Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 14 (20): 2498-2506, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.2498.2506

Key Encryption Method for SCADA Security Enhancement

[1]A. Shahzad, [1]S. Musa, [2]M. Irfan and [3]S. Asadullah
[1]Malaysian Institute of Information Technology, 1016, Jalan Sultan Ismail,
Universiti Kuala Lumpur, Kuala Lumpur, 50250, Malaysia
[2]Windfield College, Paser Seni, Kuala Lumpur, Malaysia
[3]Kulliyah of Information and Communication Technology, International Islamic University, Malaysia

Abstract: With the growing demands of Industrial Control System (ICS) in all over the world, the industries such as water, electric and gas are using real time infrastructures for communication between field devices connected within "networks such as using Local Area Network (LAN)/Wide Area Network (WAN)" or/and over internet to fulfill the requirements of industrial processing and automation. Supervisory Control and Data Acquisition (SCADA) system is part of ICS. This is system based on real-time processing infrastructure, system control and design. In existing survey, several mechanisms/solutions were developed for reliable delivery of data without any attack. Several techniques were also implemented "such as using Secure Socket Layer/Transport Layer Security (SSL/TLS), secure shell (SSH) and Internet Protocol Security (IPSec)" for securing data across internet and overcoming the attacks related with SCADA communication. These techniques have also limitations in terms of data delivery and security because these are based on TCP/IP protocol for communication and on cryptography algorithms for the purpose of security. Based on detail SCADA security analysis, the cryptography techniques have been adopted to enhance the security of these critical systems. The proposed security solution takes novel approach to implement the best security performance cryptography algorithms included AES, RSA and SHA-2, as a security layer within Distributed Network Protocol (DNP3) stack. This novel approach successfully enhanced the security of DNP3 protocol as a part of SCADA system while comparing with end-to-end security implementation.

Key words: Supervisory control and data acquisition, key encrption methods, DNP3 protocol security, cryptography algorithms, SCADA attacks/threads

INTRODUCTION

Enhanced Performance Architecture (EPA) model is simplified form of Open Systems Interconnection (OSI) seven layer model and is developed by International Electro Technical Commission (IEC). The Distributed Network Protocol 3 (DNP3) is based on this Enhanced Performance Architecture (EPA) model with additional pseudo-transport layer that performs limited functionality of transport and network layers of OSI model.

DNP3 protocol is one of important open protocol that has been used in SCADA communication "between master terminal station and remote terminal station and/or remote terminal station and master terminal station". Usually master terminal station initiates the command or sends data/message to remote terminal station and remote terminal station response according to master terminal station request.

DNP3 has three layers based on EPA model "such as application layer, data link layer and physical layer with pseudo-transport layer" that performs limited functionality of transport and network layers of OSI model. A prefix pseudo has used with transport layer because of limited functions from the existing transport and network layers of OSI model. The DNP protocol is used for both serial and Internet Protocol (IP) "Communication between master terminal station and remote terminal station".

With the uses of TCP/IP protocol; DNP3 provides communication over the internet between field devices connected in "Local Area Network (Lan)/Wide Area Network (WAN)". The DNP3 is situated at above than TCP/IP suite in the communication hierarchy for fairly communication over the internet. Figure 1 illustrates the stack (architecture) and communication flow of DNP3 protocol with TCP/IP suite (Clarke and Wright, 2013).

