Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 9 (7): 396-405, 2014
ISSN 1819-3579 / DOI: 10.3923/tasr.2014.396.405

Security Solution for SCADA Protocols Communication during Multicasting and Polling Scenario

[1]A. Shahzad, [1]S. Musa and [2]M. Irfan
[1]Malaysian Institute of Information Technology (MIIT), 1016, Jalan Sultan Ismail, Universiti Kuala Lumpur, 50250, Kuala Lumpur, Malaysia
[2]Windfield College, Paser Seni, Kuala Lumpur, Malaysia

Corresponding Author: A. Shahzad, Malaysian Institute of Information Technology (MIIT), 1016, Jalan Sultan Ismail, Universiti Kuala Lumpur, 50250, Kuala Lumpur, Malaysia

ABSTRACT

SCADA system connectivity with several types of transport protocols and open networks make SCADA communication more vulnerable from cyber attacks. Cyber security is major problem for SCADA protocols communication included DNP3, Modbus protocol and IEC 60870-5-104 protocol. In current study, multicasting communication and polling security issues have been considered and cryptography solutions have been deployed at each end of Modbus protocol and IEC 60870-5-104 protocol as part of SCADA communication. First security implementation used AES algorithm and hashing algorithm to secure the multicasting communication of Modbus protocol and IEC 60870-5-104 protocol. Second implementation used session key and hash algorithm to secure the polling communication of Modbus protocol and IEC 60870-5-104 protocol as part of SCADA communication. During communication, authentication, integrity and confidentiality attacks have been launched and behavior of system is observed during abnormal communication.

Key words: Supervisory control and data acquisition, cryptography algorithms, testbed experimentation and performance results, SCADA protocols security, issues, authenatication, confidentiality and integrity, modbus protocol, IEC60870 protocol, IEC 60870-5-104 standard, attacks and threads

INTRODUCTION

Supervisory Control And Data Acquisition (SCADA) system is a part of Industrial Control System (ICS) and have been deployed in various real time infrastructures included gas and electricity stations, etc. Supervisory Control And Data Acquisition (SCADA) systems have been used number of protocols include Fieldbus, Modbus, DNP3 and IEC60870 to control the operations of critical infrastructures that are distributed geographically at remote locations (Stouffer *et al*., 2007; NCS, 2004). Below sub-sections give detail related with the message structure of Modbus and IEC60870 protocols.

Modbus protocol message structure: Modbus protocol is used to performs number of functions or operations while deploying within process control systems as part of SCADA systems included "coil controlling functions may single or group, input command functions for reading status, register functions, diagnostics functions for testing and reporting, program functions, polling functions and reset functions". Modbus protocol receives the bytes or command form user interface and then

assemble these bytes as Protocol Data Unit (PDU). At layer 2 (OSI model), Protocol Data Unit (PDU) are convert into Application Data Unit (ADU) (Stouffer *et al.*, 2007; NCS, 2004; Modbus, 2006).

Usually, Modbus message structure is divided into following five main sections.

Message format: Master station send the request and remote station response, each message either request or response is formatted as protocol message frames within four specified fields containing number of bytes including 1 byte of address field, 1 byte of function field, variable bytes of data field and 2 bytes error checking field.

Synchronization: Modbus protocol used the synchronization mechanism for reliable communication between field devices. During communication, each device or node identifies the message frame starting frame position and session has been synchronized with message frame. Such that each character in frame must be received by target device.

Memory notation: "Four data types have specified by memory notation such as coils having one byte input, discrete having one byte input, input registers having two bytes input and holding registers containing two bytes of input".

Function codes: Modbus protocol has specify several function codes for request frame or message. Mean that each request frame is depending on the function code because target device action or response is depending on function code that has been specified within frame or request frame.

Exception response: If request frame has received by target device with errors then frame message is ignored and no response is replied against error frame or requested frame. If frame message is received by target device but the action would not supporting by target device. In this case, exception response will be transmitted from target device (Clarke *et al.*, 2004; Modbus, 2003; Dutertre, 2006).

