On the Adaptation of Physical-layer Failure Detection Mechanisms to Handle Attacks against SCADA Systems

Jose M. Rubio-Hernan* Joaquin Garcia-Alfaro*

October 12, 2014

Abstract

Supervisory Control and Data Acquisition (SCADA), is a technology to monitor industrial and critical infrastructures. The SCADA technology was conceived for centralized and isolation processes. Nowadays, it is more distributed and vulnerable to cyber attacks. SCADA systems are typically composed of three well-defined types of field devices: 1) Master Terminal Units (MTUs) and Human Machine Interfaces (HMIs), located in top and managing all communications; 2) Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), which control and acquire data from remote equipment and connect with the master station; and 3) sensors and actuators, which act as the input and output functions of the system.

Threats to SCADA systems can target the lower layers. For instance, replay and integrity attacks to alter the state estimation conducted by PLCs, actuators and sensors. Given the difficulty of handling such threats at the upper layers, detection and protection against malicious activities must be conducted at the lower layers themselves.

Several approaches in the literature propose the adaptation of physical-layer failure detection mechanisms (e.g., systems for the detection of faults and accidents) to handle malicious attacks (e.g., replay and integrity attacks conducted by malicious adversaries) [1, 2, 3]. This talk will elaborate on such approaches, and will discuss about some of their limitations. Some conclusions and perspectives for future work will be presented.

References

[1] Yilin Mo and Bruno Sinopoli. “Secure Control Against Replay Attacks.” 47th Annual Allerton Conference on Communication, Control, and Computing, pp. 911–918, 2009.

[2] Yilin Mo, Rohan Chabukswar and Bruno Sinopoli. “Detecting Integrity Attacks on SCADA Systems.” IEEE Transactions on Control Systems Technology, 22(4):1063–6536, 2014.

[3] Yannis Soupionis, Stavros Ntalampiras and Georgios Giannopoulos. “Faults and Cyber Attacks Detection in Critical Infrastructures.” 9th International Conference on Critical Information Infrastructures Security, *to appear*, 2014.

*Telecom SudParis, CNRS Samovar UMR 5157, 91000, Evry, France Email: {jose.rubio_hernan,joaquin.garcia-alfaro}@telecom-sudparis.eu.