proceedings

MDPI

Abstract

Secure SCADA-IoT Platform for Industrial Automation and Control: A Collaborative-Communication Designed Model †

Aamir Shahzad and Young-Gab Kim *

Department of Computer and Information Security, 209, Neungdong-ro, Gwangjin-gu, Sejong University, Seoul 05006, 143-747, Korea; s.aamir@sejong.ac.kr

Correspondence: alwaysgabi@sejong.ac.kr

† Presented at Symmetry 2017—The First International Conference on Symmetry, Barcelona, Spain, 16–18 October 2017.

Published: 9 January 2018

Abstract: This paper discusses the new auspicious trends of internet of things (IoT) and its advanced developments in various sectors of today's IT arena, including for industrial sectors. Each object acts as a communication node (or entity) that is able to communicate with other nodes, and corresponding information could be accessed and controlled, via several of today's commonly used electronic devices such as laptops and cellular devices, etc., through an IoT-designed platform. Moreover, in industrial automation sectors, the employment of IoT is very advantageous, in terms of remote communication support; low-cost operations and maintenance; and autonomous collaborations among remote networked field devices, etc. The facility of autonomous collaborations provisioned by IoT, in the context of a supervisory control and data acquisition (SCADA) system as part of an industrial control system, somehow exists in a distributed network protocol (DNP3) during automation and controls. Therefore, the current study takes the step to model a new IoT framework for a SCADA system, which will be efficient at facilitating industrial automation through the collaborative DNP3-Modbus acquisitions and automation, called the SCADA-IoT system. An IoT gateway is employed and configured that supports for both SCADA protocols, such as DNP3 and Modbus and is efficient at communicating, from networked field devices, with inter-processing from both. In the overall SCADA-IoT design, the transmission is carried from an enormous amount of sensors and/or field devices, employing proprietary and non-proprietary protocols; further, sent information is analyzed via big data, stored in a cloud center, monitored and controlled over a SCADA-IoT supportive platform. At the same time, information security (IS) is a big associated challenge and one of the main contributions of this study. Thus, this study also analyzed the potential security mechanisms for securing SCADA-IoT and found cryptography to be a noteworthy security solution, based on the proposed system requirements and its communication demands.

Acknowledgments: This work was supported by the faculty research fund of Sejong University in year 2017. And this work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00756, Development of interoperability and management technology of IoT system with heterogeneous ID mechanism).