IEC 50860-5-104 protocol message structure: IEC 50860-5-104 protocol standard used TCP/IP protocol for message/information transmission over LAN/WAN. In network, IEC 50860-5-104 based devices are directly connected with LAN/WAN. Such that master station send request bytes to remote station via., TCP/IP and response will be received via., TCP/IP to master station. User bytes are assembled into protocol specified data units, this is called Application Services Data Units (ASDUs). The header bytes or Application Protocol Control Information (APCI), bytes are added with ASDU bytes, this process is also called application control information. If there is no bytes within request or response message then only header or APCI will transmit to target node. In IEC 50860-5-104, APCI has contained subfield such as start, length and control fields and APCI bytes are required with ASDU bytes to generate the complete message during transmission. IEC 50860-5-101 standard has four layers in its stack such as user layer, application layer, data link layer and physical layer while IEC 50860-5-104 standard has add two more layer such as transport layer and network layer in its stack that are used for message transmission over internet or networks using TCP/IP or other protocols (Clarke *et al.*, 2004).

METHODOLOGY

Modbus protocol (TCP/IP) employment within SCADA system has no proper mechanism that addressed the security during communication between field devices. As results, modbus communication is vulnerable from several types of attacks. Usually, each system or network has different specifications for implementation and communication but with common security issues while connecting with internet. Lack of security within SCADA/Modbus communication, attack scenario has been created using Snort attacking tool to check the level of intrusions or intrusion detection with SCADA communication. Basic parameters such as Modbus header, function code, source address, destination address, protocol specification and port either sender or receiver have been defined within Snort tool configuration and subsequently, bytes are sniffed between SCADA nodes (Shahzad *et al*., 2014a, b). The abnormal traffic has been generated using of Snort too and intrusions are detected in SCADA/Modbus communication. This research reviews the security threads that have been warming SCADA/Modbus communication and gives considerations for SCADA/Modbus security enhancement (Diaz, 2011; Kobayashi *et al*., 2009).

Secure telecontrol operations are specified by IEC 60870-5-104 protocol by implementation of SSH (secure shell) protocol and performance parameters related with communication are also considered. New security stack has been implemented within Distributed Network Protocol (DNP3). The additional security layers have been deployed based on cryptography algorithms using symmetric and asymmetric algorithm to securing the communication of SCADA/DNP3 protocol. Cryptography solution has been successfully deployed within application layer and data link layer of Distributed Network Protocol (DNP3) and results are measured and verified for security evaluation (Sanchez *et al*., 2010; Musa *et al*., 2013a). At another side, security solution has been also implemented within cloud computing environment. In first phase, SCADA system has been deployed entirely within cloud environment and then security using cryptography algorithms is deployed and tested in second phase. The attacks detection ratio (%) has been also measured to validate the proposed security implementation (Al-Bakri *et al*., 2011; Shahzad *et al*., 2013).

IEC 60870 (other standards such as IEC 60870-5-101/104) protocol provides security mechanism to secure the communication of telecontrol system. The scope of security solution is restricts the unauthorized users that are interacting within communication. Application Protocol Data Units (APDUs) have been securely transmitted between the nodes and each node is able to authenticate each other during communication. The deployment of cryptography solutions and the key management process is out of scope in this research (IEC, 2013). Several attack scenarios have been highlighted included steal identification of user to get control on system, using hacking tools and perform read and write operations, gain access between SCADA nodes during communication and change the information. The attack impact ratio (%) within SCADA system has been also calculated based on attacks such as reply, repudiation, bypassing control, integrity violation, authorization violation, eavesdropping, spoofing, denial of service attack and information hacking, etc. (IEC, 2013; Holstein, 2004).

Security solutions have been specified for SCADA protocol IEC61850 series to secure the communication. Each protocol and network has different specification for implementation and communication with different level security. The security objectives such as integrity, authentication, confidentiality, authorized access, protection from eavesdropping man in middle, denial of services, data reply and spoofing are main objectives that commonly SCADA system has addressed for security purposes. Transport Layer Security (TLS) protocol has been deployed to secure the communication of IEC 62351-3. The security services such as integrity, confidentiality

and authentication has been archived during communication and communication has been protected from number of attacks such as man in middle, spoofing and encryption attacks, etc. Transport Layer Security (TLS) protocol also has been deployed to secure the communication of IEC 62351-4, such that every node authenticates each other during communication or during information exchanging. In IEC 62351-5 standard, confidentiality and integrityhas been implemented by using of TLS protocol based encryption while encryption does not deploy within IEC 62350 because of session limitation specified as 4 ms (Cheah, 2008; Kang and Robles, 2009).