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

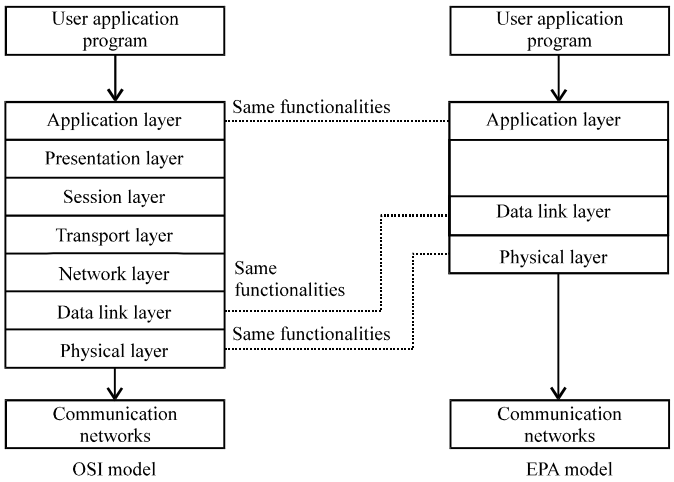

Fig. 1: Architecture and communication flow of OSI and EPA model

METHODOLOGY

Cryptographic solution (end-to-end implementation) has been developed to secure the SCADA serial communication between field devices within SCADA gas industry. Communication facts within gas and electrical industries have been analyzed in detail and also test the latency and session between field devices connected in SCADA network. Authentication security service for message/data communication between SCADA stations will achieve successfully during encryption/decryption process (using AES and SHA-1 hashing algorithm) (Musa *et al*., 2013a). Latency fact has been calculated AGA-12 test within SCADA communication between field devices and successfully checks the latency impact on different vendors devices included results as performance has been increase in Modbus protocol when comparison with Distributed Network Protocol (DNP3) while remote stations communication (in case of request) also gain high latency (impact) (Hadley *et al*., 2007; Musa *et al*., 2013b). Maize (2012), studied in detail the architecture of SCADA system and its connectivity with internet. Four major threads are specified from literature such as Cyber threads (malware, insider attacks, DoS, open access, Terrorism and crime, unauthorized access and hacker/tools), "Low-Latency Cryptography", Weak OS and Weak software and also some security recommendations are specify to secure SCADA from cyber threads such as strong network infrastructure, implementation firewalls, DMZs, IPSec, VPN, IDS, CRC and proper uses of OS and related software (William, 2013; Shahzad and Musa, 2012).

In proposed implementation also designated as Method[2], the Distributed Network Protocol (DNP3) model has been designed and the security ratio (%) has been measured against authentication, confidentiality and integrity and non-repudiation attacks, within specified layers. The symmetric AES algorithm and asymmetric RSA algorithm are used against authentication and confidentiality attacks within application layer and data link layer of DNP3 protocol. During encryption process; the bytes or data have not been encrypted itself, only the symmetric or secret key is appended with transmitted bytes. This key appended process saves the session because the latency is a major factor that has been counted during SCADA transmission or processing. The hashing algorithm using SHA-2 is used against integrity attacks within application layer, pseudo-transport layer and data link layer of DNP3 protocol. The secret key appended hashing digest is calculated first and then encryption is performed using RSA algorithm, this whole process performs the functionality of digital signature that provides protection against non-repudiation attacks. The Fig. 2 illustrates the whole encryption/decryption process within DNP3 protocol stack.

RESULTS AND DISCUSSION

SACDA testbed setup has been established successfully and network nodes have also been configured. Cryptography keys such as secret keys have been shared "between MTU and RTU and/or RTU and MTU" using secure channel (Shahzad *et al*., 2013, 2014a). In SCADA testbed, each node has two pairs of cryptography keys such as asymmetric (RSA) and symmetric (AES), with deployment of hash function within each layer of DNP3 protocol.

The main objective of current implementation provides a secure communication between SCADA nodes

