Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 9 (7): 381-395, 2014
ISSN 1819-3579 / DOI: 10.3923/tasr.2014.381.395

N-Secure Cryptography Solution for SCADA Security Enhancement

[1]A. Shahzad, [1]S. Musa and [2]M. Irfan
[1]Malaysian Institute of Information Technology, 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, 1016, Jalan Sultan Ismail, Universiti Kuala Lumpur, 50250, Kuala Lumpur, Malaysia

ABSTRACT

In the initial structure (or design) of SCADA system, there is no security mechanism that provides services or solutions for preventing and detecting the communication attacks over internet. "Using modern communication facilities, SCADA platform is vulnerable from different types of internet attacks that create major problems" within communication in the terms of security, reliability, scalability and other performance parameters. The existing study related with SCADA security implementations have been analyzed and then propose a solution which is based on asymmetric and symmetric cryptography algorithms. In this proposed implementation, the prototype for Distributed Network Protocol (DNP3) has been developed which is based on "application layer, pseudo-transport layer and data link layer" of DNP3 protocol. Current solution takes bytes (user data) from DNP3 layers and deploys the proposed solution as new security layer within each layer of DNP3. A "dynamic cryptography buffer" has been deployed and utilized during whole security implementation within DNP3 protocol. When the proposed implementation has been deployed and the security services "(such as authentication, integrity, confidentiality and non-repudiation)" are tested (verified) successfully "between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and RTUs and MTU", then the attacks (related with security services) such as shared key guessing, brute force, cracking key, man-in-the-middle, packet/data injection, packet/data replay and deletion have launched, using built-in tools as attacker and the performance (results) are measured based on system behavior.

Key words: Supervisory control and data acquisition, DNP3 protocol security, cryptography algorithms, performance results, SCADA communication attacks

INTRODUCTION

Distributed Network Protocol (DNP3) deployment within real time industries or sectors is increasing day-by-day in all over the world, more especially in continent America, Asia, Europe and Australia. The real time infrastructures have been deploying DNP3 protocol widely to control, monitors and access the data across several connected stations or devices, with utilization of enhanced communication features which made system (or network) performance more convenient and reliable (Stouffer *et al*., 2007; NCS, 2004).

With the increasing requirements of real time infrastructures, the Distributed Network Protocol (DNP3) provides enhance features, to make connection with number of advance networks over

internet using of Transport Control Protocol (TCP)/Internet Protocol (IP). "Distributed Network Protocol (DNP3) stood at the upper level from Transport Control Protocol (TCP)/Internet Protocol (IP) which made reliable delivery of data while connecting with internet".

DNP3 PROTOCOL STACK WITH CRYPTOGRAPHY DYNAMIC BUFFER

DNP3 protocol has defined and used three layers in its stack included "application layer, data link layer and physical layer" and also has additional pseudo-transport layer which perform the limited functions and features of transport layer and network layer, defined from Open Systems Interconnection model (OSI). In DNP3 protocol, application layer takes random user data (bytes) from upper layer called user application layer or via., user interface that are supported and defined for communication (DNP3 protocol communication). The user bytes from upper layer is treated as Application Services Data Unit (ASDU) bytes. Application layer adds header bytes with assembled Application Services Data Unit (ASDU) bytes and this process is designated as Application Protocol Data Unit (APDU) or APDU bytes. The size of ASDU bytes are not limited or fixed, these bytes are followed by user application layer or user interface. At the other side, each Application Protocol Data Unit (APDU) bytes or size is limited upto 1992 bytes (the original APDU sized is upto 2048 bytes while the APDU size is limited upto 1992 bytes and remaining 56 bytes are utilized for "dynamic cryptography buffer" implementation) but bytes are distinct in the case of request and response headers. During application layer bytes construction, request header consists of 2 bytes, while response header size is upto 4 bytes in APDU bytes. In case, large numbers of bytes have been received from user layer than multiple APDU bytes are constructed and also designated as fragments.

Upon receiving, the bytes from upper layer (Application Layer of Distributed Network Protocol or DNP3) to pseudo-transport layer, these upcoming bytes are treated as transport layer user data or Transport Services Data Unit (TSDU) bytes. These bytes (TSDU bytes) are further divided into small units and each unit size is upto 249 bytes. The pseudo-transport layer then adds 1 byte of header field with each divided unit and designed as Transport Protocol Data Unit (TPDU) or TPDU bytes. Each Transport Protocol Data Unit (TPDU) bytes can easily fixed within Link Protocol Data Unit (LPDU) bytes within data link layer of DNP3 protocol. Data link layer has been received the Link Service Data Unit (LSDU) bytes and adds 10 bytes of header field, this process is also designed as Link Protocol Data Unit (LPDU) bytes. Each Link Protocol Data Unit (LPDU) contains 32 bytes, Cyclic Redundancy Code (CRC) which is used to detect error during transmission of LPDU bytes or frame, size upto 292 bytes (NCS, 2004). Figure 1 illustrates the DNP3 protocol stack and communication flow between sender and receiver.

MATERIALS AND METHODS

SCADA system implementation using control protocols such Distributed Network Protocol (DNP3), fieldbus, modbus and other IP protocols are harmfully and critical for SCADA communication between field devices, because these protocols are design without any security concerned that fully or partially provide protection against cyber attacks. Firewalls are uses between SCADA system and corporate networks or internet but are unable to fully integrate with SCADA networks (system), such as in term of SCADA protocols (DNP3 or Modbus) development and configuration. So, lack of security information and configuration with protocols, increasing more vulnerabilities for SCADA platform and causing major security issues for critical infrastructure (Cai *et al*., 2008; Shahzad and Musa, 2012; Ismail *et al*., 2013).