In SCADA system, master station initial the request message and send to remote station. Upon receiving, remote station will generate the response and send back to master station. The current research analysis the security threads/attacks and vulnerabilities that are interacting within the communication of SCADA/ IEC 60870-5-104 standard. IEC 60870-5-104 has been designed without any security concerned and also lack of authentication or cryptography mechanism. The detail literature has been reviewed that is based on SCADA system and DCS system implementations and also number of protocols included IEC 60870-5, IEC 60870-5-101, IEC 60870-5-104 and Distributed Network Protocol (DNP3). The security threads/attacks and vulnerabilities analysis has been conducted and a method called "Fuzz" is proposed for testing the IEC 60870-5-104 protocol between nodes or field devices. The fuzzing is a tool or testing method that is used to test the input message or random bytes and display the result on its interface. The fuzzing tool used two types of testing methods such as valid fuzz in which input bytes are resembled for desire result and simple fuzz in which input bytes are depeded on "pseudo random number generator" (Cheah, 2008; Shahzad *et al*., 2014b).

RESULTS AND DISCUSSION

Several times SCADA test bed using IEC60870-5-104 and Modbus have been run and carefully results are measured include security ratio (%), attack impact ratio (%) and latency measured in milliseconds during normal/abnormal communication or traffic. In testbed setup, five remote stations such as RTU1, RTU2, RTU3, RTU4 and RTU5 are configured with master station with the bandwidth of 5 Mbps (Musa *et al*., 2013b; Shahzad *et al*., 2013).

Multicasting communication security: Master stations initiate the multicasting communication and send the message to remote stations. The message has been encrypted by secret key, generated from AES algorithm and then hash value is calculated using SHA-2 hashing algorithm. Secret key has been securely shared by master station and remote stations using secure channels. The RSA algorithm is not reliable for multicasting communication, because too many keys are acquired during communication which significantly affect the performance of critical systems.

The state M100/I20 represents the master station request initialization process and state M101/I20 represents the bytes encryption process. When encryption process has been completed and master station multicast the message then remote stations decrypted the message at state M102/I22. If any message will be responded back such as confirmation or other to master station, remote station generated the response at state M104/I24 to state M106/I26. The states, state M107/I27 and state M108/I28 show that master station has received the response from remote station. The states, state M310/I53 to state M312 represent that attacks such authentication, integrity and confidentiality have been detected and system behavior is measured at state M313/I56.

Encryption process (Proof):

- Multicasting message = $(\text{Encry}(\text{payload}_{(SC_k, \text{Hash}, \text{Node})}))^n$, n = 1, 2, 3, ..., n-1
- Encrypted message (Payload), multicast from sender node to receiver nodes

Where:

- Total No. of nodes within communication is depending on value 'n'
- $SC_{k(\text{Node})}$(User bytes) encrypted payload using secret key and designated as payload[1]
- $\text{Hash}_{(\text{Node})}$(User bytes) payload digests using SHA-2 and designated as Hash_payload

Decryption process (proof):

- Multicasting message = Decry $(\text{Encry}(\text{payload}_{(SC_k, \text{Hash}, \text{Node})}))^1$
- Decry $(\text{Encry}(\text{payload}_{(SC_k, \text{Hash}, \text{Node})}))^2$, $(\text{Encry}(\text{payload}_{(SC_k, \text{Hash}, \text{Node})}))^2$, ..., decry $(\text{Encry}(\text{payload}_{(SC_k, \text{Hash}, \text{Node})}))^{n-1}$
- Multicasting message has been received from master (sender) node to remote (target) nodes
- $SC_{k(\text{Sender, target node})}$(User bytes)
- $\text{Hash}_{(\text{Target node})}$(User bytes) = $\text{Hash}_{(\text{Sender})}$(User bytes), successfully verified the security services such as data authentication, data integrity and data confidentiality during communication at each end (master to target nodes)

Figure 1 and 2 shows the overall performance results that have been measured within SCADA testbed during normal and abnormal communication. Figure 1 shows the performance measurements captured within SCADA/ IEC60870-5-104 testbed while Fig. 2 shows the performance measurements captured within SCADA/Modbus testbed. In Fig. 1 and 2, the red maker represent the authentication attacks, black maker represent the integrity attacks and orange maker represent the confidentiality attacks within communication.