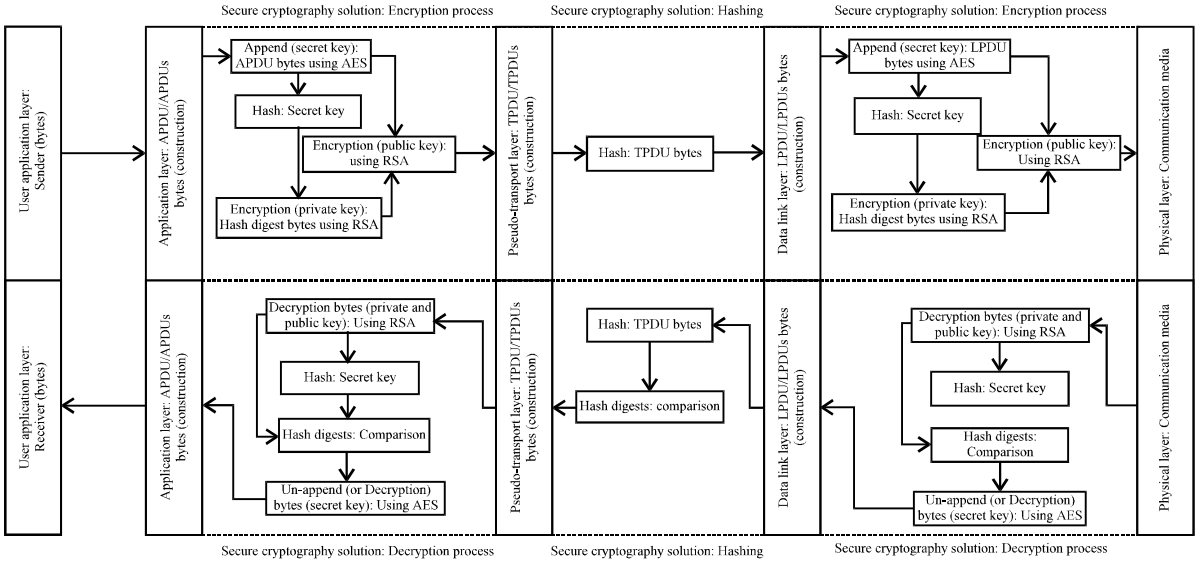

Fig. 2: Security implementation within DNP3 protocol stack

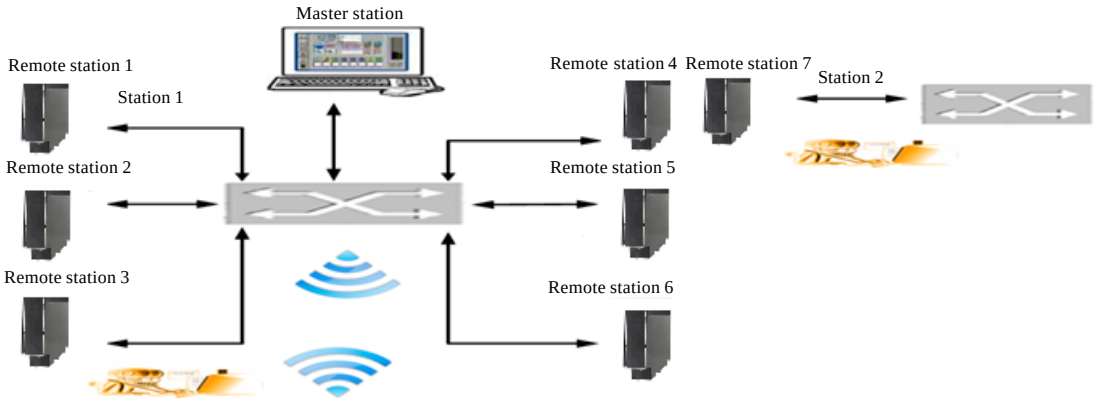

Fig. 3: SCADA/DNP3 testbed setup

such that master station can communicates with other nodes or remote stations/substations within SCADA network in secure manners and determined unambiguously that authorized remote nodes are communicating with master station. Remote stations are also determined unambiguously that authorized master node is communicating and accessing the services and operations of remote stations (Shahzad *et al*., 2013, 2014b).

DNP3 PROTOCOL MESSAGE STRUCTURE AND COMMUNICATION

In proposed implementation, communication has been initiated by master terminal unit and in few critical cases, remote terminal unit may initiate the communication. Master station with logical IP address and port number initiated the communication with remote terminal unit with logical IP address and port number. Random numbers of request bytes have been received from user application layer to DNP3 protocol for further processing or execution (Musa *et al*., 2013a). These numbers of bytes are being manipulated or constructed within DNP3 protocol and proposed security solution has also been implemented successfully within each layer such as application layer, pseudo-transport layer and data link layer before transmitting to remote terminal unit. Figure 3 illustrates the SCADA/DNP3 testbed setup between station1 and station 2.

Request bytes (dummy packet) structure and communication: DNP3 protocol application layer takes input message from user application layer or user interface and then make conversion into manageable blocks called Application Service Data Unit (ASDU) bytes. Each ASDU size has been limited or fixed upto 1990 bytes in case of message request and 1988 bytes in the case of message response. After construction of ASDU bytes, Application Header (AH) in both request and response are added with ASDU bytes, known as Application Protocol Data Unit (APDU) bytes. These APDU bytes will utilize as Transport Service Data Unit (TSDU) within pseudo-transport layer and then further utilize within data link layer such that TPDU bytes are treated as user bytes during construction of Link Protocol Data Unit (LPDU) bytes. Figure 4 illustrates the deployment process of message or bytes while transmitted from MTU (with IP address: 189.233.211.133 and logical port No. 2010) to RTU (with IP address: 189.233.211.155 and logical port No.2020) or request from MTU to RTU.

Application layer in Fig. 4, each offset within Application Protocol Data Unit (APDU) structure has been represented a packet and total number of packets are logical limited up to eight in length. The bytes within APDU structure in Fig. 4 are the application layer user bytes or data bytes.

The byte $OS_{0060}.R_{0005}.C_{0005}.B_{0005}$, represents the application control information or flow control and byte $OS_{0060}.R_{0005}.C_{0006}.B_{0006}$, is the application layer function code or code '0x0000' is utilized for confirmation.

The empty bytes $OS_{0060}.R_{0005}.C_{0007}.B_{0007}\_OS_{0060}.R_{0005}.C_{0010}.B_{0010}$ are represented the object header bytes. When APDU bytes have been constructed successfully then, cryptography proposed solution is deployed

