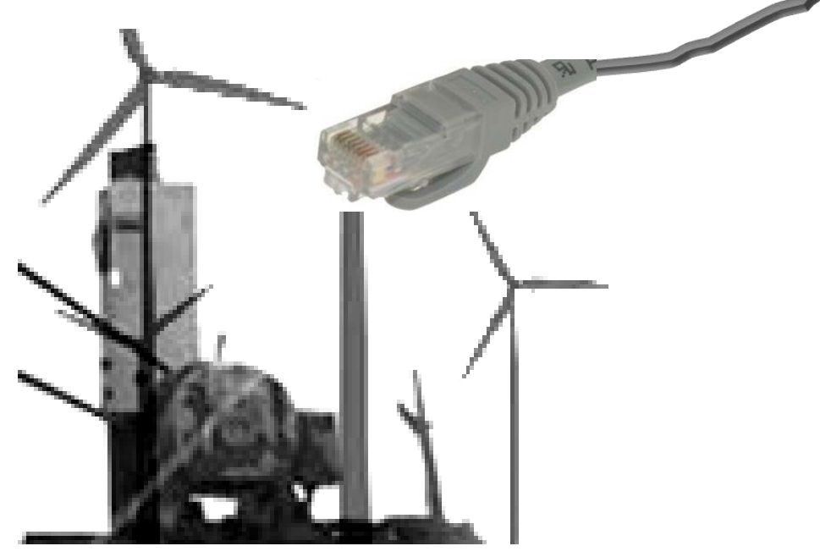
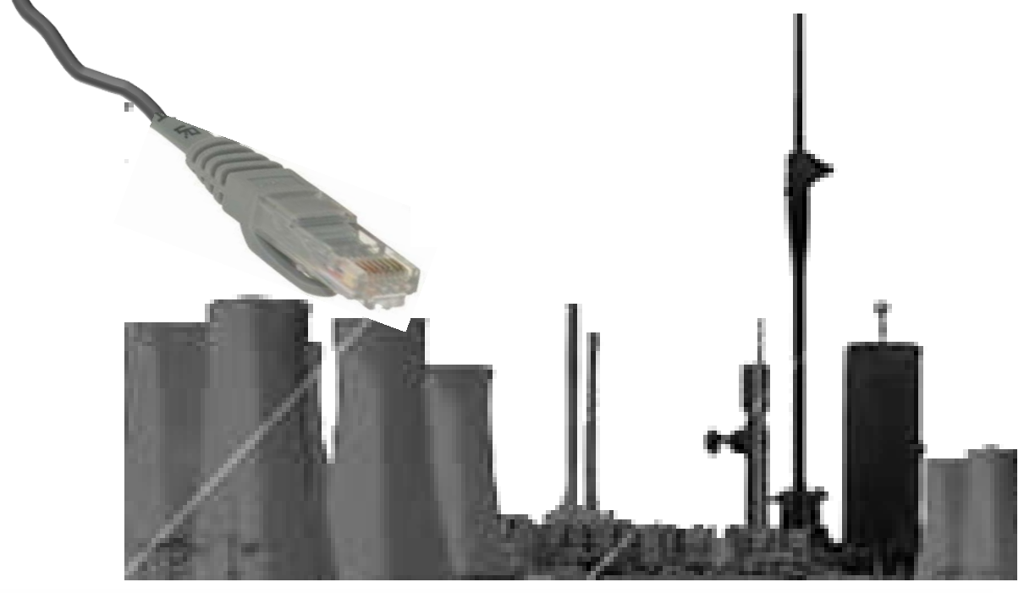


SCADA ACTIVITY PROFILE

Improving SCADA Security with Context-aware Network Profiling

Dina Hadžiosmanović*, Robin Sommer†‡, Damiano Bolzoni*, Pieter Hartel*
University of Twente, Enschede, The Netherland,
†International Computer Science Institute, Berkeley, ‡Lawrence Berkeley National Laboratory, Berkeley, CA, USA



PROBLEM

Common approaches for describing SCADA network operation are too coarse:

- flow-based analyses such as [1] cannot distinguish different types of protocols messages;
- protocol-level analyses such as [2][3] focus on the preferred usage of protocol parameters but cannot capture patterns of data communication.

IDEA

Use application-layer context to interpret SCADA commands:

1. **Extract details of process operations from the network level,**
2. **Find patterns of usual SCADA activity,**
   e.g., track memory access patterns for SCADA devices.