Performance Fig. 3 shows the average latency that has been measured during communication. Green line represents the latency calculated from Modbus testbed and blue line shows the latency from IEC60870-5-104 testbed as part of SCADA system.

Polling communication security: In SCADA system, master station poll the remote station within fixed interval or may random interval or session. Time interval is important aspect in critical infrastructures operations or SCADA system. In some cases, master station set the polling interval at each and every second or milliseconds and remote station send the response within this specified interval. Usually, cryptography solutions are not reliable in case of polling request within SCADA systems because encryption consume much time for implementation. Due to the security limitation in Modbus and IEC60870-5-104 as part of SCADA system, security solution has been proposed to secure the Modbus and IEC60870-5-104 protocol communication during polling request. Each time master station is polling the remote station, polling request is encrypted by session key. The polling request is set as fixed or dynamic interval, the session key life is directly proportional to polling session. If response has been not received within specified session then session key will expire and new session key is deployed for next polling request.

The states, state M500/I500, state M502/I502, state M507/I507 and state M510/I510 in Fig. 4 representing the pooling request while states; M501/I501, state M506/I506, state M508/I508 and state M511/I511 representing the pooling response. The attacks such as authentication, integrity and confidentiality have been detected at states; M503/I503, state M504/I504,

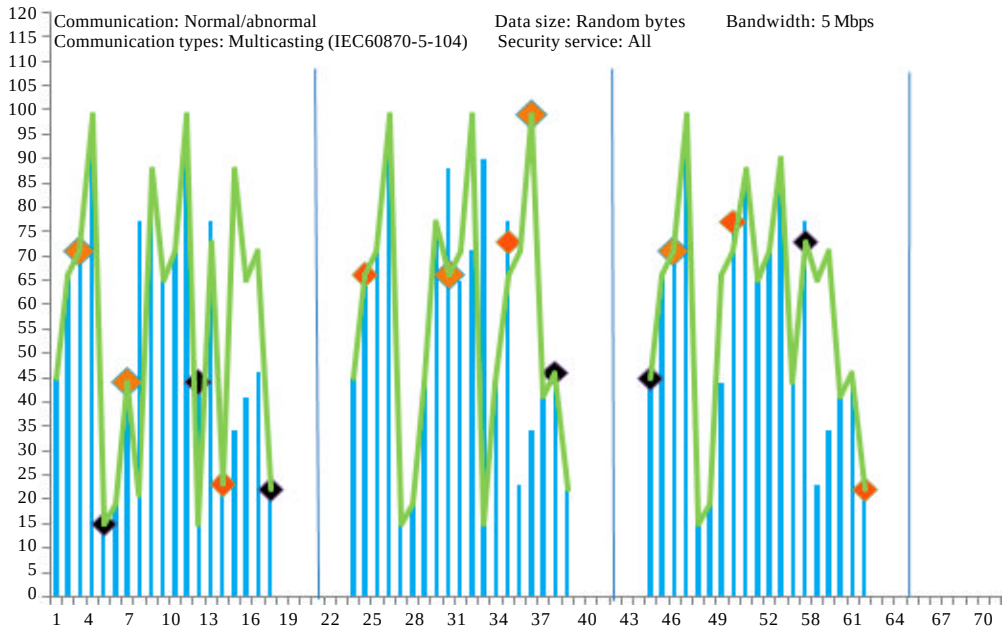

Fig. 1: Multicasting normal/abnormal communication using IEC60870-5-104

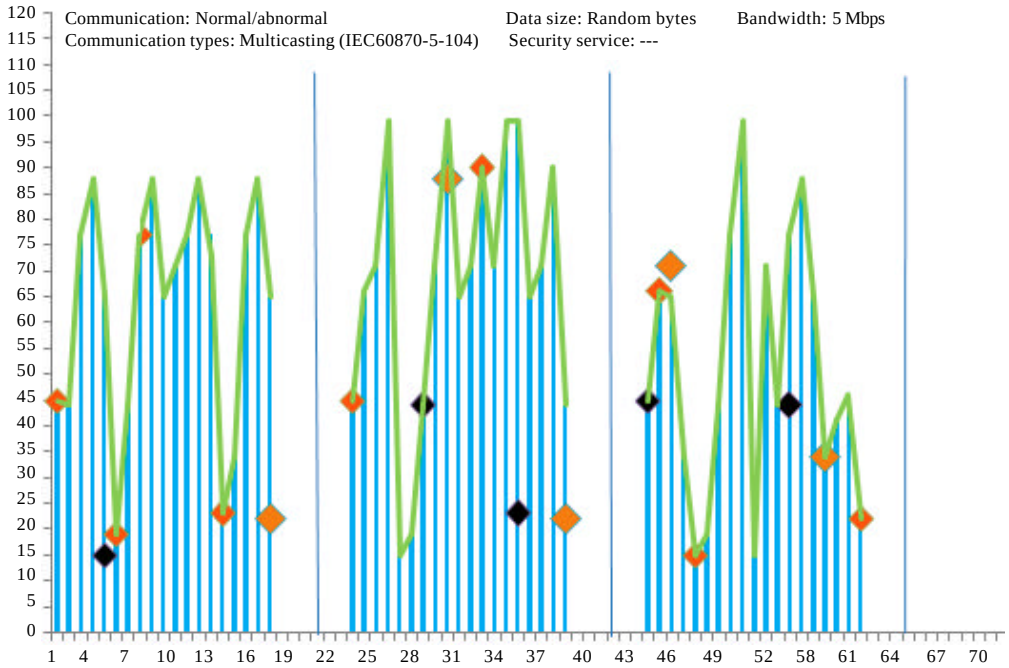

Fig. 2: Multicasting normal/abnormal communication using modbus

state M505/I505. For more Modbus and IEC60870-5-104 protocols security enhancement, hash algorithm has been also deployed during polling (request or response).

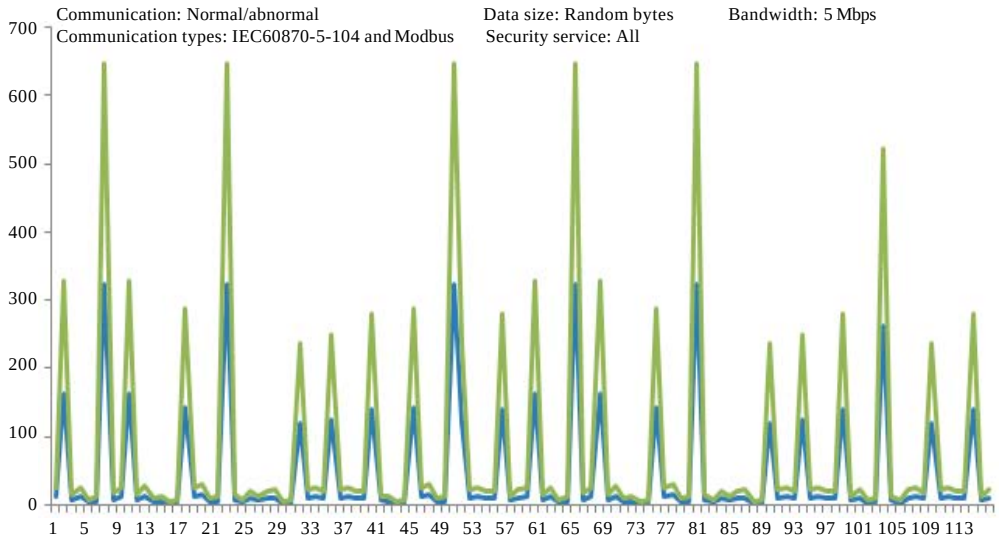

Fig. 3: Latency duing multicasting communication using modbus and IEC60870-5-104 protocols