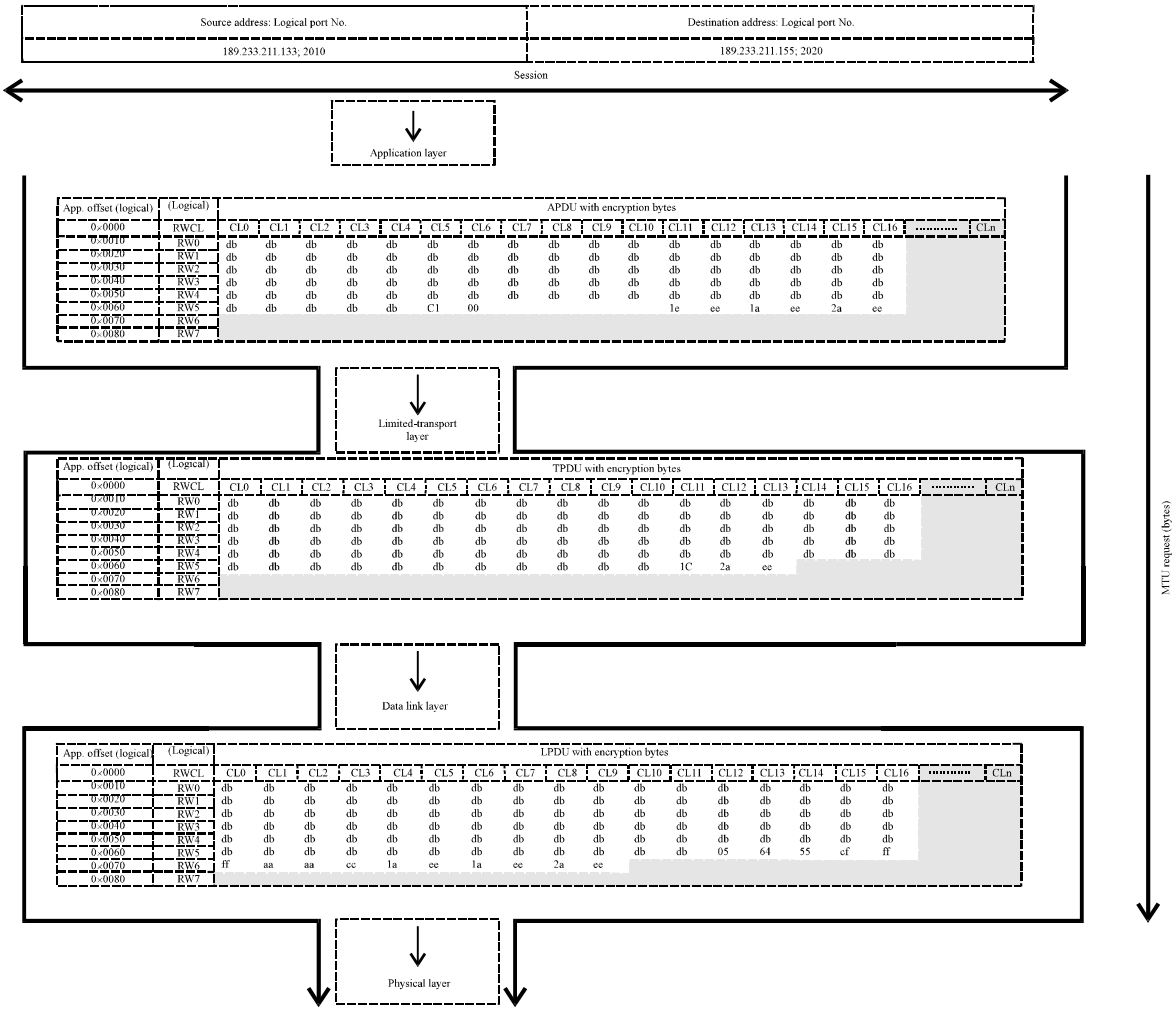

Fig. 4: MTU request bytes (structure and communication)

before transmitting to pseudo-transport layer. The bytes $OS_{0060}.R_{0005}.C_{0011}.B_{0011}\_OS_{0060}.R_{0005}.C_{0011}.B_{0016}$ are the cryptography information or bytes that have been utilized for security implementation.

Bytes format (hex):

$$OS_{xxxx}\text{-}R_{xxxx}\text{-}C_{xxxx}\text{-}B_{xxxx}$$

APDU (User bytes):

$OS_{0010}.R_{0000}.C_{0000}.B_{0000}\_OS_{0010}.R_{0000}.C_{0016}.B_{0016}$,

$OS_{0020}.R_{0001}.C_{0000}.B_{0000}\_OS_{0020}.R_{0001}.C_{0016}.B_{0016}$,

$OS_{0030}.R_{0002}.C_{0000}.B_{0000}\_OS_{0030}.R_{0002}.C_{0016}.B_{0016}$,

$OS_{0040}.R_{0003}.C_{0000}.B_{0000}\_OS_{0040}.R_{0003}.C_{0016}.B_{0016}$,

$OS_{0050}.R_{0004}.C_{0000}.B_{0000}\_OS_{0050}.R_{0004}.C_{0016}.B_{0016}$,

$OS_{0060}.R_{0005}.C_{0000}.B_{0000}\_OS_{0060}.R_{0005}.C_{0004}.B_{0004}$

Where:
OS = Offset
R = Row
C = Column
B = Bytes within APDU structure

Offset '0x0000' is utilized for initialization process of APDU.

The shaded bytes $OS_{0070}.R_{0007}.C_{0000}.B_{0000}\_OS_{0070}.R_{0007}.C....B...$ and $OS_{0060}.R_{0006}.C_{0000}.B_{0000}\_OS_{0060}.R_{0006}.C....B...$, or all shaded area or bytes within APDU will be utilized for future implementation or may allocated for dynamic buffer upon need.

