Chapter 7
Fuzzy–Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems

Saša D Milić

https://orcid.org/0000-0001-5757-3430
Electrical Engineering Institute Nikola Tesla, Serbia

ABSTRACT

This chapter provides a complex data analysis of critical infrastructure SCADA vulnerabilities and exploits using fuzzy-decision algorithms. These algorithms are presented in two case studies describing possible scenarios of the cyber attack on two vital multi-parameter remote monitoring systems. The main objects of the cyber attack analysis are data obtained from their common SCADA system. The main focus is on multiparameter remote monitoring systems for monitoring electricity production and water traffic processes in the lock of hydropower plant. Newly developed fuzzy decision algorithms for comprehensive data analysis are presented to recognize the cyber attack. The results of the fuzzy modeling are directly dependent on the complex choice of the if-then rules on the basis of which decisions are made. In addition, two fuzzy logic systems (FLS-T1 and FLS-T2) are used for modeling several cyber attack scenarios.

INTRODUCTION

World economy faces unprecedented challenges, whether from soaring population growth, energy resource constraints, or warming climate and myopic financial markets. Today's trends and financial climate in the electricity market dictate the constant need for improving operations in the power system. Market liberalization and market operations in the electricity sector have set new requirements to improve the strategies of maintenance and electricity production in power plants. Consumers have a major impact on the market, mostly through companies that are involved in trade with electricity. There are also several

powerful strategic weapons used by market and industry leaders to leverage their positional advantages (Lin, Chen, & Chu, 2015).

Sustainable technology and sustainable development are different facets of the same approach. Despite of the rising awareness of the urgency in finding more efficient and effective ways to achieve sustainable development, comprehensive and consistent meaning is still elusive both in theory and practice (Jakšić, Rakićević, & Jovanović, 2018; Ritala, Olander, Michailova, & Husted, 2015).

Supervisory Control and Data Acquisition (SCADA) system is a computer-based monitor and control system. In other words, SCADA is a main networked system for monitoring and controlling all technical systems and processes in the power facilities. The older SCADA systems were isolated and localized from conventional networks having specialist protocols such as Modbus, Profibus, etc. for interfaces with devices on the basic level. These protocols are a commonly available means of connecting industrial electronic devices such as smart sensors, programmable logic controllers (PLCs), microprocessor-controlled electronic devices, remote terminal units (RTUs), and industrial computers.

The end of the 20th century was marked by a rapid expansion of the Internet. The expansion of the Internet is accompanied by a widespread application of the Transmission Control Protocol/Internet Protocol (TCP/IP). It is a communication protocol used to interconnect network devices on the internet, intranet, and extranet.

Today we have gone a step further. The need for connecting devices over the Internet has required new communication concepts. Internet of Things (IoT) encompasses everything connected to the internet. Industrial Internet of Things (IIoT) is the network of multitude of smart electronic devices (smart sensors, PLCs, monitoring systems, alarm and warning units) connected by communications technologies. IIoT enables better monitoring of technological processes, the use of cloud technology, comprehensive multiparametric analysis, better fault and aging prediction and timely decision making. The growth of the IIoT is drastically changing how experts, engineers and managers of power plants interact with multiparameter remote monitoring systems, smart sensors, alarm and warning units, and different kind of RTUs (Boyes, Hallaq, Cunningham, & Watson, 2018; Sisinni, Saifullah, Han, Jennehag, & Gidlund, 2018). Today, a large number of embedded devices, RTUs, smart sensors, and complex monitoring systems are used in safety and security-critical applications such as SCADA systems and Machine to Machine (M2M) communication in power plants and traffic infrastructure (Babić, Milić, & Rakić, 2017; Milić & Srećković, 2008; Milić, Žigić, & Ponjavić, 2013; Misović, Milić, & Đurović, 2016). SCADA systems are used in many critical infrastructure applications (Falco, Caldera, & Shrobe, 2018). These applications are increasingly becoming the targets of cyber attacks. The IIoT changes in the power system and traffic by creating a new imperative to share data from smart sensors and monitoring systems managed by SCADA with alarm, warning and control systems. This data sharing concept brings many benefits. Some of these benefits are: energy savings, timely maintenance, condition based maintenance, prediction based maintenance, maintenance based on risk assessment, better assessment of fault probability, better investment planning, more reliable production, staff reduction, etc. A detailed economic analysis shows even greater benefits when taking into account the savings from production and traffic optimization.

Improving maintenance and increasing energy efficiency by reducing unplanned outages involves the continuous introduction of new monitoring systems and modernization of old ones. With the constant introduction of new monitoring systems and smart sensors, the number of observed parameters increases, which significantly complicates the existing SCADA systems. In addition to the many benefits that are achieved by analyzing the data obtained from the SCADA system, there are also serious risks associated

Related Content

A Framework for External Interference-Aware Distributed Channel Assignment

Felix Juraschek, Mesut Günesand Bastian Blywis (2013). *Security, Design, and Architecture for Broadband and Wireless Network Technologies (pp. 293-307).*

www.irma-international.org/chapter/framework-external-interference-aware-distributed/77425

Waste Management System for Smart City Using IoT

Golden Julie E. (2019). *The IoT and the Next Revolutions Automating the World (pp. 1-15).*

www.irma-international.org/chapter/waste-management-system-for-smart-city-using-iot/234019

Fundamental Principles of IoT

Mahesh Kumar Jha, Monika Singhand Anindita Sahoo (2021). *Principles and Applications of Narrowband Internet of Things (NBIoT) (pp. 1-25).*

www.irma-international.org/chapter/fundamental-principles-of-iot/268943

TCP for Wireless Internet: Solutions and Challenges

Alaa Ghaleb-Seddik, Yacine Ghamri-Doudaneand Sidi Mohammed Senouci (2012). *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications (pp. 1-44).*

www.irma-international.org/chapter/tcp-wireless-internet/63544

Artificial Intelligence and Machine Learning Approaches in Smart City Services

Mona Bakri Hassan Dahab, Elmustafa Sayed Ali Ahmed, Rania A. Mokhtarand Rashid A. Saeed (2023). *Handbook of Research on Network-Enabled IoT Applications for Smart City Services (pp. 339-352).*

www.irma-international.org/chapter/artificial-intelligence-and-machine-learning-approaches-in-smart-city-services/331341