Chapter 11

Infrequent Pattern Identification in SCADA Systems Using Unsupervised Learning

Mohiuddin Ahmed
UNSW Canberra, Australia

ABSTRACT

In recent years, it has been revealed that these critical infrastructures such as SCADA systems have been the target of cyber-terrorism. In general cyber-attacks are infrequent in nature and hence infrequent pattern identification in SCADA systems is an important research issue. Therefore, design and development of an efficient infrequent pattern detection technique is a research priority. In this chapter, the effectiveness of co-clustering which is advantageous over regular clustering for creating more fine-grained representation of the data and computationally efficient is explored for infrequent pattern identification in SCADA systems. A multi-stage co-clustering based infrequent pattern detection technique is proposed and applied on seven benchmark SCADA datasets which includes practical industrial datasets. The proposed method shows its superiority over existing clustering based techniques in terms of computational complexity which is essential for practical deployment in a SCADA framework.

INTRODUCTION

Nation’s critical infrastructures including Energy, Gas and Water networks need advanced monitoring and control for reliable and smooth operation of the whole interconnected complex system. Still today, the Industrial Control Systems (ICS) of these critical infrastructures rely on the Supervisory Control and Data Acquisition (SCADA) systems (Figure 1.) for system wide monitoring and control. Typically, SCADA system includes Remote Terminal Units (RTUs) with Intelligent Electronic Devices (IEDs), Programmable Logic Controllers (PLCs), a telemetry system, a Human Machine Interface (HMI) and a supervisory (computer) system. In a SCADA system, the supervisory system is connected with the RTUs through communication infrastructures. In the SCADA conception, data acquisition is the first task done by the monitoring and sensing devices. For example, in an Energy System Phasor Measurement

Units (PMU) measure the Global Positioning System (GPS) synchronised system states, e.g., voltage magnitudes and angles. This information is then sent to the control room. Once data acquisition task is completed, the second task involves with the intelligent decision making in the control centre. Finally, the control decisions are sent to the RTU/PLC to adjust or override the current states. The whole process is a feedback system where all devices and modules play a vital role for information monitoring, processing and control. Due to numerous advantages towards a reliable and efficient system operation, SCADA systems are widely used in different sectors of critical infrastructures. In recent years, SCADA system is facing new type of threats that did not appear before. Often these threats or unusual activities are considered as anomalies, outliers, infrequent patterns. In this chapter, we will use the term infrequent pattern to avoid any ambiguity.

Figure 1. SCADA architecture