Harnessing the Unknown in Advanced Metering Infrastructure Traffic

Valentin Tudor (tudor@chalmers.se)
Chalmers University of Technology

May 19, 2015

Summary

Due to security and privacy concerns, the communication between the AMI devices is encrypted, making it more secure against malicious third parties but also obscuring the ability of the network owner to detect any misbehaving user or equipment. We are investigating how to balance the need for confidentiality with the need to monitor the AMI which is important in the context of developing intrusion detection solutions for the AMI. We develop one important component for an AMI Intrusion Detection System (IDS), which we call the *Encrypted Command Recognition (ECR)* sensor (depicted in Figure 1). ECR's purpose is to accurately determine the individual commands that are passed in an encrypted or hard to parse form in an AMI communication network. This is done in a privacy-preserving fashion, without decrypting the traffic and without accessing the sensitive data transmitted in the AMI communication network.

We analyze the characteristics of the devices in the AMI and based on their functionality, communication patterns and protocols we extract a set of features that characterize the communication protocols used. Compared with the classical ICT domain, where the human being is the communication initiator and modeler through his interaction with the computer systems, in the AMI the communication is mainly initiated automatically, by the devices themselves. Even though a human operator sometimes would manually query AMI devices, the largest volume of the communication follows certain patterns, as the automatic readings will take the majority of the traffic exchanged while the maintenance commands might be concentrated in a fixed time period. These extracted features are used to create a classifier with the help of supervised learning and we study its efficiency on traffic captured in a realistic AMI testbed. We focus on two AMI protocols, one which is encrypted and one which is difficult to parse due to its proprietary implementation.

The ECR module can become an important component of a distributed IDS for the AMI environment and it will give the operator a better view on the status of his network and help in the early detection of possible misbehaviors and even attacks.

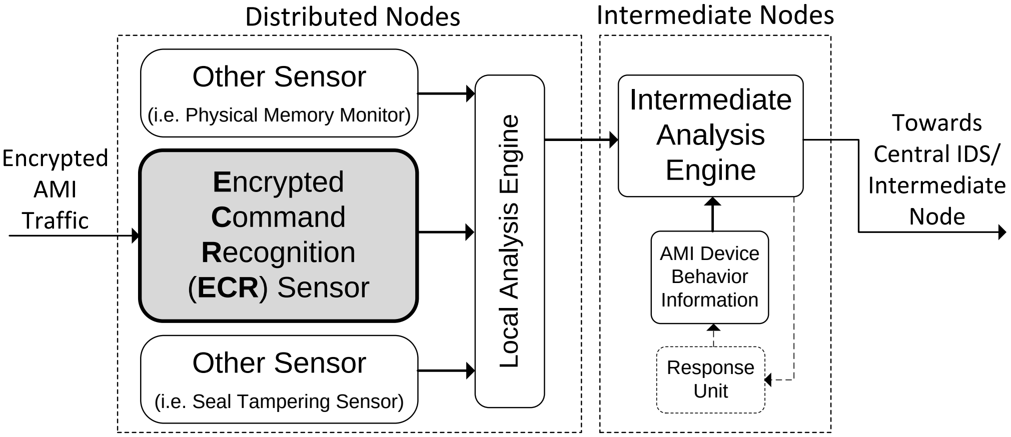
Distributed Nodes
Intermediate Nodes
Other Sensor
(i.e. Physical Memory Monitor)
Encrypted AMI Traffic
Encrypted Command Recognition (ECR) Sensor
Other Sensor
(i.e. Seal Tampering Sensor)
Local Analysis Engine
Intermediate Analysis Engine
AMI Device Behavior Information
Response Unit
Towards Central IDS/ Intermediate Node

Figure 1: The *ECR* sensor in an AMI Intrusion Detection System