Cybersecurity for Control Systems

Almgren M.[1], Aoudi W.[1], Ekstedt M.[3], Iqbal A.[3], Lin C.[2], and Nadjm-Tehrani S.[2]

[1]Chalmers University of Technology
[2]Linköping University
[3]KTH Royal Institute of Technology

Problem statement

Control systems used in critical infrastructures such as the electricity grid, gas distribution, and water treatment plants, are increasingly dependent for their functioning on Information and Communication Technology (ICT) solutions which poses new challenges pertaining to cyber-security. Recent incidents have shown that Industrial Control Systems (ICS), encompassing several types of control systems including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DSC), and Programmable Logic Controllers (PLC), are increasingly exposed to sophisticated and targeted attacks. Recent deliberate disruptions of the ICT capabilities demonstrate that cyber-attacks can have a significant impact on these critical systems. The power outage cyber-attack in Ukraine [4], the Stuxnet attack on an Iranian nuclear plant [2], the German steel mill cyber attack [3], and the Maroochy water breach [5] are just a few cases in point. RICS is a Swedish research center on Resilient Information and Control Systems that aims at increasing the competence in the area of ICT security for critical infrastructures, and will contribute to improved security through better understanding of the vulnerabilities and risks of such systems. The research in RICS will rest on the three pillars: data analysis and emulation, risk and vulnerability analysis using attack modelling, and real-time detection of adverse events and anomalies.

RICS-el reference model

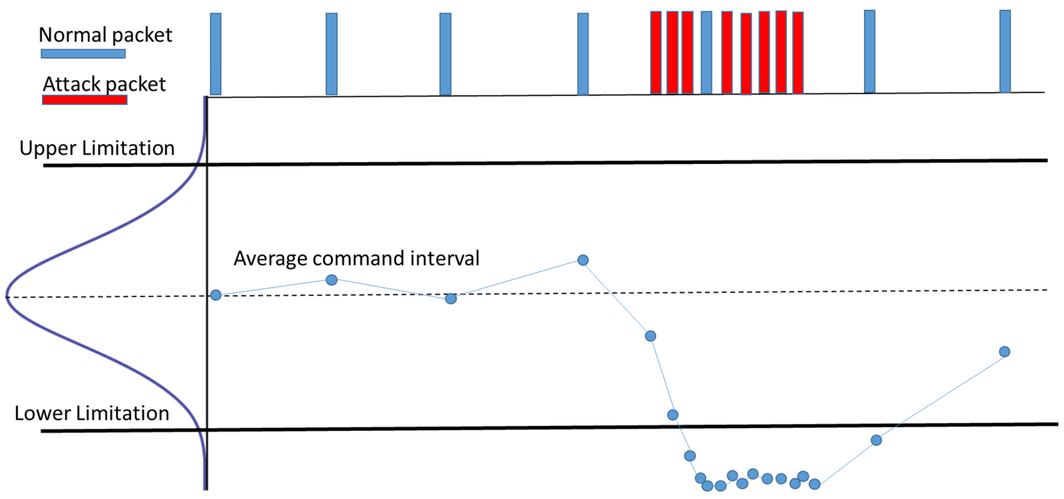
The increasing use of intelligent devices in Critical Infrastructures (CI) has enabled a lot more functionalities within several domains that have several evident advantages. However, the same automation also brings challenges when it comes to malicious use, either internally or externally. One such challenge is to attribute an attack and ascertain what was its starting point, who did what, when and why.

Creating a reference model (RICS-el) of a typical IT infrastructure of an office network of a power utility company along with an implementation in FOI's Cyber Range And Training Environment (CRATE) [1], and connecting this reference model with a SCADA system, and then using this whole infrastructure as a testbed to study cyber-security will certainly help in understanding cyber-security for such an environment.

Using the RICS-el reference model as a benchmark and by conducting cyber attacks, we will generate valuable data. Such a testbed will help in conducting further research to better understand cyber-security in critical infrastructures. Furthermore, the model will help us identify vulnerabilities for assets that are essential for the operation of such systems, and develop methods for protecting these assets.

Network-based anomaly detection

Compared with standard information and communication systems networks, ICS networks exhibit more stable and persistent communication patterns since their communications are usually triggered by polling mechanisms. Typically, a master device periodically retrieves certain data from field devices such as PLCs in order to provide a real-time view of the industrial processes. Commands to trigger certain processes can also occur at predictable times.