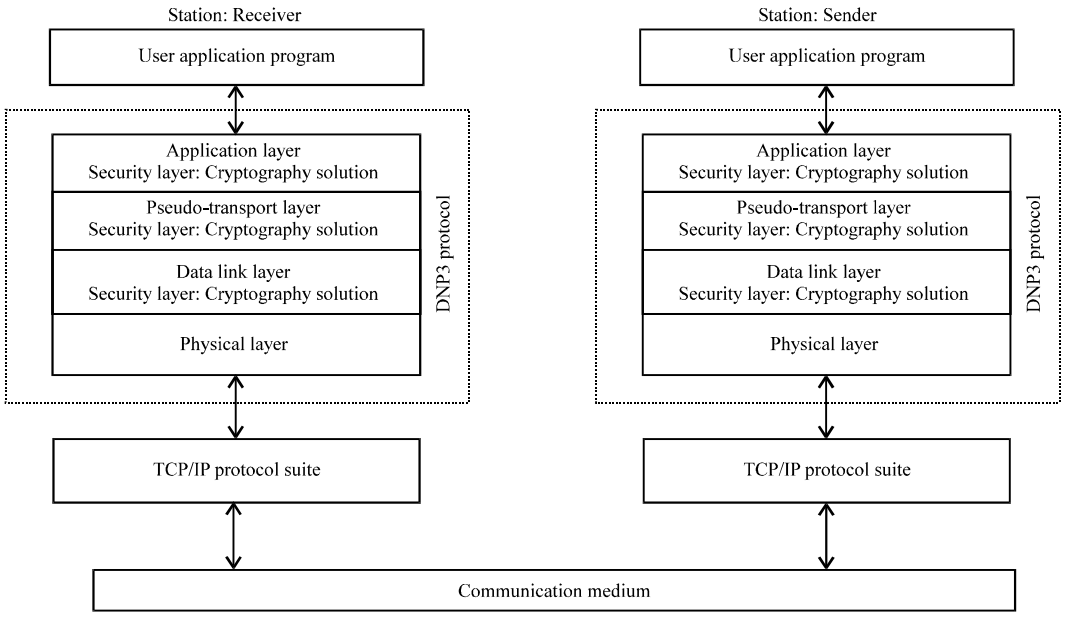

Fig. 1: DNP3 protocol communication flow with TCP/IP protocol suite

Asymmetric cryptography algorithm has been uses to secure SCADA communication between master station (control center) and cell phone. The communications between two stations (nodes) have been take place by using GPRS and WAP. Asymmetric algorithm uses two keys such as public and private. The SCADA communication is initial between master and remote station (cell phone). The message/data digest is calculate by using hash function and hash digest is encrypted by private key (Digital Signature Algorithm or DSA). Public key is uses to encrypt the private message-digest and sent to remote station. On remote station received, first public key is uses to decrypted the private message-digest and then message hash function is perform to compare with master hash digest (Musa *et al*., 2013b; Shahzad *et al*., 2013). Usually RSA algorithm uses 1024 and 2028 key size and much slower when compare with symmetric algorithms. Detail results have been calculated from implementation and security services such authentication and data integrity successfully perform during "communication between master station and remote station or/and remote station and master station". So, this is not possible for attacker to attack on SCADA system when ever connected with internet (Permann and Rohde, 2005; Robles and Kim, 2011).

In proposed implementation or designated as Method[1], the cryptography algorithms such as AES and RSA have been deployed to secure the SCADA/DNP3 communication, against authentication and confidentially attacks and SHA-2 hashing algorithm is deployed against integrity attacks. The function called "digital signature" has been generated which is based on hashing (using SHA-2) and RSA algorithm that provides the security against non-repudiation attacks. Figure 2 illustrates the whole cryptography implementation within DNP3 protocol stack as a part of SCADA system.

TESTBED SETUP AND CONFIGURATION

In order to measure the performance results, SCADA/DNP3 communication setup (Testbed) has been established (for capturing or measuring results). In testbed setup, seven Remote Terminal Units (RTUs) included RTU1, RTU2, RTU3, RTU4, RTU5, RTU6 and RTU7 are connected with

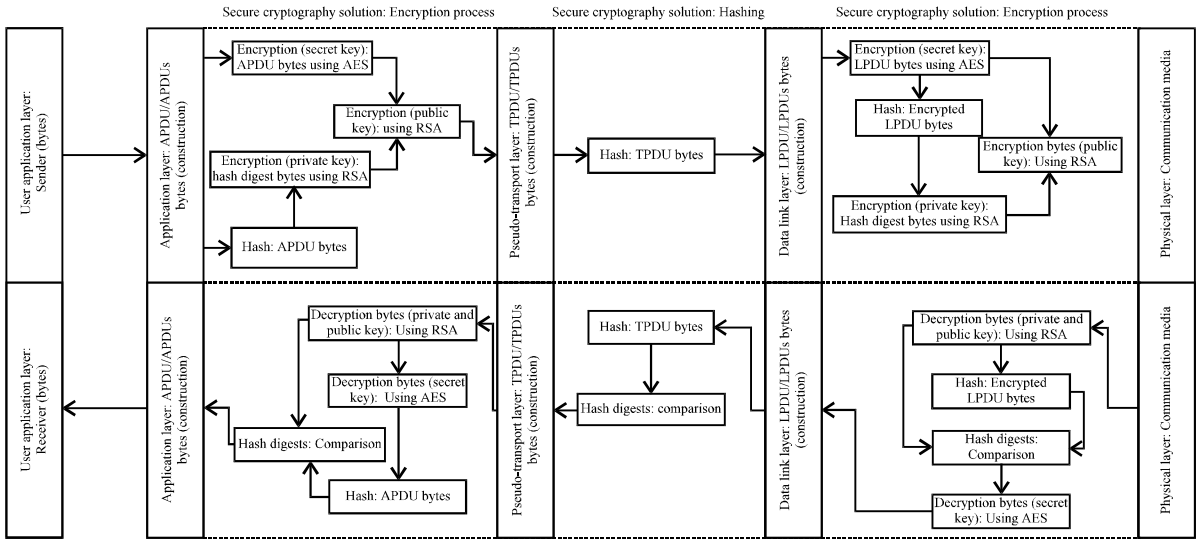

Fig. 2: Cryptography implementation within SCADA/DNP3 protocol stack

Master Terminal Unit (MTU) in station1 and station2. In station1; RTU1, RTU2, RTU3, RTU4, RTU5, RTU6 are directly connected with Master Terminal Unit (MTU) or master station using switch within Local Area Network (LAN) while RTU7 is located at station 2, distance away from station1 within Wide Area Network (WAN). The testbed communication is carried out successfully between station1 and station2, using two different Malaysian telecom connection (or Unifi connections). Both station1 (LAN) and station2 (WAN) are using Malaysian telecom connection (Unifi connections), with the bandwidth upto 5 Mbps (Musa *et al*., 2013a, b; Shahzad *et al*., 2013).

The data/information has been send and received several times "between Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) or/and Remote Terminal Unit (RTU) and Master Terminal Unit (MTU)", with bandwidth upto 5 Mbps. The performance results are measured from SCADA/DNP3 testbed is two fold in the case of normal communication (for latency measurement) and case of abnormal communication or attacker attack (Shahzad *et al*., 2014).

"The testbed experiments have been run several times and carefully performance results are observed in both normal and abnormal communication/traffic" and performance (latency) contents are measured, using format Hour: Minute: Second: Millisecond or hh:mm:ss:ms. Figure 3 illustrates the SCADA/DNP3 testbed communication setup.

PERFORMANCE MEASUREMENT AND DISCUSSION

Several times random bytes (data) have been transmitted "between MTU and RTU and/or RTU and MTU". Master station initial the communication and then send data (bytes) to RTU. Upon message (data) receiving, RTU has been ensuring that all "security services such as authentication, integrity, confidentiality and non-repudiation, achieved successfully" and communication has been done (completed) error free or without any attack. When response has been generated and RTU send the response to MTU. Upon receiving, master station also ensures that "all security services such as authentication, integrity, confidentiality and non-repudiation, achieved successfully" and communication has been done (completed) error free or without any attack. Figure 4 illustrates the

