Timing-based Anomaly Detection in SCADA Networks

Chih-Yuan Lin, Simin Nadjm-Tehrani and Mikael Asplund

[1] Linköping University, Linköping, Sweden
{chih-yuan.lin, simin.nadjm-tehrani, mikael.asplund}@liu.se

Keywords: SCADA system, Anomaly detection, Traffic periodicity.

Abstract. Supervisory Control and Data Acquisition (SCADA) systems operating our critical infrastructure are becoming increasingly depend on information and communication technologies and being connected to the Internet. These pose new challenges related to cyber security while allowing improved flexibility and ease of use of the systems. SCADA systems exhibit more stable and persistent communication patterns since most of the traffic is generated by polling mechanism. Typically, a master device retrieves data from field devices such as Programmable Logical Controller (PLC) periodically in order to provide 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 for water.

We propose a timing-based anomaly detection in SCADA networks by monitoring statistical attributes of traffic periodicity. Our approach uses sampling distribution of the mean and the range to model the inter-arrival times of repeated events in the same master-PLC communication channel. This work was completed within RICS: the research centre on Resilient Information and Control Systems (www.rics.se) financed by Swedish Civil Contingencies Agency (MSB). In this talk a short description of the following contributions is presented:

- We analyze the periodicity of SCADA traffic collected from real and simulated systems and show that the traffic periodicity exits in both request and response direction including some asynchronous events.
- We study a number of attack scenarios being formed of only valid requests/responses but breaking the traffic periodicity.
- We explore sampling distribution approaches for timing-based anomaly detection and show the proposed IDS can detect both the change of mean and dispersion of request/response inter-arrival times even though the change is small in every single inter-arrival time.