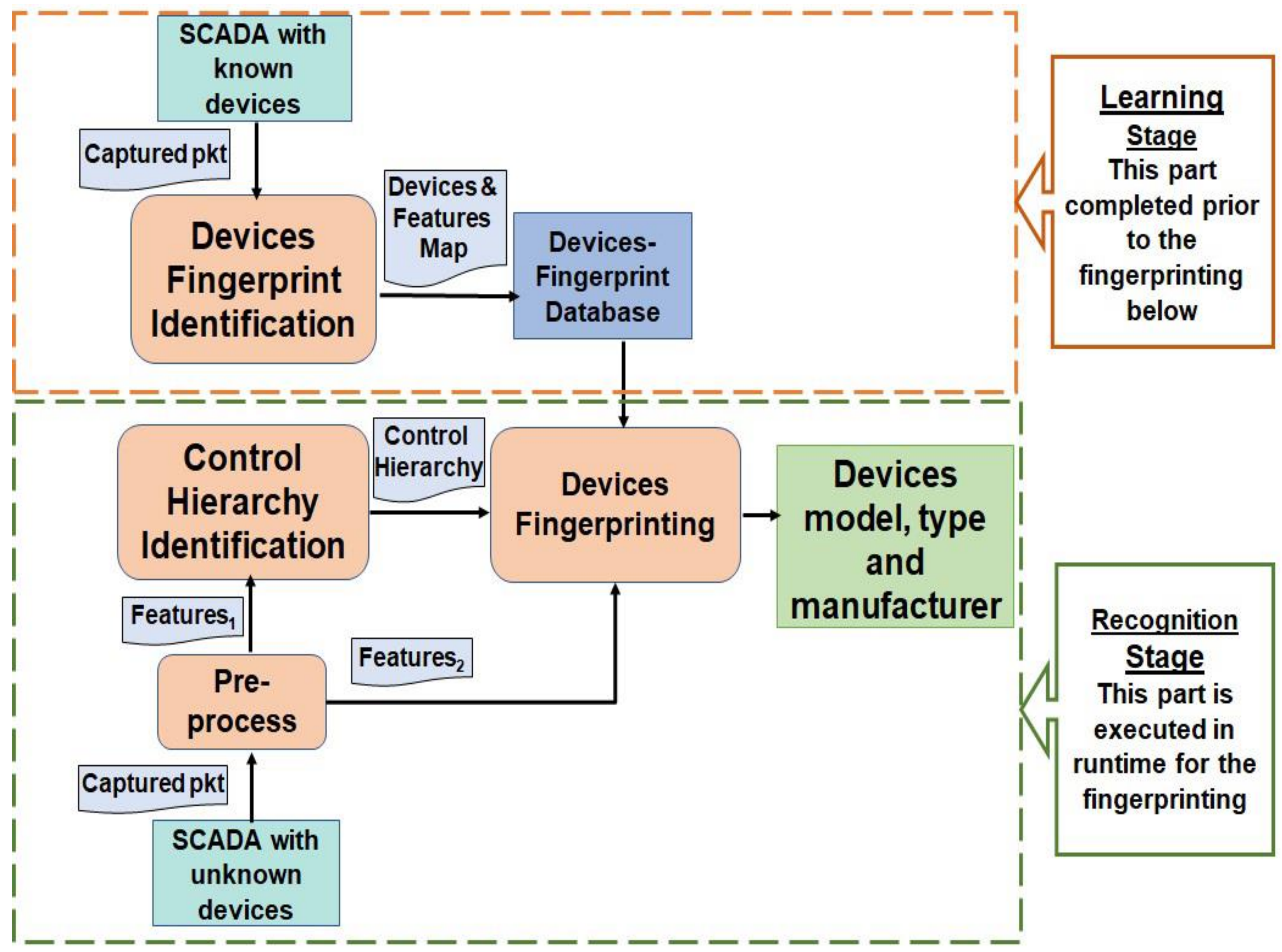

Figure 1: Devices Recognition Hybrid Approach

ICS/SCADA Control Hierarchy

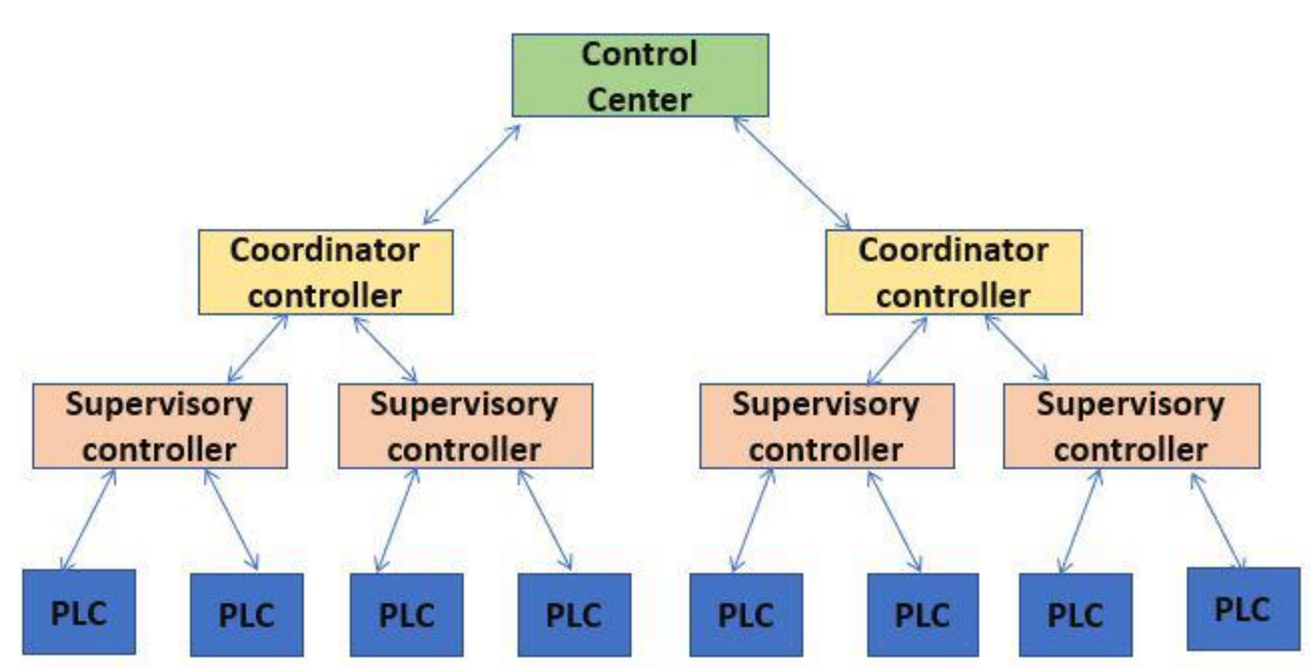

Figure 2: Standard ICS/SCADA Control Hierarchy

SCADA devices fingerprint parameters

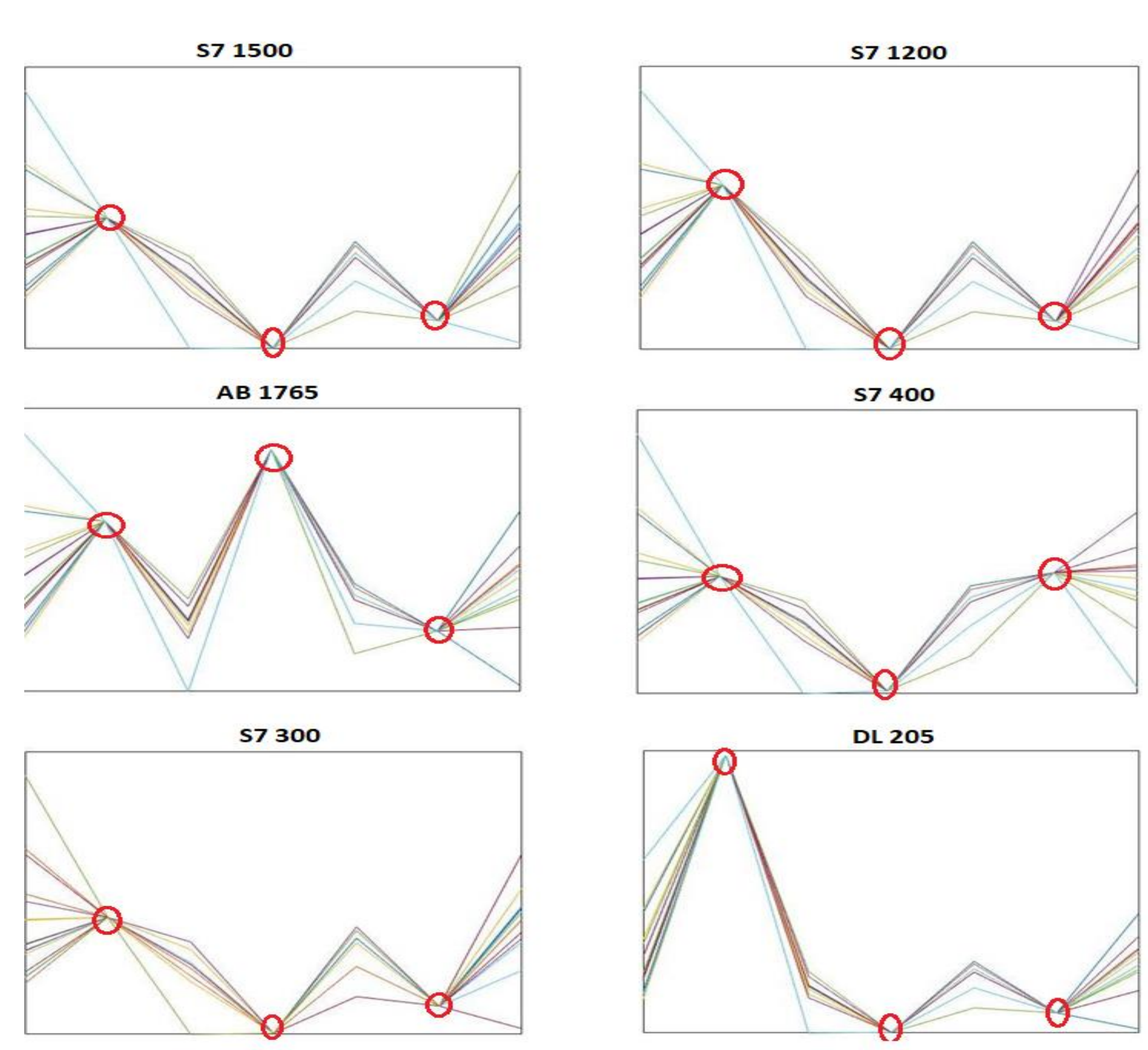

Figure 3: PLCs Data Analysis

Control Hierarchy Identification

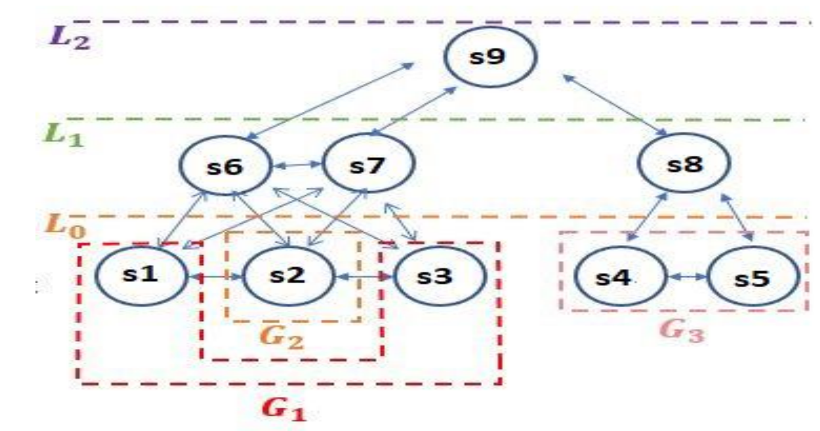

Figure 4: Control Hierarchy Identification example

Case study

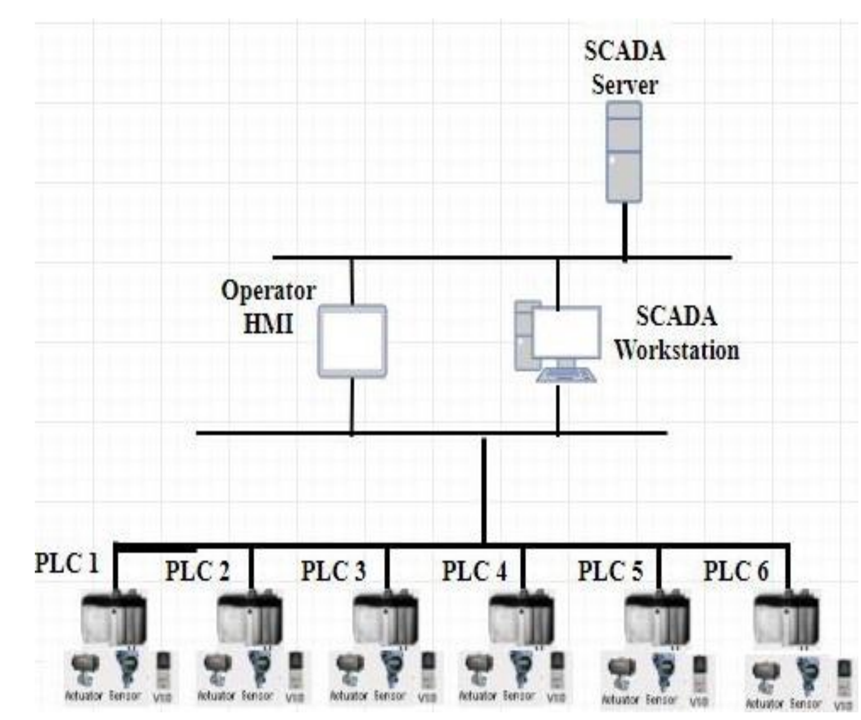

