Performance analysis of different communication protocols under cyberattacks

Abstract

The aim of this report is to analyze the performance of different communication protocols under a cyberattack. The goal is to conduct a performance analysis of different communication protocols commonly used in power systems, such as Modbus, DNP3, and IEC61850. In addition to evaluating their resilience to cyber-attacks and identifying potential vulnerabilities. This is done by creating real-time simulations of communication networks using OPAL-RT using these different protocols and performing tests and attacks on each of them. After these tests we can determine which protocols are the most reliable, as well as have the best performance while or after attacks.

Introduction

The objective of this report is to conduct a comprehensive performance analysis of communication protocols commonly employed in power systems, specifically focusing on Modbus, DNP3, and IEC61850. The primary aim is to assess the resilience of these protocols against cyber-attacks and identify potential vulnerabilities. This analysis involves testing the protocols' defensive capabilities under cyber-attack scenarios and evaluating their performance during such attacks.

Selecting a secure and reliable protocol depends on various factors, including specific use cases, required levels of security and reliability, and compatibility with existing

systems and infrastructure. Organizations and system designers must carefully evaluate these protocols and consider their specific needs before making a final decision. For instance, the widely used Modbus protocol in industrial automation and power systems lacks robust security features, but its security can be enhanced by implementing additional measures such as virtual private networks (VPNs), firewalls, and encryption (“Modbus, DNP3 and Hart. Infosec Resources”, 2021). On the other hand, DNP3 offers improved security features, including authentication and encryption, compared to Modbus (“Difference between Modbus and DNP3 communication protocols”, 2019).

Accurate simulations of communication networks and thorough testing are crucial in order to provide valuable recommendations for enhancing the security and resilience of these protocols. By contributing to the body of knowledge in the field of communication protocols for power systems, this research aims to influence the development and implementation of more secure and reliable protocols in the power industry.

Methods

1. The first step is to create models using MATLAB Simulink as shown in Fig. 1 This means data in this model should be shared over the communication network.

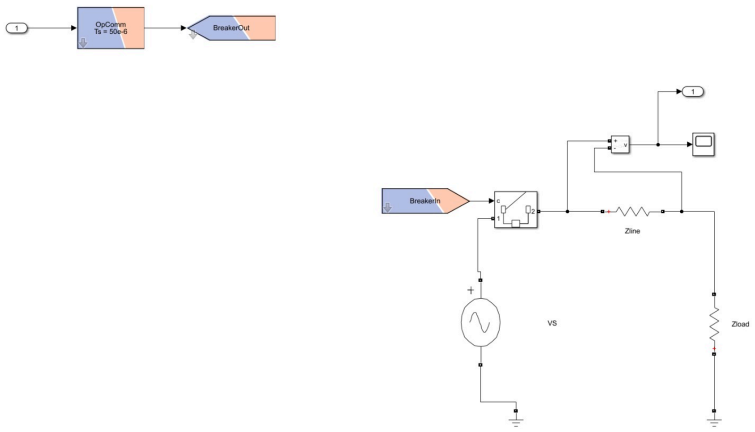

Fig. 1 Simple simulink module.

2. Next step is to configure and map the module as shown in Fig. 2 and 3 to the specific protocol that is to be tested. For this the communication nodes are developed using RT-Lab and finally mapping them to a communication network using Exata CPS network simulaotr. software.

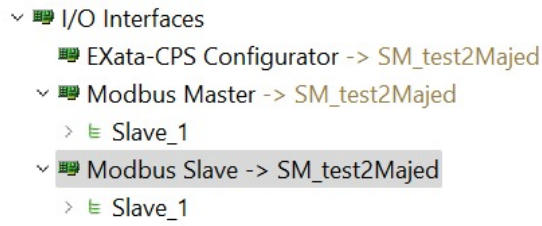

Fig. 2 Configuring nodes (Modbus protocol).

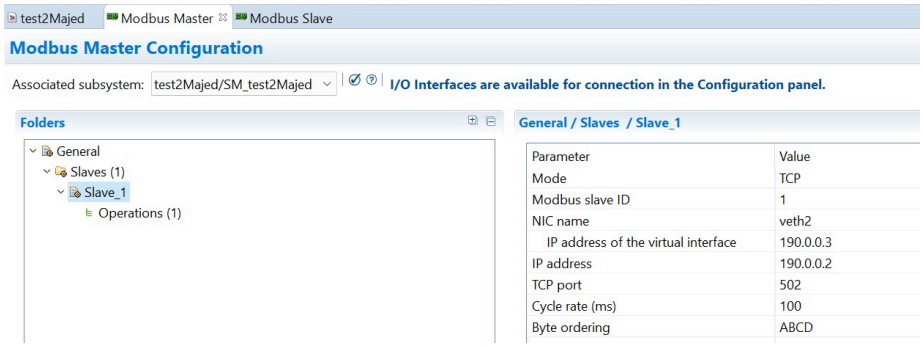

Fig. 3 Configuring Modbus slaves.

3. Finally a communication network is created using Exata as shown in Fig. 4 and should be run on the OPAL-RT simulator along with the power system simulation to exchange data in real time.

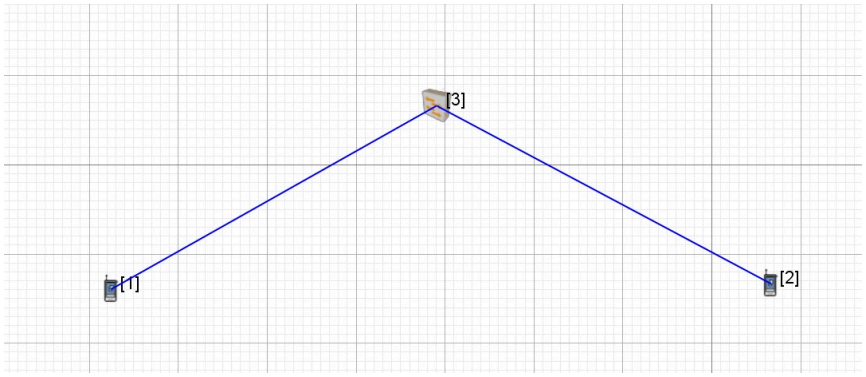

Fig. 4 Exata software network creation.

Expected results

Upon successfully establishing networks utilizing the different protocols, the Exata tool will be leveraged to conduct targeted attacks on each network. This process will generate valuable data and analytics, offering insights into the response of the network employing each specific protocol under attackBy subjecting the networks to simulated attacks, Exata will enable the collection of comprehensive information regarding the performance, resilience, and vulnerabilities of each protocol. The analytics derived from these tests will provide a quantitative assessment of how effectively each network utilizing a particular protocol responds and withstands cyber threats.

References

1. J. (2021, March 25). Modbus, DNP3 and Hart. Infosec Resources. https://resources.infosecinstitute.com/topic/modbus-dnp3-and-hart/.
2. Staff, E. (2019, September 8). Difference between Modbus and DNP3 communication protocols. Inst Tools. https://instrumentationtools.com/difference-modbus-dnp3-communication-protocols/#:~:text=Modbus%20and%20DNP%20are%20both,485%2C%20and%20TCP%2FIP.