Pseudo-transport layer in Fig. 4, each packet/segment or TPDU has random bytes but in the case of APDU or application layer buffer had been full, then each offset within pseudo-transport layer structure has been represented a packet or segment. Each TPDU size is limited up to 250 bytes. Total number of packets are logical limited up to eight in length while application layer buffer had been full. The below bytes within TPDU structure are the user bytes from upper layer.

Bytes format (hex):

$$OS_{xxxx}\text{-}R_{xxxx}\text{-}C_{xxxx}\text{-}B_{xxxx}$$

TPDU bytes (logical):

$OS_{0110}.R_{0001}.C_{0000}.B_{0000}\_OS_{0110}.R_{0000}.C_{0016}.B_{0016}$,

$OS_{0120}.R_{0001}.C_{0000}.B_{0000}\_OS_{0120}.R_{0001}.C_{0016}.B_{0016}$,

$OS_{0130}.R_{0002}.C_{0000}.B_{0000}\_OS_{0130}.R_{0002}.C_{0016}.B_{0016}$,

$OS_{0140}.R_{0003}.C_{0000}.B_{0000}\_OS_{0140}.R_{0003}.C_{0016}.B_{0016}$

$OS_{0150}.R_{0004}.C_{0000}.B_{0000}\_OS_{0150}.R_{0004}.C_{0016}.B_{0016}$

$OS_{0160}.R_{0005}.C_{0000}.B_{0000}\_OS_{0160}.R_{0005}.C_{0004}.B_{0004}$

Where:
OS = Offset
R = Row
C = Column
B = Bytes with each APDU

The byte $OS_{0160}.R_{0005}.C_{0011}.B_{0011}$ represents the pseudo-transport layer header or TH control information (flow control) and bytes $OS_{0160}.R_{0005}.C_{00012}.B_{00012}.OS_{0160}.R_{0005}.C_{0013}.B_{0013}$ are the cryptography information that have been utilized for security implementation.

In data link layer (Fig. 4), each packet has also random bytes but in the case of APDU or application layer buffer had been full, then each offset within data link layer has been logically represented a packet or frame. Each LPDU size is limited up to 292 bytes with CRC bytes, with user bytes up to 250 bytes from upper layer. Total numbers of packets are logical limited up to eight in length while application layer buffer had been full. The below bytes within LPDU structure are the user bytes from upper layer.

Bytes format (hex):

$$OS_{xxxx}\text{-}R_{xxxx}\text{-}C_{xxxx}\text{-}B_{xxxx}$$

LPDU bytes (logical):

$OS_{0210}.R_{0000}.C_{0000}.B_{0000}\_OS_{0210}.R_{0000}.C_{0016}.B_{0016}$,

$OS_{0220}.R_{0001}.C_{0000}.B_{0000}\_OS_{0220}.R_{0001}.C_{0016}.B_{0016}$,

$OS_{0230}.R_{0002}.C_{0000}.B_{0000}\_OS_{0230}.R_{0002}.C_{0016}.B_{0016}$,

$OS_{0240}.R_{0003}.C_{0000}.B_{0000}\_OS_{0240}.R_{0003}.C_{0016}.B_{0016}$,

$OS_{0250}.R_{0004}.C_{0000}.B_{0000}\_OS_{0250}.R_{0004}.C_{0016}.B_{0016}$,

$OS_{0260}.R_{0005}.C_{0000}.B_{0000}\_OS_{0260}.R_{0005}.C_{0004}.B_{0013}$

Where:
OS = Offset
R = Row
C = Column
B = Bytes with each APDU

The bytes $OS_{0260}.R_{0005}.C_{00014}.B_{00014\_}$, $OS_{0260}.R_{0005}.C_{0016}.B_{0016}$ and $OS_{0270}.R_{0005}.C_{0000}.B_{0000}$, $OS_{0270\_}R_{0005}.C_{0003}.B_{0003}$ represent the data link layer header or LH and bytes $OS_{0270}.R_{0006}.C_{00004}.B_{0004}$, $OS_{0270\_}R_{0006}.C_{009}.B_{0009}$ are the cryptography information (bytes) that have been utilized for security implementation. When MTU request message has been constructed successfully with deployment of proposed security solution, then message is ready to transmit to RTU.

Response bytes: Structure and communication: Upon receiving MTU request message, RTU generates the response message according to request message. Figure 5 illustrates the deployment process of response message or bytes.

While transmitted from RTU with IP address: 189.233.211.155 and logical port No. 2020 MTU with IP address: 189.233.211.133 and logical port No. 2010 or response from RTU to MTU. The pseudo-transport layer and data link layer specifications for response message construction are same as MTU request message in pseudo-transport layer and data link layer of DNP3. No changes has been taken place within response message. In APDU response structure, the bytes $OS_{0070}.R_{0006}.C_{0007}.B_{0007}$, $OS_{0007\_}R_{0006}.C_{0008}.B_{0008}$ are representing the application layer 'IIN (internal indication) or response bytes. Internal indication is two bytes fields follow by function code and used to send response message to master station or uses within response message.

