

A SCADA Intermediate Simulation Platform to Enhance the System Security

A Amir Shahzad^{#1}, Naixue Xiong^{*2} (IEEE Member), Muhammad Irfan^{#3}, Malrey Lee^{#4}, Shahid Hussain^{#5} (IEEE Member)

[#]561-756, Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, & Department of Computer Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, Korea

^{*}The School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, 200093 China

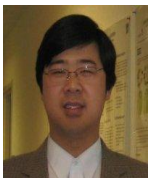
¹mail2aamirshahzad@gmail.com, ²xionгнаixue@gmail.com (Corresponding Author), ³irfanview2@gmail.com, ⁴mrlee@jbnu.ac.kr, ⁵shahiduop@jbnu.ac.kr

Abstract— SCADA (supervisory control and data acquisition) systems are increasing rapidly in the terms of uses and deployments in real time industrial processing, approximately all over the world. To fulfill, the underlying advanced acuirements of industrial process; the SCADA systems are gaining and deploying more advance features for infrastructural developments, from arena of information technology (IT). Now days, the SCADA systems are also connected with several open networks and allow the transmission of data (bytes) geographically, within local area networks (LANs)/wide area networks (WANs) over internet using “transport control protocol (TCP)/internet protocol (IP) and others”. With the increasing of SCADA system connectivity with number of open networks or/and protocols, several organizations included “dnp.org, Trianglemicroworks,Inc, NS network solutions, ASE-systems, modbus.org, fieldbus.org and others”, have been deploying the security mechanisms to secure the communication of SCADA systems as part of industrial control systems (ICSs). In proposed study, based on existing security analysis of SCADA systems, the security implementation via cryptography mechanism has been placed between SCADA nodes during transmission of bytes. The “secure cryptography intermediate node (SCIN)” has been situated between SCADA communication nodes during transmission. Each time communication has been occurred between participated nodes, bytes are passed through SCIN which provides two-way secure communication link or channel against attacks

Keyword—Supervisory Control and Data Acquisition System, SCADA Security, Secure Cryptography Intermediate Node, Cryptography Approaches, Simulation Test



A Amir Shahzad received “PhD degree in Network Security and Cryptography” from University Kuala Lumpur, Malaysia and is teaching computer science and I.T courses at University Kuala Lumpur. He involves his students in “traditional and real time networks, security and policies”. His professional interests focus on “networks security via cryptography, networks protocols configuration and related security, software engineering, artificial intelligence, multimedia design and applications, and biometric information systems.”



Dr. Naixue Xiong is currently holding a position of professor in School of Computer Science Colorado Technical University, USA



Muhammad Irfan received his Bachelor of Information Systems (Hons) in Network Technology from The Infrastructure University Kuala Lumpur (IUKL), Kuala Lumpur, Malaysia. His professional interests focus on computer networks and security.



Malrey Lee is an associate Professor in the Department of Electronics and information Engineering and member of Research Center for Advanced Image and Information Technology at Chonbuk National University, South Korea. She has over forty publications in various areas of Computer Science, concentrating on Artificial Intelligence, Robotics, Medical Healthcare and Software Engineering.



Shahid Hussain is currently a Master Degree Student in School of Electronics & Information Engineering, & Department of Computer Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, Korea.