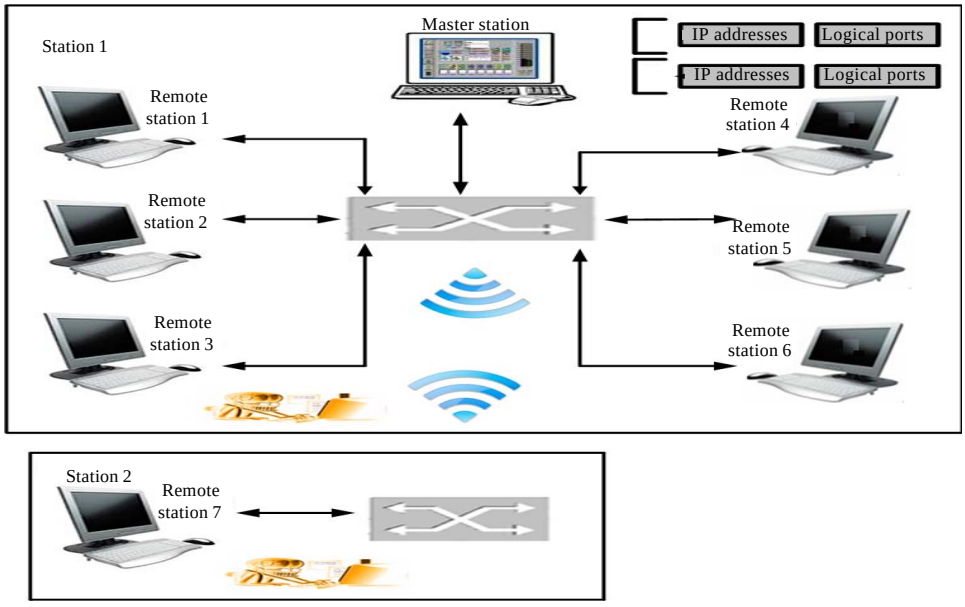

Fig. 3: SCADA/DNP3 testbed communication setup

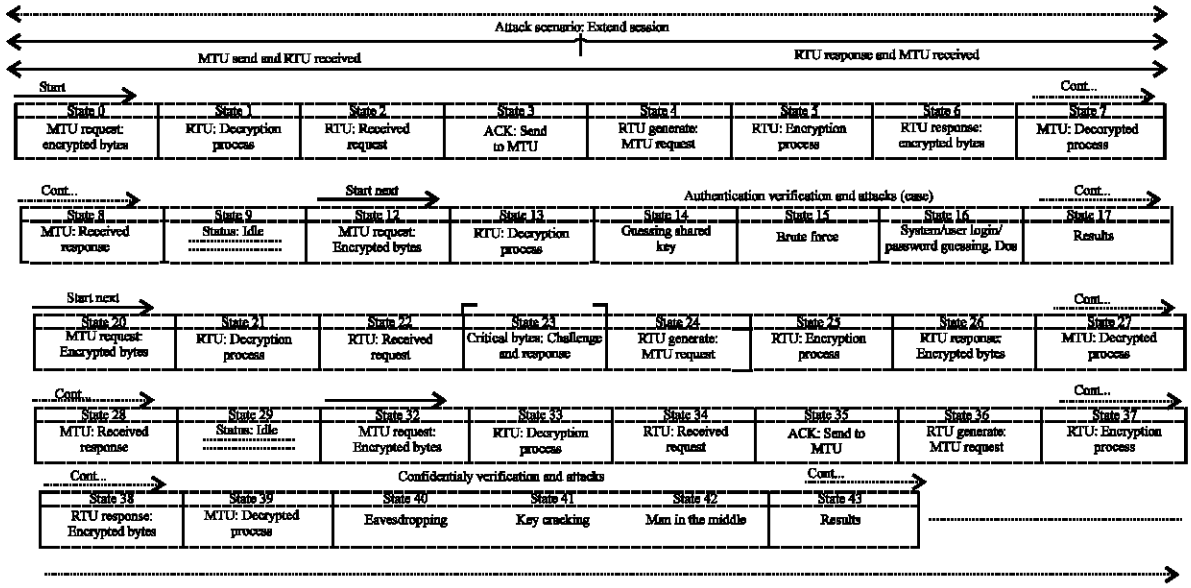

Fig. 4: Normal/abnormal communication (with authentication and confidentiality attacks)

communication (normal and abnormal) sequence between MTU and RTU and/or RTU to MTU. The security ("security services such as authentication and confidentiality") has been also verified (tested), upon receiving of message (request/response).

In Fig. 4, state 0_state 12 shows the complete encryption/decryption process, included master station sends request and remote station sends the response. The security services such as "authentication, integrity, confidentiality and non-repudiation", have been also verified by

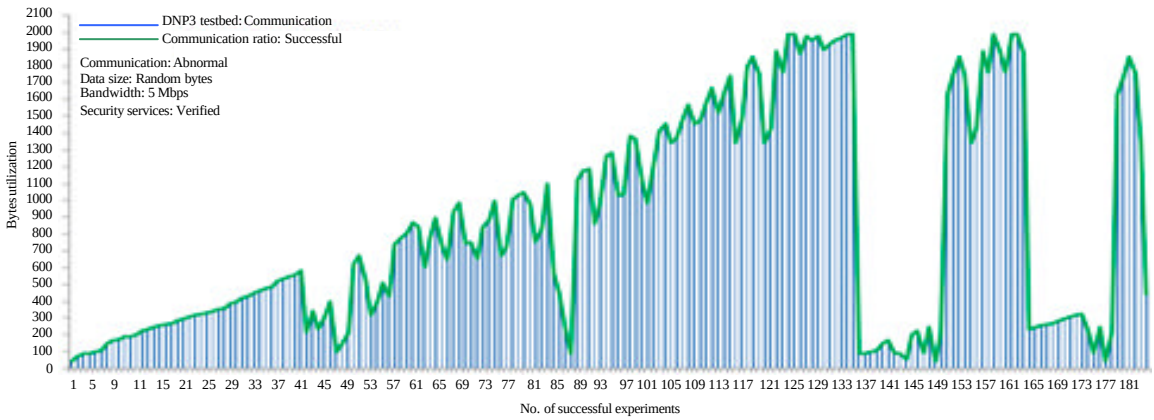

Fig. 5: Normal communication between SCAD/DNP3 nodes

MTU/RTU upon message (bytes) receiving (request/response). The performance Fig. 5, show the successful normal communication between master station and remote station or vice versa.

During communication, several time attacks have been launched to intercept the communication and again control on SCADA system. In Fig. 4, state 14__state16 are authentication attacks included guessing shared key, brute force, system/user login/password guessing and DOS that have been launched successfully within communication. "Figure 6 shows the performance (results) during attacker attacks or ratio (%) of authentication attacks that have been successful during communication (with and without using Method[1]). In Fig. 6a shows the performance (results) with implementation of Method[1] while right side representing the performance (results) without implementation of Method[1"].

During communication, critical bytes have been received at state 23 (Fig. 4). At this state, critical bytes mean, bytes may not be transmitted included bytes loss during communication, message or packet incomplete constructed and transmitted, time increased and no feedback from target device. All these scenarios are taken place due to network connection problems or other (no attacker case). If these types of situations happen, then challenge/response solution will deploy on specific bytes which had been loosed during communication, not on whole message. In Fig. 4, the state 40, 41 and 42 are confidentiality attacks included eavesdropping, key cracking and man-in-the-middle which have been launched successfully within communication.

"The Fig. 7 shows the performance (results) during attacker attack or ratio of confidentiality attacks that have been successful during communication (with and without using Method[1]). In Fig. 7a shows the performance (results) with implementation of Method[1] while right side representing the performance (results) without implementation of Method[1"].

In Fig. 8, from state 110-153, the communications has been continued and all security services are also verified, successful during communications. The state 154, 155 and 156 are the integrity attacks included frame injection, data replay and data deletion that have been launched successfully within communication. "Figure 9 shows the performance (results) during attacker attack or ratio of integrity attacks that have been successful during communication (with and without using Method[1]). In Fig. 9a shows the performance (results) with implementation of Method[1] while right side representing the performance (results) without implementation of Method[1"].