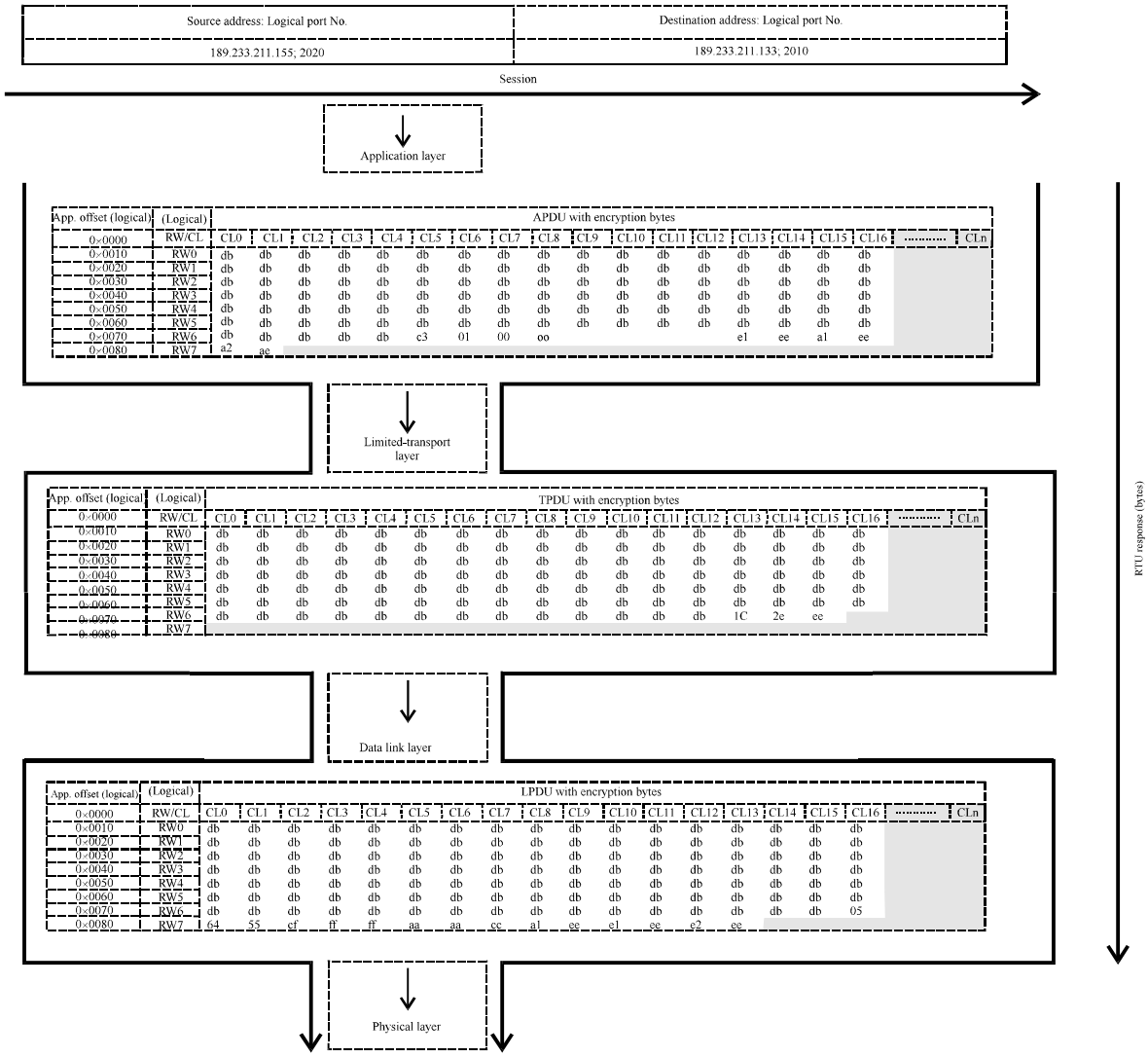

Fig. 5: RTU response bytes (structure and communication)

Each bit within IIN fields ($IIN_{S(0.1)}$_$IIN_{E(1.7)}$ and $IIN_{S(2.0)}$_$IIN_{E(2.7)}$) has specific meaning for response message. The below bytes are the cryptography information or bytes that have been utilized for security implementation.