Figure 5. SCADA Architecture of the Water Treatment System

```
----------------------------------------------
L0 groups
g1 = {'192.168.1.10', '192.168.1.20', '192.168.1.30', '192.168.1.40','192.168.1.50', '192.168.1.60'}
L0 = g1
L1+ groups
L1 = {'192.168.1.100', '192.168.1.200'}
L2 = {'192.168.1.201'}
----------------------------
```

Figure 6. Water Treatment CPS control hierarchy identification output

```
------------------------------------------------------
---192.168.1.10 is Allen Bradly Logix 1765 PLC--
---192.168.1.20 is Allen Bradly Logix 1765 PLC--
---192.168.1.30 is Allen Bradly Logix 1765 PLC--
---192.168.1.40 is Allen Bradly Logix 1765 PLC--
---192.168.1.50 is Allen Bradly Logix 1765 PLC--
---192.168.1.60 is Allen Bradly Logix 1765 PLC--
--------192.168.1.100 is Allen Bradly HMI-------
--------192.168.1.200 is SCADA Station----------
--------192.168.1.201 is SCADA Station----------
--------------------------------------------------------
------------------------------------------------------
```

Figure 7. Water Treatment CPS device recognition output

Future Direction

Discovering the devices included in ICS/SCADA systems is an essential first step toward improving their overall cybersecurity.

A next step would be to implement the proposed approach along with systems security analysis and mitigation tools, to enhance their overall security and defense strategies against potential cyberattacks.

* This paper was published in FIP/IEEE IM 2019