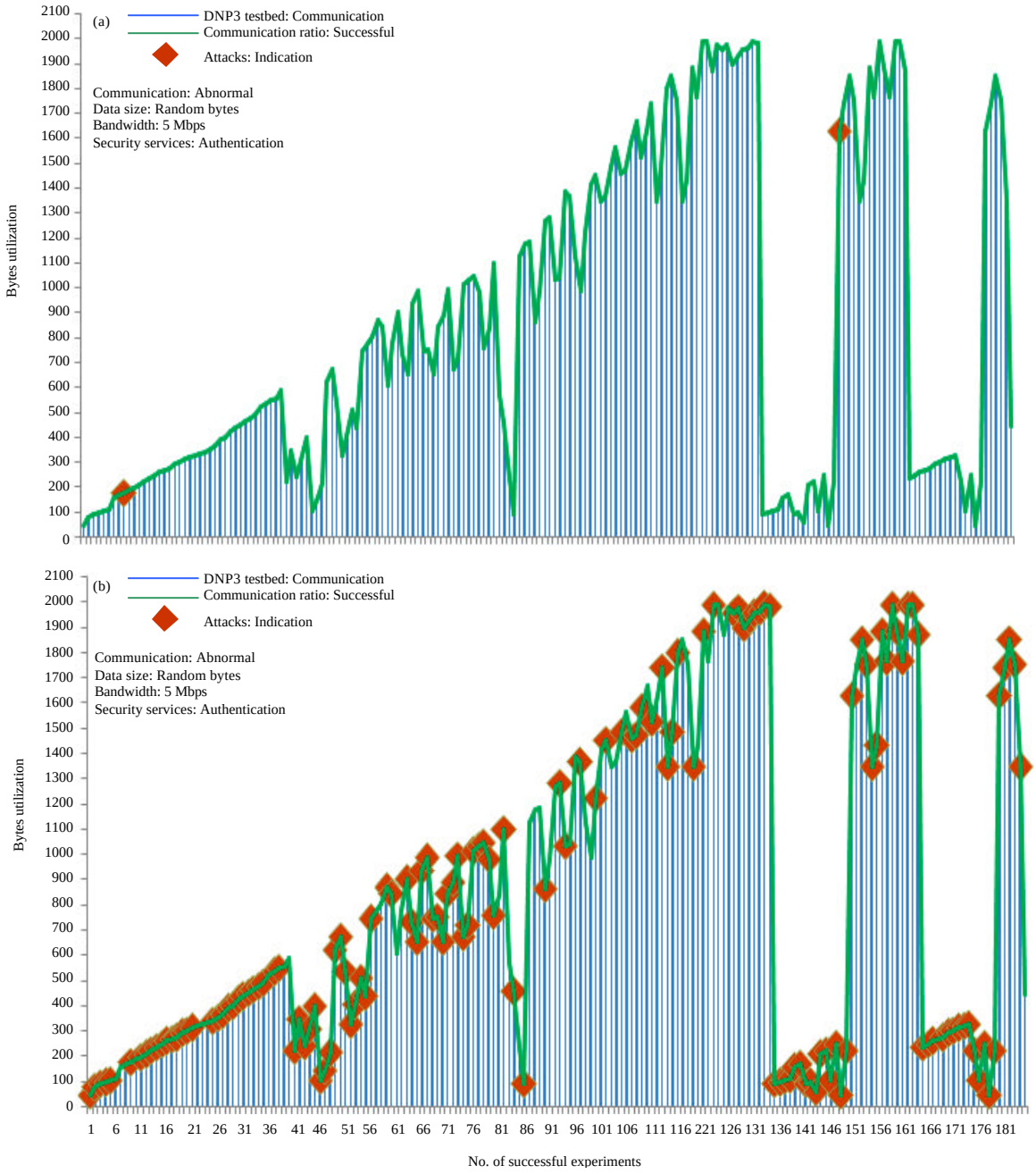

Fig. 6(a-b): Authentication attacks: Performance results during communication (MTU/RTU)

In Fig. 8, from state 158-299, the communications has been continued and all security services are also verified successful. At the state 303, RTU verified the non-repudiation function (using digital signature) and after verification, acknowledgement (message) has been transmitted to MTU. At the state 309, MTU also verified the non-repudiation function and after verification, acknowledgement (message) has been transmitted to RTU. Thus, verification (non-repudiation function) shows that error free communication has been occurred between MTU and RTU.

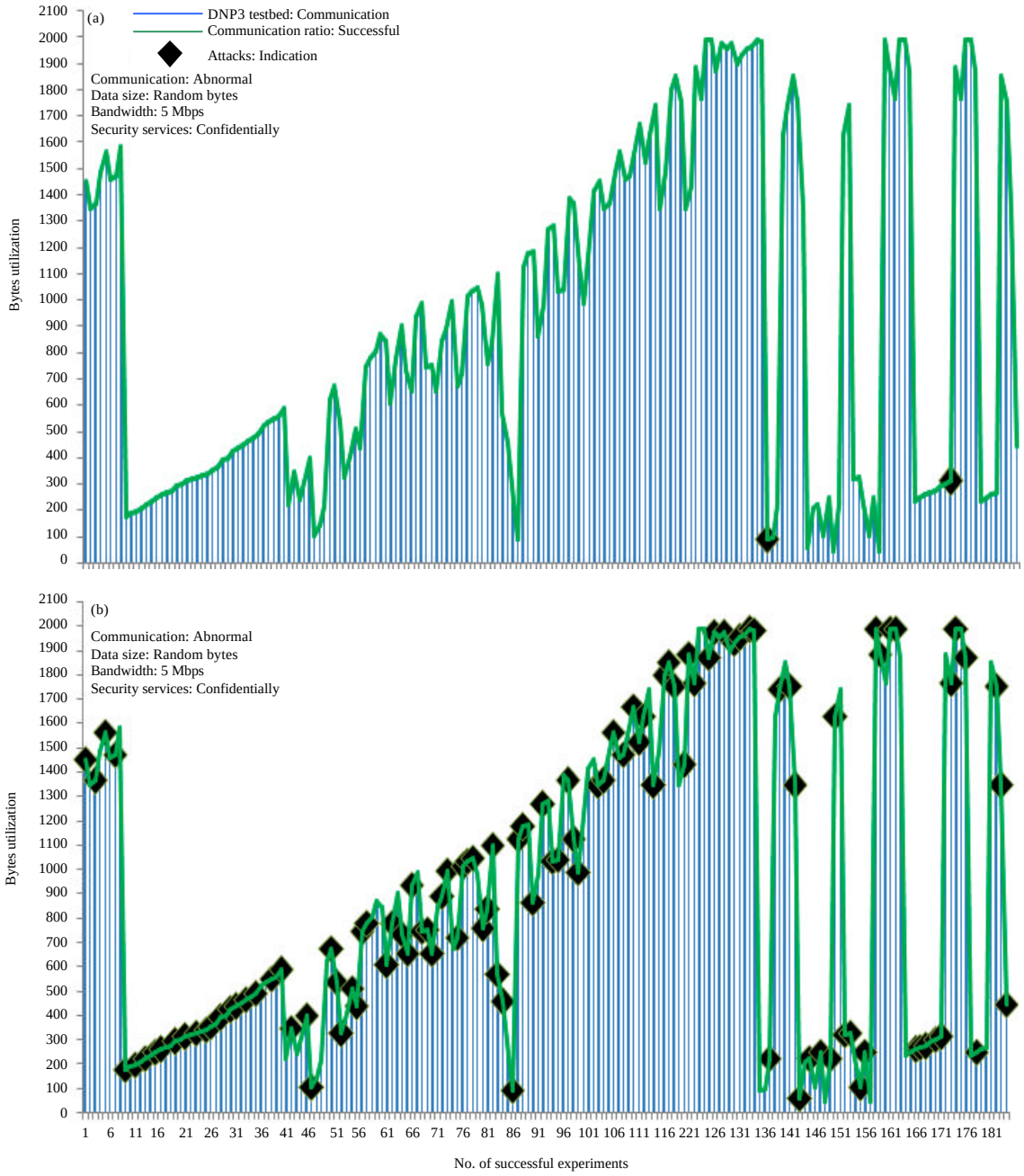

Fig. 7(a-b): Confidentiality attacks: Performance results during communication (MTU/RTU)

"Figure 10 shows the performance (results) during attacker attack or ratio of non-repudiation attacks that have been successful during communication (with and without using Method[1]). In Fig. 10a shows the performance (results) with implementation of Method[1] while right side representing the performance (results) without implementation of Method[1*].