Bytes format (hex):

$$OS_{XXXX}\text{-}R_{XXXX}\text{-}C_{XXXX}\text{-}B_{XXXX}$$

APDU/LPDU security bytes (logical):

$$OS_{0070}.R_{0006}.C_{0013}.B_{0013}\_OS_{0070}\_R_{0006}.C_{0013}.B_{0016}$$

TPDU security bytes (logical):

$$OS_{0080}.R_{0007}.C_{0000}.B_{0000},\ OS_{0080}\_R_{0006}.C_{0013}.B_{0016}$$

Where:

S = Start value

E = End value within internal indication fields or $IIN_{S(1.0)}$_$IIN_{E(1.7)}$ and $IIN_{S(2.0)}$_$IIN_{E(2.7)}$

The pseudo-transport layer and data link layer specifications for response message construction remain same as MTU requested message in pseudo-transport layer and data link layer of DNP3 but different cryptography information are utilized which also distinguished the request and response message.

Figure 6 shows the performance (results) during attacker attack or ratio of authentication, confidentiality, integrity and non-repudiation attacks that have been successful during SCADA/DNP3 testbed communication using Method[2].

The proposed Method[2] has been implemented successfully within SCADA/DNP3 communication and all security services are achieved successfully.

In performance Fig. 7, Method[2] has been implemented at each end of SCADA/DNP3 communication. The red and black color) markers are representing the authentication and confidentiality attacks while orange and brown color markers are representing the integrity and non-repudiation attacks. As conclusion, the attack detection ratio (%) and impact ratio (%) are comparatively high, with the implementation of Method[1] during end-to-end communication while this ratio (%) has been very low, within SCADA/DNP3 testbed communication within DNP Protocol stack.

In Fig. 8, the latency or propagation delay has been measured and comparison is created between both communications as Method[2] within and end-to-end SCADA/DNP3. The blue line in Fig. 8 shows the high latency while measured within DNP3 testbed or DNP3 protocol stack and red line in Fig. 8 shows the low latency by implementation of Method[2], at each end of SCADA/DNP3 communication. The Table 1 shows the

Table 1: Security performance (results)

Testbed	Attack detection (%)	Attack impact (%)	Security (%)
With DNP3 security	8	3	97
End-to-end security	31	21	79

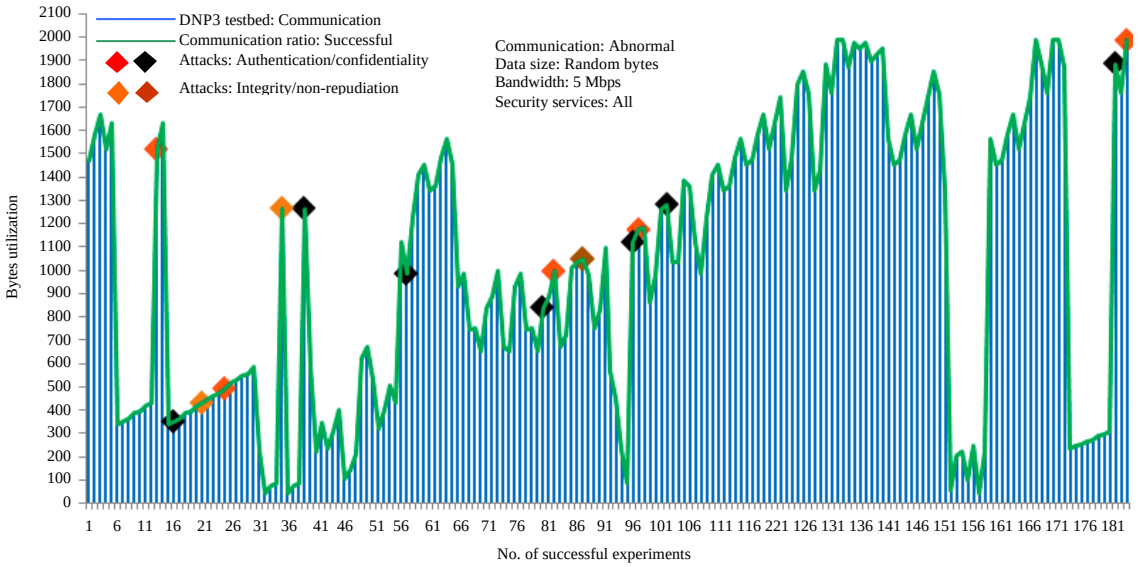

Fig. 6: Performance results during abnormal communication (MTU/RTU)