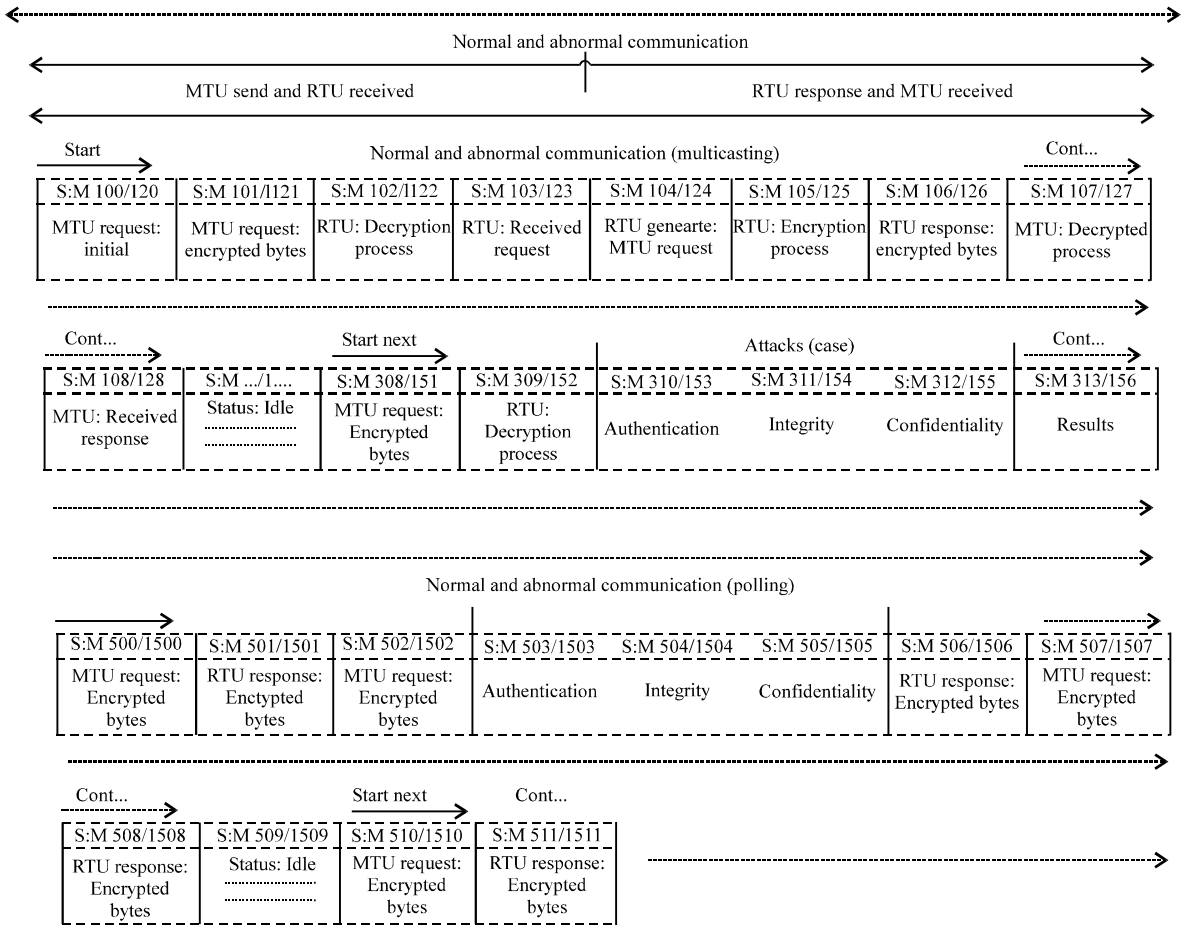

Fig. 4: SCADA protocols communication multicasting and polling scenario

Encryption process (Proof):

- Encryption = $SE_{k(Sender)}$(User bytes) designated as payload[1]
- $Hash_{(Sender)}(SE_{k(Sender)})$, designated as Hash_payload

Decryption process (Proof):

- Decryption = $SE_{k(Receiver)}$(User bytes)
- $Hash_{(Receiver)}[SE_{k(Sender)}]$
- $Hash_{(Target\ node)} == Hash_{(Sender\ Node)}$

The decryption process performed and successfully verified the security services such as data authentication, data integrity and data confidentiality during communication.