In performance Fig. 11-12, Method[1] has been implemented at each end of SCADA/DNP3 communication. The Fig. 11a-b show the authentication and confidentiahty attacks (detection) with

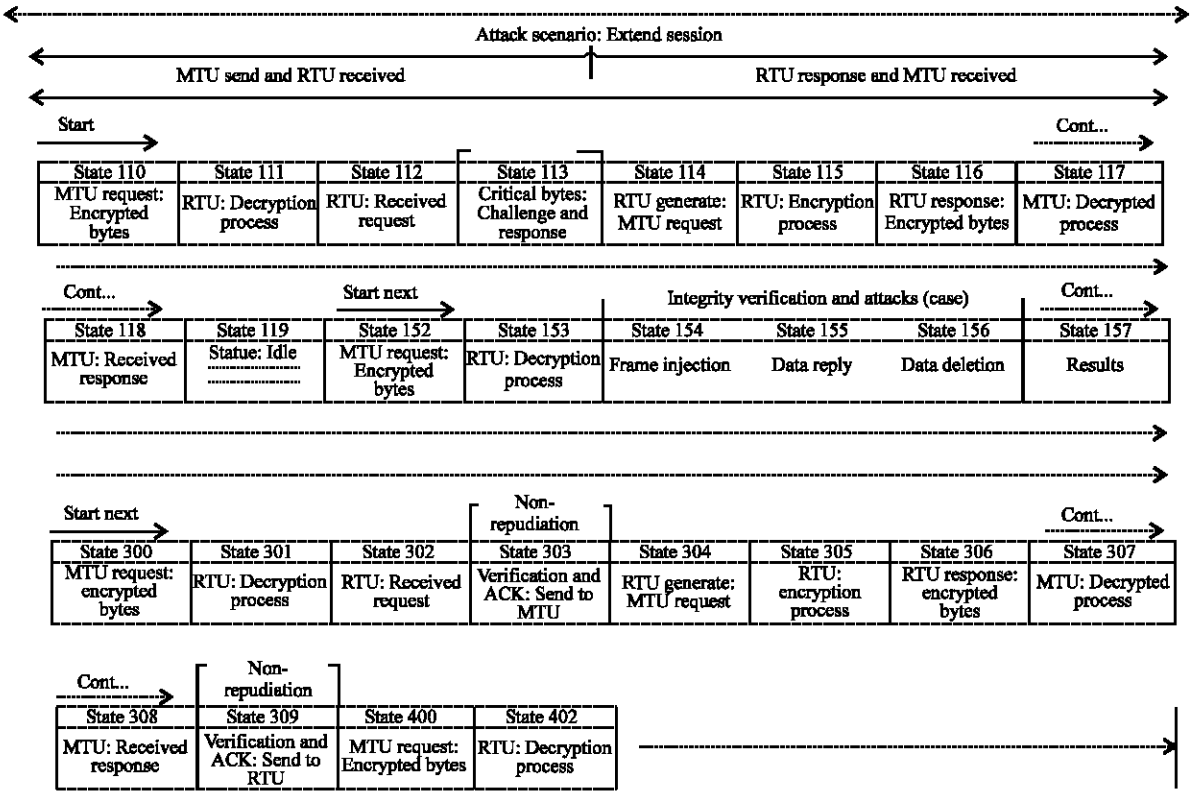

Fig. 8: Normal/abnormal communication (with integrity and non-repudiation attacks)

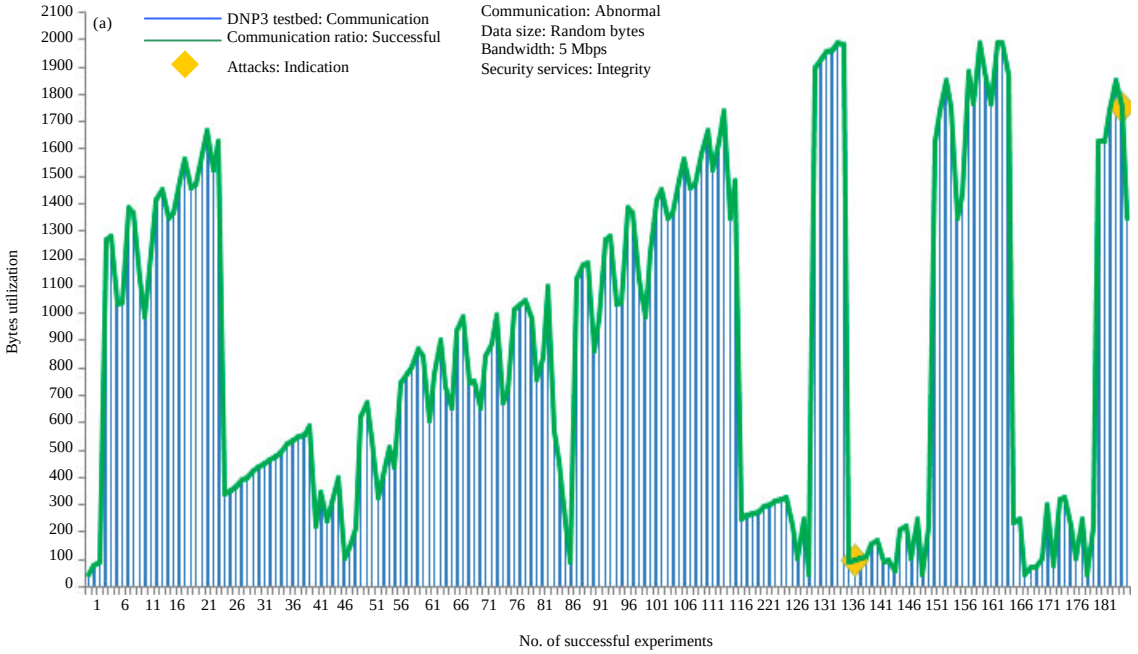

Fig. 9(a-b): Continue

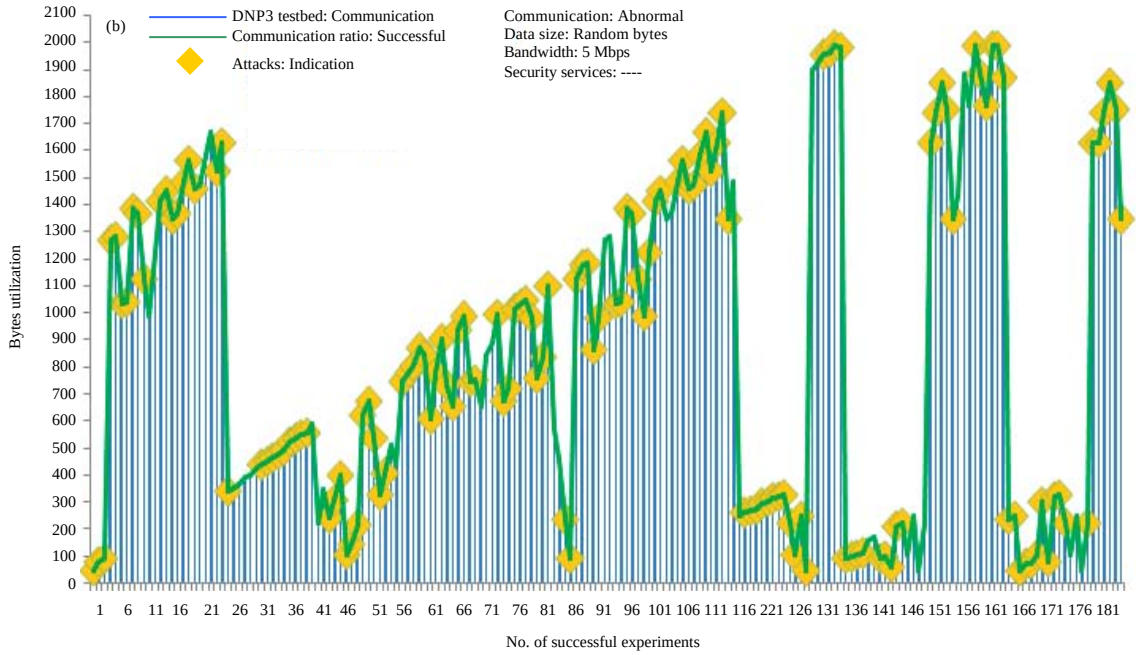

Fig. 9(a-b): Integrity attacks: Performance results during communication (MTU/RTU)

