Chapter 17
Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems

Leandros Maglaras
De Montfort University, UK

Helge Janicke
De Montfort University, UK

Jianmin Jiang
Shenzhen University, China

Andrew Crampton
University of Huddersfield, UK

ABSTRACT

SCADA (Supervisory Control and Data Acquisition) systems are a critical part of modern national critical infrastructure (CI) systems. Due to the rapid increase of sophisticated cyber threats with exponentially destructive effects, intrusion detection systems (IDS) must systematically evolve. Specific intrusion detection systems that reassure both high accuracy, low rate of false alarms and decreased overhead on the network traffic must be designed for SCADA systems. In this book chapter we present a novel IDS, namely K-OCSVM, that combines both the capability of detecting novel attacks with high accuracy, due to its core One-Class Support Vector Machine (OCSVM) classification mechanism and the ability to effectively distinguish real alarms from possible attacks under different circumstances, due to its internal recursive k-means clustering algorithm. The effectiveness of the proposed method is evaluated through extensive simulations that are conducted using realistic datasets extracted from small and medium sized HTB SCADA testbeds.

DOI: 10.4018/978-1-5225-9866-4.ch017

INTRODUCTION

In order to modernize the national critical infrastructure, cyber-physical systems are becoming a vital part of them. Cyber-attacks tend to target important assets of the system, taking advantage of vulnerabilities on the architecture design or weaknesses of the defense systems. Lately several research efforts have revealed the importance of human factor on the cyber security assurance of a system (Evans, 2016; Ayres, 2016). Most of the weaknesses in CIs arise from the fact that system architects tend to adopt off-the-shelf technologies from the IT world, without a significant change, thus relying on the "airgap" security principle that falsely assumes that an apparently isolated and obscure systems are implicitly secure. The integration of new technologies, especially Internet-like communications networks, may introduce some new threats to the security of a smart grid. In such a network there are three crucial aspects of security that may be threatened due to the CIA-triad, these being: confidentiality, integrity, and availability (Woo, 2015)

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. An attack on this occurs when an unauthorized person, entity or process enters the system and accesses the information.
- Integrity refers to safeguarding the accuracy and completeness of assets, which ensures that the information in the system will not be modified by attacks.
- Availability pertains to the property of being accessible and usable upon demand by an authorized entity. The resources need to be kept accessible at all times to authorized entities or processes.

The integration of new technologies such as smart meters and sensors can bring new vulnerabilities to a smart grid that combined with the traditional cyber threats like malware, spyware and computer viruses make the situation complex and hard to deal with. (Sadeghi, 2015). In the three main control systems of a CI, the SCADA is the central nerve system that constantly collects the latest status from remote units, such as RTUs and PLCs. The communication between the different sub networks and the control system of a power grid can be blocked or cut off due to component failures or communication delays. If one of the crucial communication channels fails to connect in the operational environment, the control of important facilities may be impossible leading to possible power outages. In this situation, the effect of some widely known attacks can have devastating consequences on SCADA systems.

Intrusion detection systems can be classified into centralized intrusion detection systems (CIDS) and distributed intrusion detection systems (DIDS) depending on how the different components are distributed (Kenkre, 2014). In a CIDS the analysis of the data is performed in some fixed locations independently on the number of hosts that are monitored, while in a DIDS several IDS can be located in different places inside the smart grid. DIDS has specific advantages over CIDS. For instance, it is highly scalable easily extensible and scalable (Vasilomanolakis, 2014). It is evident that the development of distributed IDS specifically designed for SCADA systems, being able to ensure an adequate balance between high accuracy, low false alarm rate and reduced network traffic overhead, is needed. The above discussion clearly indicates that specific intrusion detection systems that reassure both high accuracy, low rate of false alarms and decreased overhead on the network traffic need to be designed for SCADA systems. Based on this need, new IDSs are constantly introduced belonging to two main categories; signature based and misuse detection. There has been considerable amount of work regarding SCADA intrusion and anomaly detection. Some IDS solutions involve combining network traces and physical process