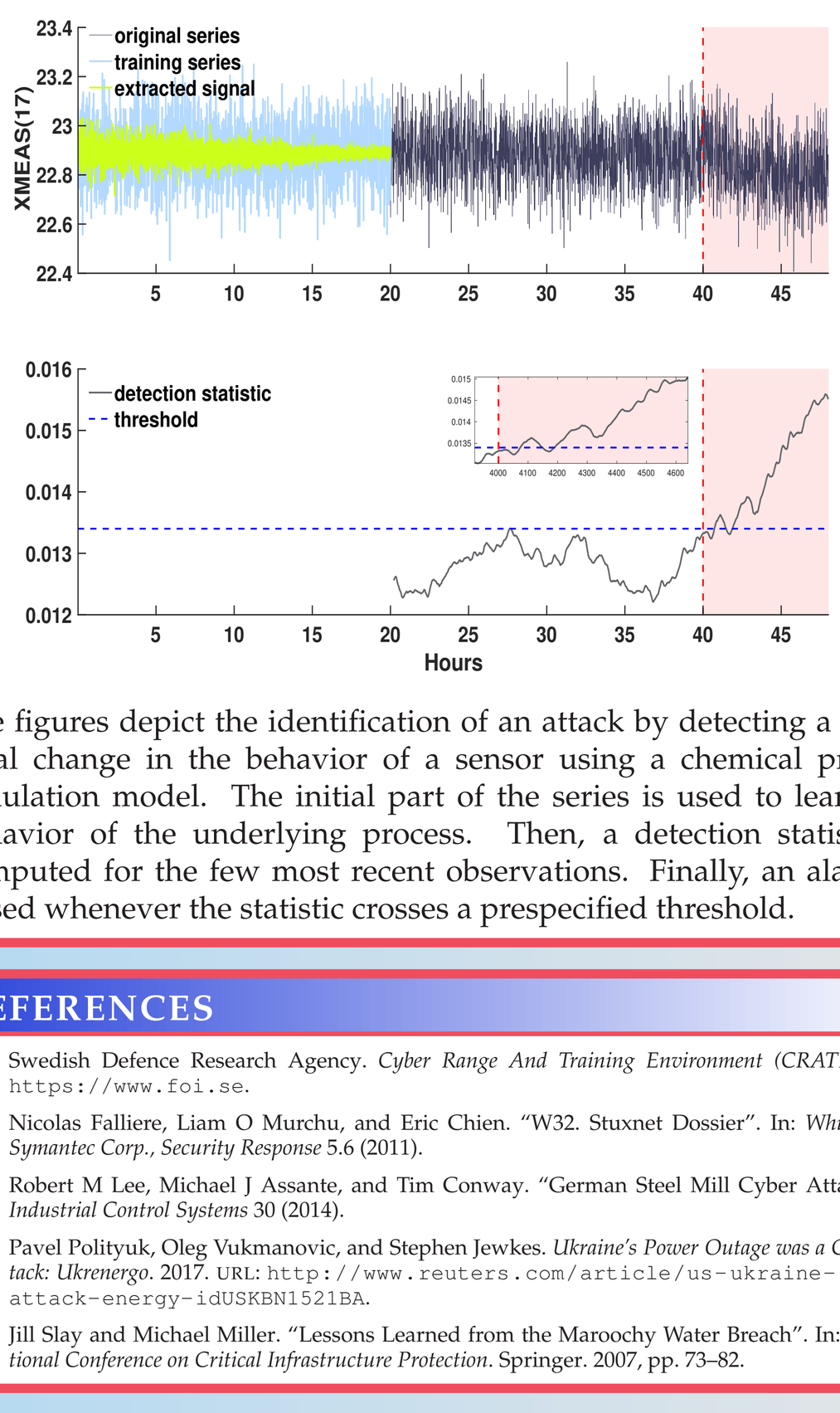


For example, in water utilities, the master device may need to send such commands as "Turn on pumps" everyday at 9:00PM, accounting for the increased demand of water. Therefore, anomaly detection techniques targeting the timing behaviors have been the focus of many researchers to advance the ICS security. The figure shows how an anomaly detector exploiting sampling distribution of mean detects flooding attacks.

Physics-based attack detection

One fundamental difference between a classical IT-based system and an ICS is that the latter interacts with the physical world by controlling a physical process. The incorporation of cyber elements in controlling the physical process introduces new security challenges. In response to these challenges, in recent years, there has been a growing interest in developing complementary intrusion detection capabilities that can detect attacks at the process level.

Recent research has shown that by closely monitoring the behavior of the physical process, it is possible to detect intruders that manage to circumvent the security measures implemented at the IT-infrastructure level. Tools from statistics and time-series analysis can be used to learn or model the underlying physical process from observed data, and subsequently detect *structural changes* in its behavior.



The figures depict the identification of an attack by detecting a structural change in the behavior of a sensor using a chemical process simulation model. The initial part of the series is used to learn the behavior of the underlying process. Then, a detection statistic is computed for the few most recent observations. Finally, an alarm is raised whenever the statistic crosses a prespecified threshold.

References

[1] Swedish Defence Research Agency. *Cyber Range And Training Environment (CRATE)*. URL: https://www.foi.se.

[2] Nicolas Falliere, Liam O Murchu, and Eric Chien. "W32. Stuxnet Dossier". In: *White paper, Symantec Corp., Security Response* 5.6 (2011).

[3] Robert M Lee, Michael J Assante, and Tim Conway. "German Steel Mill Cyber Attack". In: *Industrial Control Systems* 30 (2014).

[4] Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes. *Ukraine's Power Outage was a Cyber Attack: Ukrenergo*. 2017. URL: http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.

[5] Jill Slay and Michael Miller. "Lessons Learned from the Maroochy Water Breach". In: *International Conference on Critical Infrastructure Protection*. Springer. 2007, pp. 73–82.

Acknowledgment

The research leading to these results has been mainly supported by the Swedish Civil Contingencies Agency (MSB) within the Centre for Resilient Information and Control Systems (RICS).