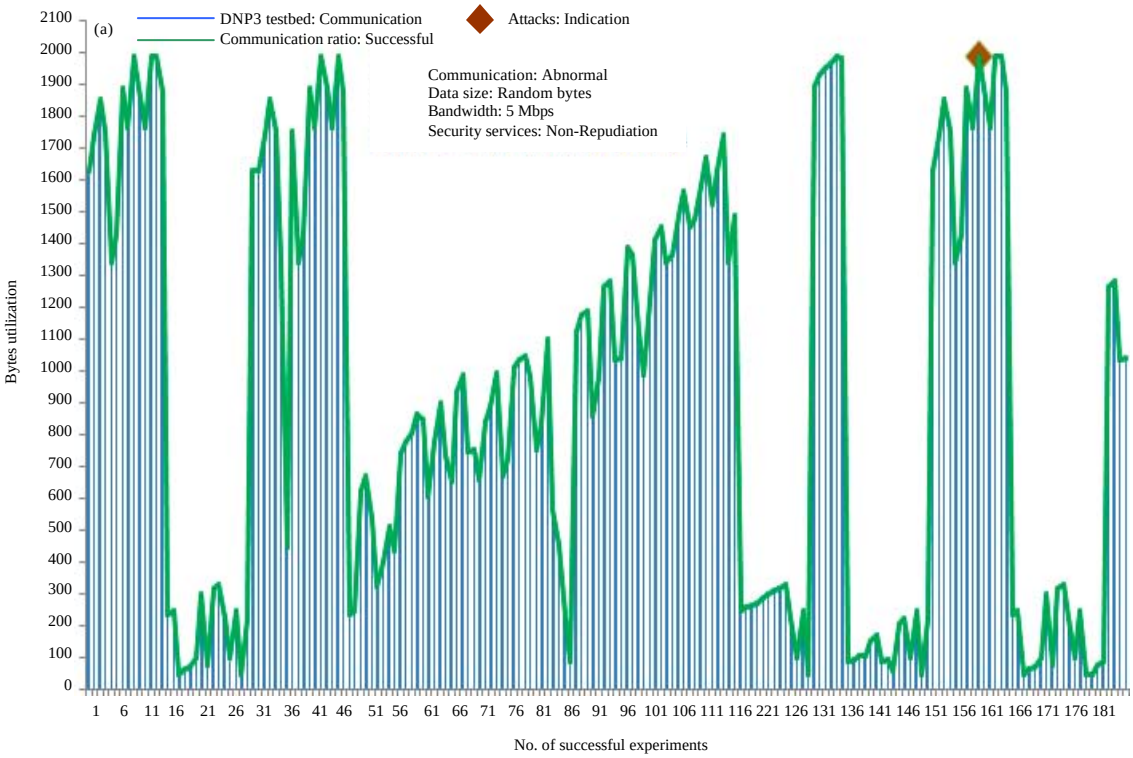

Fig. 10(a-b): Continue

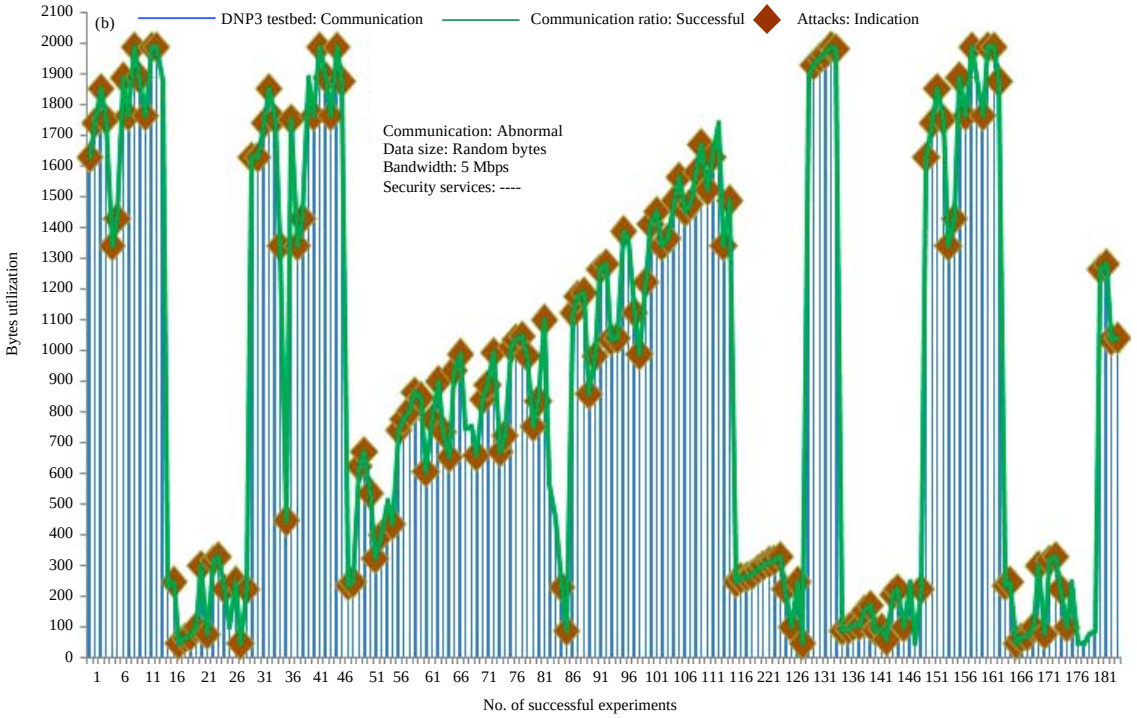

Fig. 10(a-b): Non-repudiation attacks: Performance results during communication (MTU/RTU)