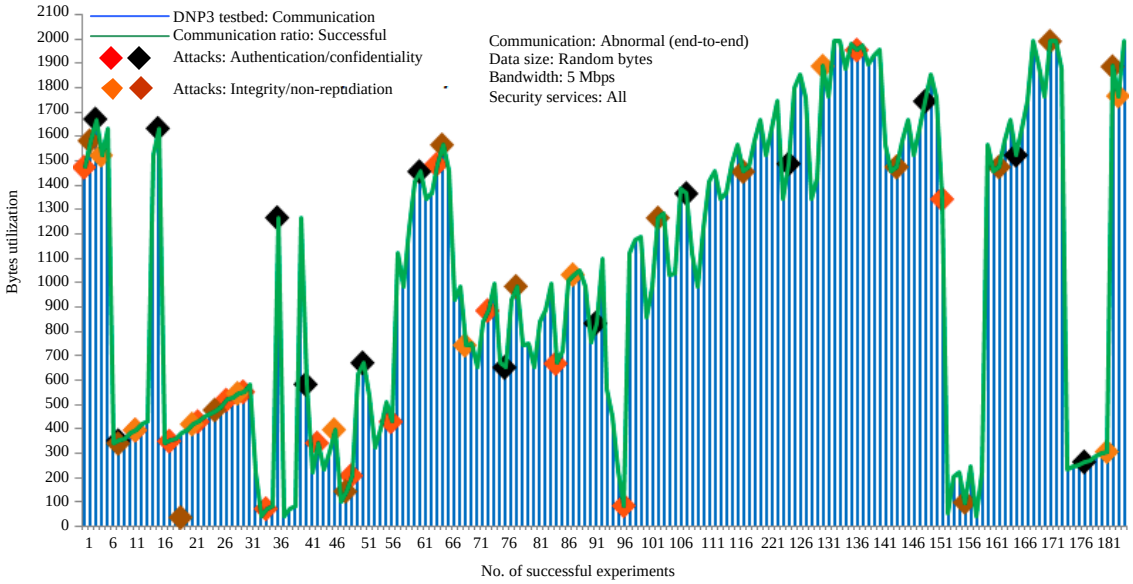

Fig. 7: End-to-end, abnormal communication

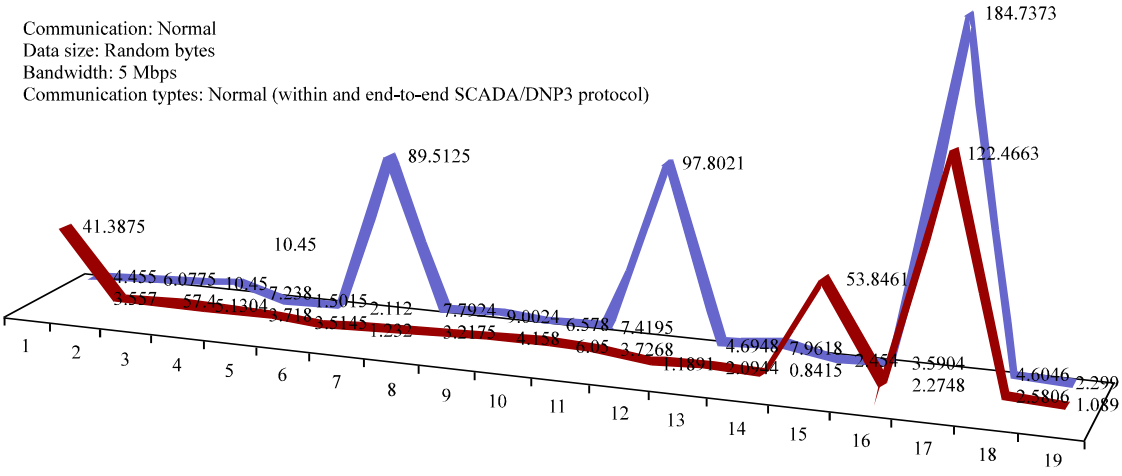

Fig. 8: Latency comparison using method[2]

overall security performance included attack detection, impact and security ratio (%).

CONCLUSION

In this study, the analysis based on SCADA/DNP3 security issues has been conducted and potential security solution is deployed to enhance the security of these critical systems. In implementation phase, DNP3 protocol stack has been designed and the security using cryptography solution is deployed within DNP3 protocol layers. The performance results included attack detection ratio (%), attack impact ratio (%) and security ratio (%) have been observed and also comparison is created with end-to-end performance results which are significantly low in the terms of security ratio (%) and high in the case of attack detection ratio (%) and attack impact ratio (%).

In this implementation, unbalance system is used within SCADA/DNP3 communication, mean that only master station can be initialized or able to send the request and terminal stations will response according to master request. But there is also need to implements the balanced system within SCADA/DNP3 communication. In balanced system; each station within SCADA hierarchical

network, act as master or slave station together or any station is authorized to send the request and response message.

REFERENCES

Clarke, D. and E. Wright, 2013. Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Elsevier, Paris, pp: 73-129.

Hadley, M.D., K.A. Huston and T.W. Edgar, 2007. AGA-12, Part 2 performance test results. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/9-AGA-12_Part_2_Performance.pdf

Maize, K., 2012. Cyber threats to SCADA systems are real. http://www.managingpowermag.com/it/Cyber-SCADA-Systems-Are-Real-_388.html

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.

Shahzad, A. and S. Musa, 2012. Cryptography and authentication placement to provide secure channel for SCADA communication. Int. J. Secur., 6: 28-44.

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.

William, T.S., 2013. SCADA system vulnerabilities to cyber attack. Electric Energy, http://www.electricenergyonline.com/show_article.php?mag=&article=181