Figure 5 shows the overall polling performance results that have been measured within SCADA testbed during normal and abnormal communication. In Fig. 5, the red marker represents the authentication attacks, black marker represents the integrity attacks and orange marker represents the confidentiality attacks within communication.

Performance comparison: The below Table 1 shows the overall security results that have been measured during both communication included multicasting and polling communication (abnormal communication). In multicasting communication (using IEC60870-5-104 protocol), the attack detection ratio (%) = 18, 19 and 17 and impact ratio (%) = 13, 14 and 13% while the attack detection ratio (%) = 23, 18 and 17% and impact ratio (%) = 14, 15 and 15%, during Modbus communication (multicasting).

In polling communication, the attack detection ratio (%) = 38, 34 and 33% and impact ratio (%) = 17, 15 and 17%. The overall performance results show that the proposed solutions successfully enhanced the security during SCADA/Protocols communication and cryptography mechanism provides better performance (security) while comparing with other security solutions included firewall, DMZs and security patterns (Musa *et al*., 2013a; Shahzad *et al*., 2013).

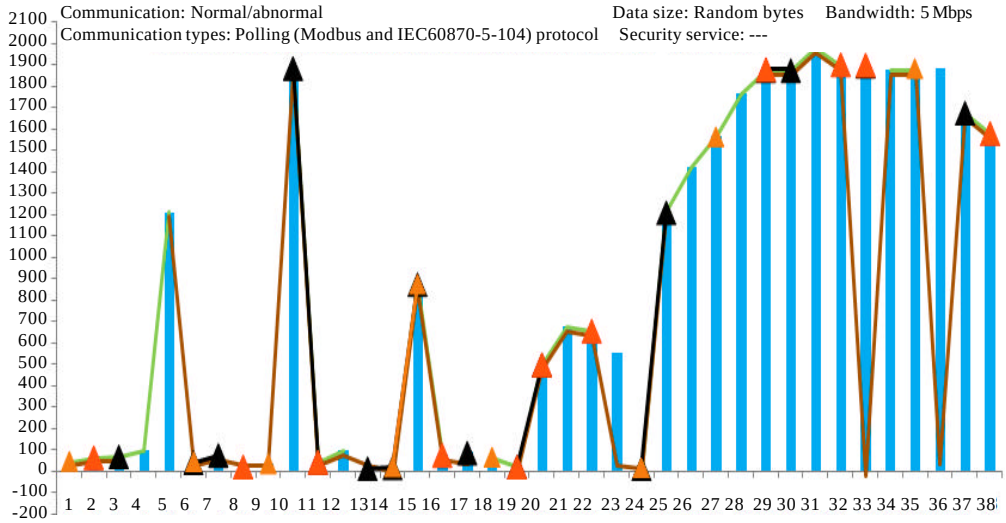

Fig. 5: Polling normal/abnormal communication using modbus and IEC60870-5-104 protocols

Table 1: Attack detection and impact ratio

	Abnormal: Multicasting communication security No. of experiments: 70 for each test		Abnormal: Polling communication security No. of experiments: 38 for each test	
Attacks	Attack detection (%)	Attack impact (%)	Attack detection (%)	Attack impact (%)
Authentication	App. 18,23	App. 13,14	App. 38	App. 17
Integrity	App. 19,18	App. 14,15	App. 34	App. 15
Confidentiality	App. 17,17	App. 13,15	App. 33	App. 17

Results are written without any decimal point and value has been around and App. is stand for approximately value

CONCLUSION AND FUTURE WORK

Cyber security is a major problem for SCADA protocols communication included DNP3, Modbus protocol and IEC 60870-5-104 protocol. Several existing security solutions have been deployed within SCADA point-to-point communication but limited security solutions are suggested for multicasting communication and polling either request or response within specified interval. The proposed implementation overcomes the security issues that are present within multicasting and polling communication of Modbus protocol and IEC 60870-5-104 protocol as part of SCADA communication. The security goals such as authentication, integrity and confidentiality of data have been achieved and the performance results show that the system or proposed testbed has resistance to overcome the attacks and successfully enhanced the security of SCADA system.