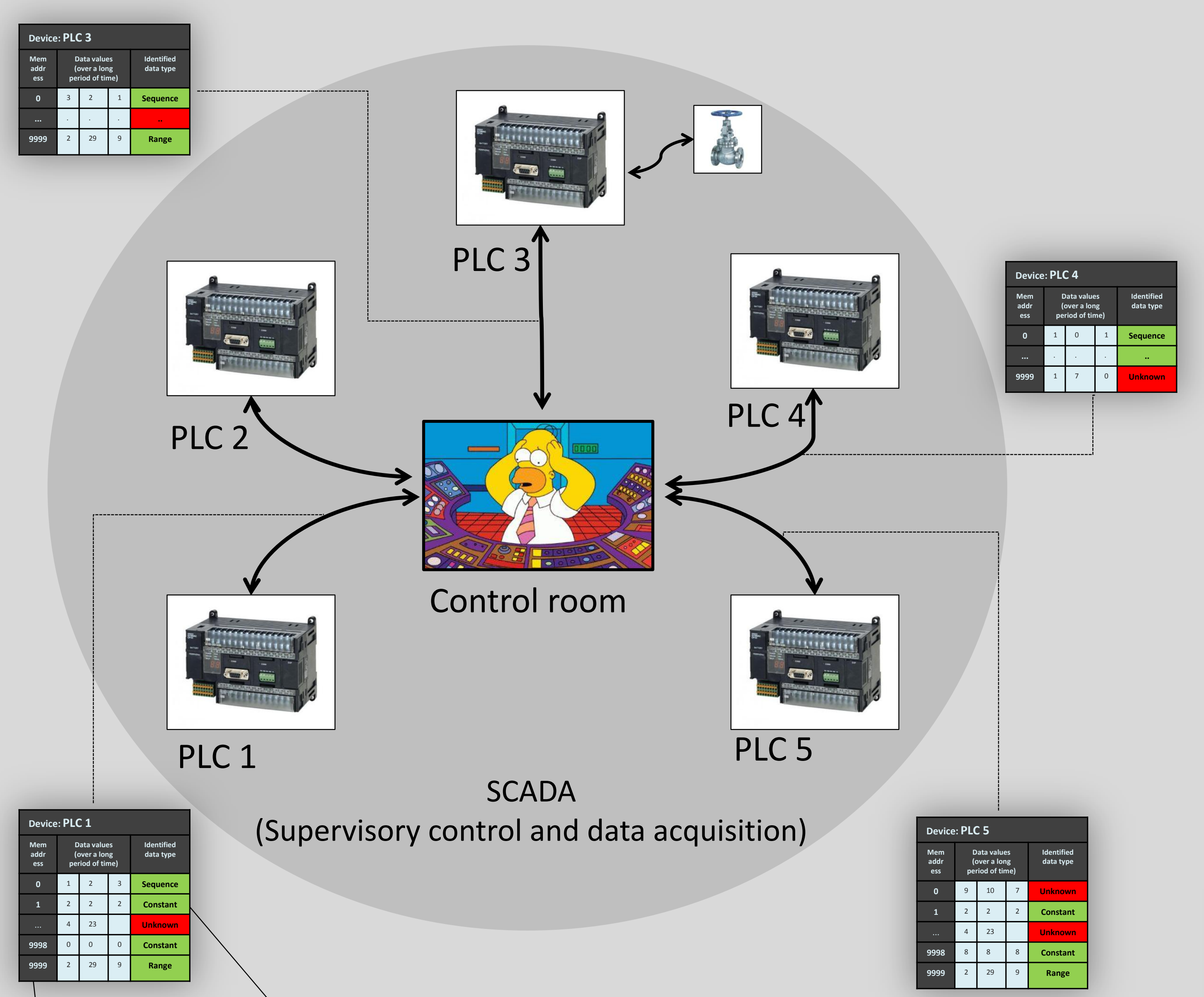
$$\underbrace{\hphantom{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}}$$

LEVERAGE HIGH LEVEL PROCESS SEMANTICS TO DETECT DEVIATIONS

ENVIRONMENTS & DATA

- 5 real-life SCADA facilities that perform purification and distribution of water and gas,
- Up to 50 days of network traces with about 20 devices per facility,
- Typical protocols include: Modbus, MMS, IEC 104.