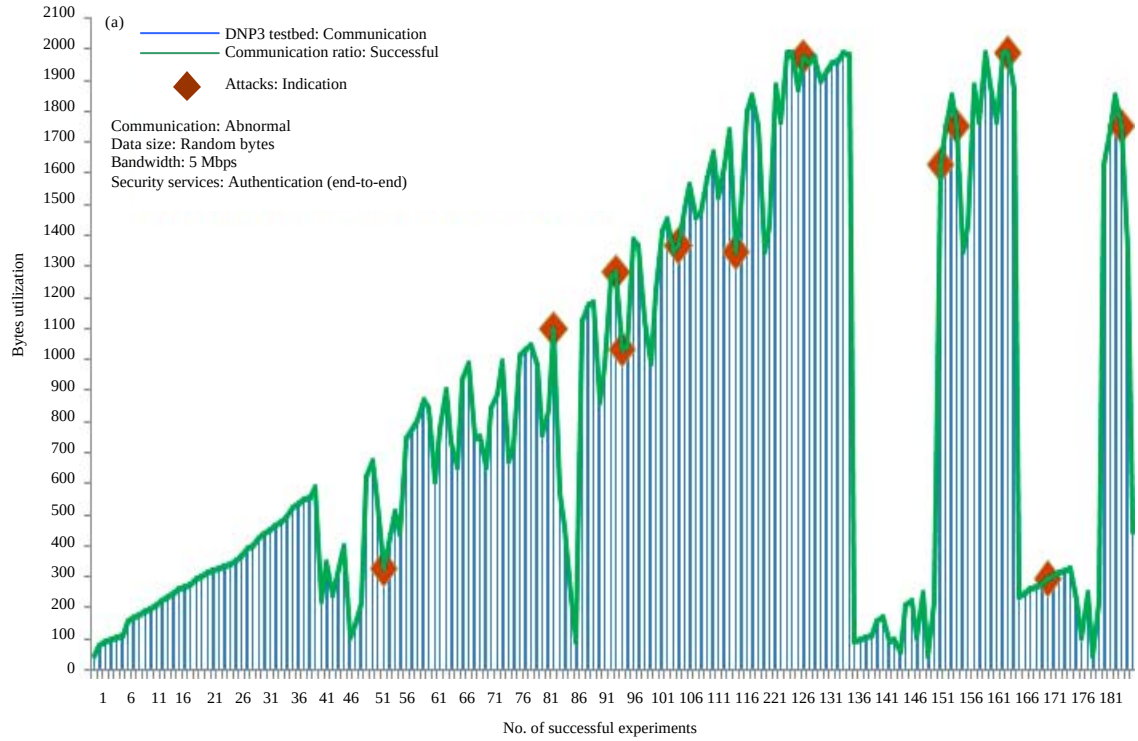

Fig. 11(a-b): Continue

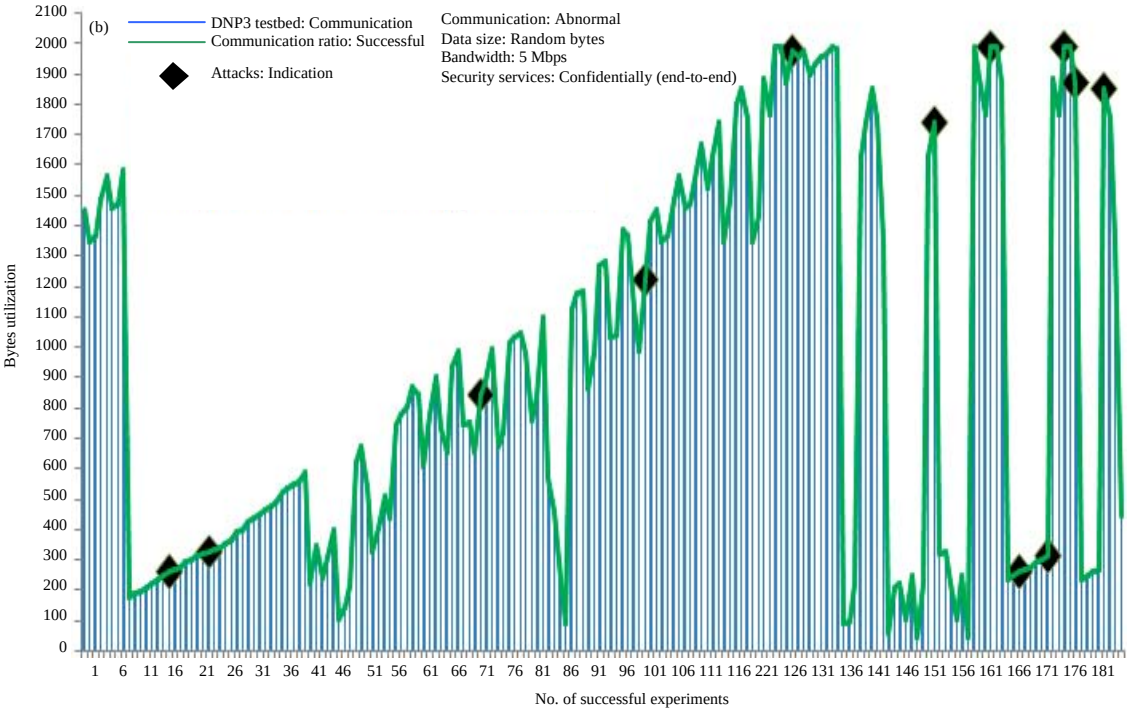

Fig. 11(a-b): End-to-end (a) Authentication and (b) Confidentiality attacks

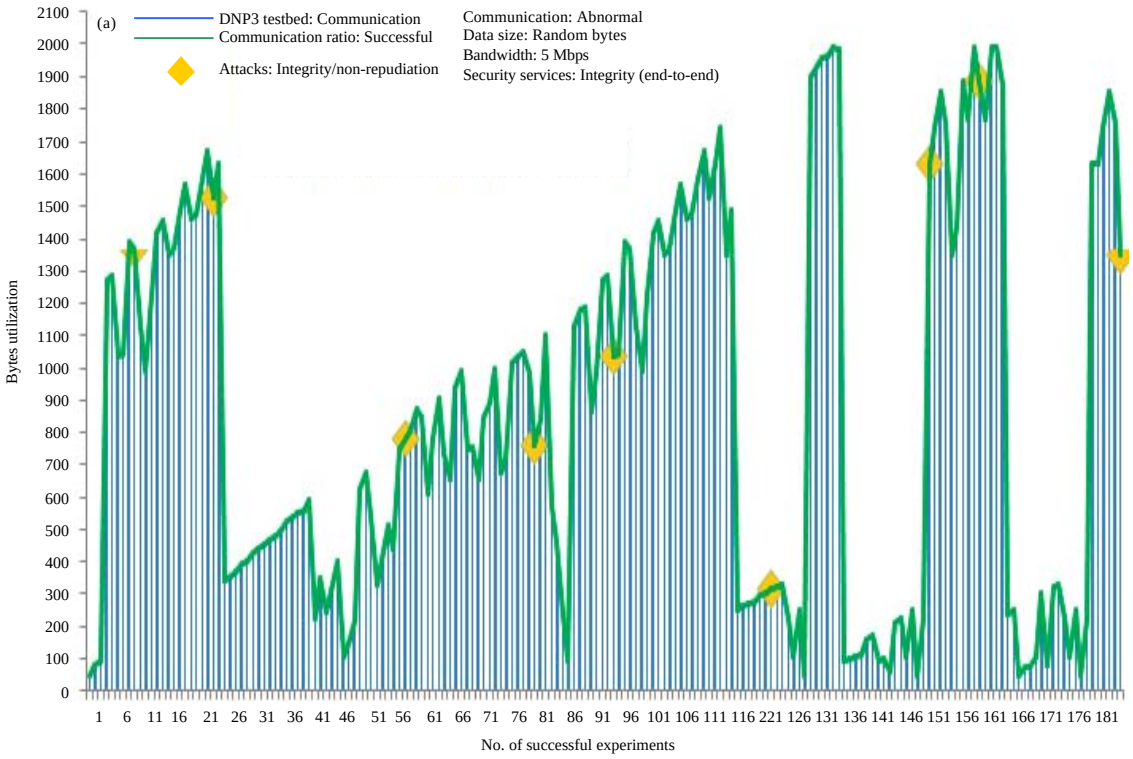

Fig. 12(a-b): Continue

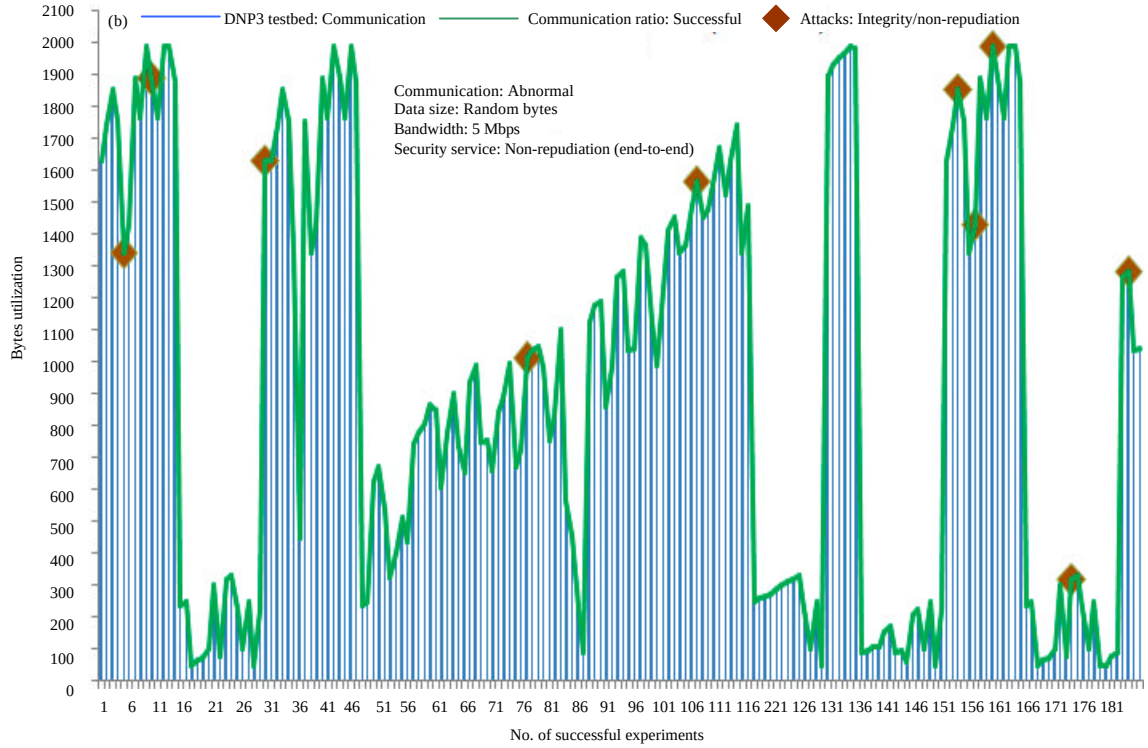

Fig. 12(a-b): End-to-end, (a) Integrity and (b) Non-Repudiation attacks

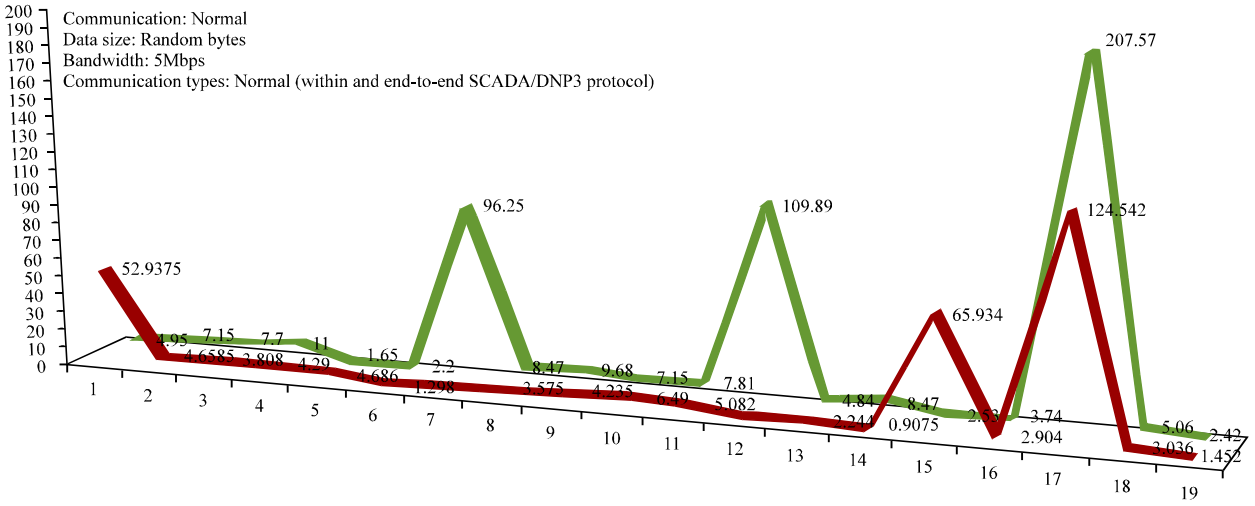

Fig. 13: Latency comparison

the implementation of Method[1].The Fig. 12a-b show the integrity and non-repudiation attacks (detection) with the implementation of Method[1]. "The red and black (color) markers in Fig. 11a-b, are representing the authentication and confidentiality attacks while orange and brown (color) markers in Fig. 12a-b are representing the integrity and non-repudiation attacks".

In performance Fig. 13, the latency has been measured by deploying proposed cryptography solution (Method[1]) within DNP3 protocol stack (first measurement) and each end of SCADA/DNP3

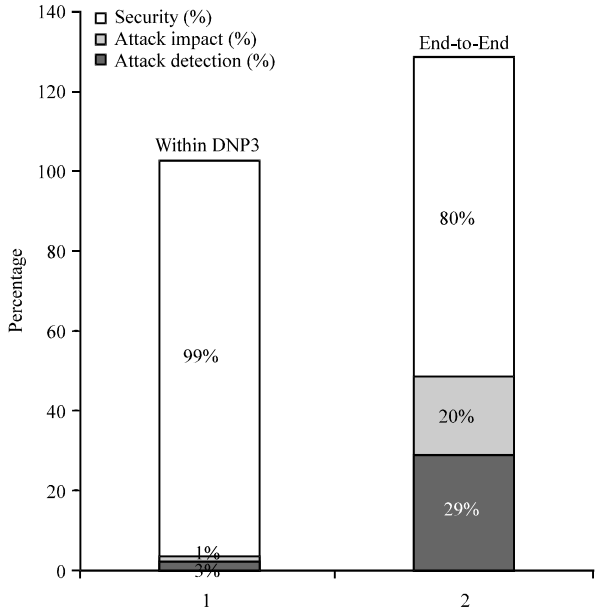

Fig. 14: Security measurement

tested (second measurement). "The green line shows the latency measured during bytes transmission, within DNP3 protocol stack while red line shows the latency during end-to-end communication which is comparatively low from first measurement (within DNP3 protocol stack)". The X-axis presents the numbers of experiment perform during normal communication and Y-axis presents the data rate (bytes) transmission between nodes, within tesbed. Figure 14, shows the level (%) of security included attack detection and impact.

CONCLUSION AND FUTURE WORK