In future work, the current security solutions will implement inside the SCADA protocols or within protocols stack before transmitting to the physical layer.

REFERENCES

Al-Bakri, S.H., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2011. Securing peer-to-peer mobile communications using public key cryptography: New security strategy. Int. J. Phys. Sci., 6: 930-938.

Cheah, Z.B., 2008. Testing and exploring vulnerabilities of the applications implementing IEC 60870-5-104 protocol. Master's Thesis, Stockholm, Sweden.

Clarke, G., D. Reynders and E. Wright, 2004. Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems. Elsevier, Paris.

Diaz, J.J., 2011. Using SNORT for intrusion detection in Modbus TCP/IP communications. The SANS Institute Reading Room. December 7, 2011. http://www.sans.org/reading-room/whitepapers/detection/snort-intrusion-detection-modbus-tcp-ip-communications-33844.

Dutertre, B., 2006. Formal modeling and analysis of the modbus protocol. SRI International, October 11, 2006. www.csl.sri.com/~bruno/publis/formal_modbus.pdf.

Holstein, D.K., 2004. Cyber security tools for SCADA. The International Society of Automation, USA., October 6, 2004.

IEC, 2013. Telecontrol equipment and systems-part 5-7: Transmission protocols-security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351). International Electrotechnical Commission, IEC/TS 60870-5-7. http://webstore.iec.ch/preview/info_iec60870-5-7%7Bed1.0%7Den.pdf.

Kang, D.J. and R.J. Robles, 2009. Compartmentalization of protocols in SCADA communication. Int. J. Adv. Sci. Technol., 8: 27-36.

Kobayashi, T.H., A.B. Batista Jr., J.P.S. Medeiros, J.M.F. Filho, A.M. Brito Jr. and P.S.M. Pires, 2009. Analysis of malicious traffic in Modbus/TCP communication. Crit. Inform. Infrastruct. Security, 5508: 200-210.

Modbus, 2003. Implementing MODBUS/TCP avoiding multi-vendor pitfalls. The Modbus Organization.

Modbus, 2006. MODBUS messaging on TCP/IP implementation guide. Modbus-IDA, October 24, 2006.

Musa, S., A.A. Shahzad and A. Aborujilah, 2013a. Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, January 17-19, 2013, Kota Kinabalu, Malaysia.

Musa, S., A.A. Shahzad and A. Aborujilah, 2013b. Simulation base implementation for placement of security services in real time environment. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, January 17-19, 2013, Kota Kinabalu, Malaysia.

NCS, 2004. Supervisory Control and Data Acquisition (SCADA) systems. Technical Information Bulletin 04-1, National Communications System, October, 2004.

Sanchez, G., I. Gomez, J. Luque, J. Benjumea and O. Rivera, 2010. Using internet protocols to implement IEC 60870-5 telecontrol functions. IEEE Trans. Power Delivery, 25: 407-416.

Shahzad, A., S. Musa, A. Aborujilah, M.N. Ismail and M. Irfan, 2013. Conceptual model of real time infrastructure within cloud computing environment. Int. J. Comput. Networks, 5: 18-24.

Shahzad, A., S. Musa, A. Aborujilah and M. Irfan, 2014a. A new cloud based supervisory control and data acquisition implementation to enhance the level of security using testbed. J. Comput. Sci., 10: 652-659.

Shahzad, A. S. Musa, A. Aborujilah and M. Irfan, 2014b. Industrial Control Systems (ICSs) Vulnerabilities analysis and SCADA security enhancement using testbed encryption. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, January 9-11, 2014, Siem Reap, Cambodia.

Stouffer, K., J. Falco and K. Kent, 2007. Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security: Recommendations of the national institute of standards and technology. National Institute of Standards and Technology, Gaithersburg.