APPROACH

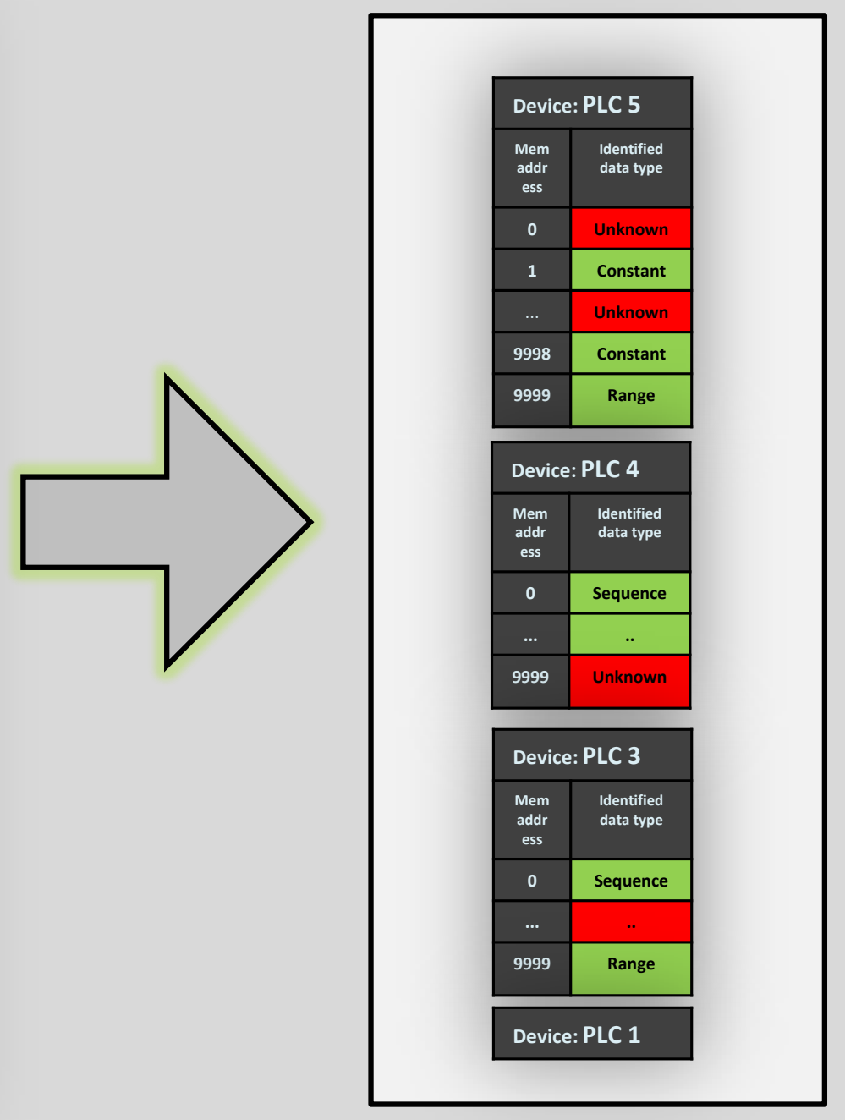


SCADA
(Supervisory control and data acquisition)

Device: PLC 1

Mem address	Data values (over a long period of time)						Identified data type
0	1	2	3	4	5	...	Sequence
1	2	2	2	2	2	...	Constant
2	59	7655	3	456	28	...	Unknown
2	56	52	57	51	58	..	Range
...	61	63	65	67	69	...	Sequence
...	4	237	56	134	1	...	Unknown
9998	0	0	0	0	0	...	Constant
9999	20	29	29	28	26	...	Range

Mapped patterns of memory access for one device (PLC1)



Aggregated profiles of access patterns for SCADA devices

1. Use Bro [4] framework to parse network traffic;
2. Reconstruct the usage of memory locations for each device in the network;
3. Identify addresses which store "predictable" data types (ranges, sequences, constants,...) ;
4. Use labelled addresses to profile usual operation across the network;
5. Monitor for deviations.

PRELIMINARY ANALYSES

- Identified relevant classes of attacks;
- Processed around 10h of Modbus network traffic across several days in 2 different real-life facilities consisting of 20 devices with 5000 active memory locations per device;
- Tests show that 70-80% of memory locations on each device store "predictable" data types;
- The approach appears promising for modelling the majority of SCADA devices in a network.

FUTURE CHALLENGES

- Track relationships between read and write operations ;
- Explore patterns of different address granularity
- Extend the approach to other SCADA protocols, such as MMS and IEC 104;
- Generalize approach beyond memory tracking.

REFERENCES

[1] Alfonso Valdes and Steven Cheung. Communication pattern anomaly detection in process control systems. In 2009 IEEE International Conference on Technologies for Homeland Security, Waltham, MA, May 11–12, 2009.
[2] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. Using model-based intrusion detection for SCADA networks. In Proceedings of the SCADA Security Scientific Symposium, 2007.
[3] Tofino. Tofino security appliance, accessed March, 2012. https://www.tofinosecurity.com/products/tofino-security-appliance.
[4] Vern Paxson. Bro: a system for detecting network intruders in real-time. Comput. Netw., 31:2435–2463, 1999.

UNIVERSITY OF TWENTE.

ICSI
INTERNATIONAL COMPUTER SCIENCE INSTITUTE