In the initial structure of SCADA/DNP3 system, there is no security mechanism that provides protection against communication attacks. The existing work related with SCADA end-to-end security implementations has been analyzed and then cryptography based security solution has been implemented within DNP3 protocol as a part of SCADA system. In testbed; random bytes (data) have been transmitted securely between nodes (or SCADA nodes) and the performance results evaluate that the proposed implementation provides high security while comparing with end-to-end security solutions. This study gives alternative solution to secure SCADA/protocols communication.

Current study is based on DNP3 protocol security. The security mechanism (proposed Security solution) has been deployed within distributed network protocol (DNP3) and also each end of DNP3 as part of SCADA system. This is also need to implement (security mechanism) in other SCADA protocols such as Modbus, Fieldbus and Profibus, etc. These protocols were also designed without any security concerned. Using advance communication platforms; these protocols are "vulnerable from different types of attacks" which generate major issues or problems during communication.

REFERENCES

Cai, J., J. Wang and X. Yu, 2008. SCADA system security: Complexity, history and new developments. Proceedings of the 6th International Conference on Industrial Informatics, July 13-16, 2008, Daejeon, South Korea, pp: 569-574.

Ismail, M.N., A. Aborujilah, S. Musa and A. Shahzad, 2013. Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach. 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, 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.

Permann, M.R. and K. Rohde, 2005. Cyber assessment methods for SCADA security. Proceedings of the 15th Annual Conference on Joint ISA POWID/EPRI Controls and Instrumentation, June, 2005, La Jolla, California.

Robles, R.J. and T.H. Kim, 2011. Scheme to secure communication of SCADA master station and remote HMI's through smart phones. J. Secur. Eng., 8: 349-358.

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

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.