Random Network Coding for Secure Packet Transmission in SCADA Networks

Sajid Nazir
School of Computing, Engineering and Built Environment
Glasgow Caledonian University
Glasgow, UK, G4 0BA
sajid.nazir@gcu.ac.uk

Mohammad Kaleem
Department of Electrical Engineering
COMSATS University
Islamabad, Pakistan
mkaleem@comsats.edu.pk

***Abstract*—Industrial control systems were designed as closed systems without any consideration or need for Internet connectivity. This design choice resulted in most SCADA protocol implementations being plain text with little security against attackers. Information on SCADA systems and protocols is readily available in public domain, making them a target for malicious attacks. Network coding is a lightweight technique based on simple XOR operations for error correction that can also help secure the message. This paper proposes use of network coding for protection of message interchanges with the field devices in an industrial network. The results show that the proposed method effectively protects the communications against a malicious adversary.**

***Keywords*—** *security, industrial control systems, cyber-attack, SCADA, communication protocol*

I. INTRODUCTION

Industrial Control Systems (ICS) are used to control industrial processes, and are used for control and monitoring in many domains [1] [2]. Process control systems are used in manufacturing industries, similarly the building automation systems control the services in buildings, and energy management systems control the generation and distribution of power. Newer applications are in robotic systems and modern cars Engine Monitoring Systems (EMS). Supervisory Control and Data Acquisition (SCADA) are used to control and monitor an ICS over a large geographical area. SCADA system as shown in Figure 1 is a network of sensors, control devices, Human Machine Interface (HMI), actuators, databases and SCADA software. These systems manage critical infrastructures and any disruption in control and communications can have severe health, safety and financial implications.

The initial SCADA system design was a closed system with no outside communication links thus precluding the need for any inherent protection in the industrial protocols [3]. However the recent technological innovations with their associated benefits of remote connectivity and timely event notifications have resulted in the integration of Internet connectivity with SCADA system and devices. SCADA Internet connectivity [3][4] exposes a lot of different protocols and devices that are used to transfer information between the sensors, Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), and mobile devices.

Most of SCADA protocols had roots in early systems and were based on simplicity and obscurity of operation rather than security. SCADA technology and protocols are quite different from those of Personal Computer (PC) world [5].

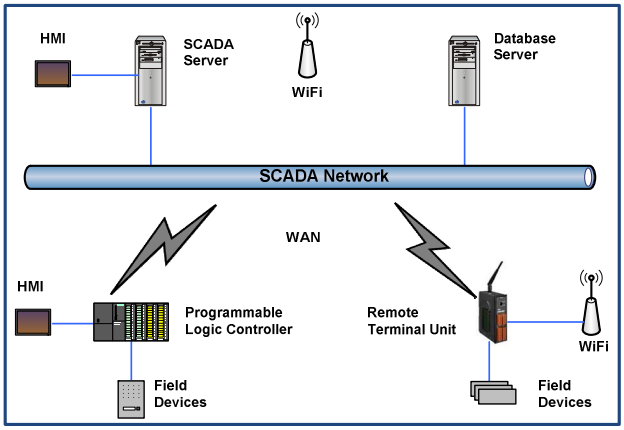

Fig. 1. *SCADA System.*

SCADA systems continuously collect measurements from the sensors and relay commands to the control and monitoring equipment [3]. SCADA systems have very tight timing constraints and any delay or disruption can be detrimental to its operation [6]. The near real-time operation of SCADA systems and limited processing capabilities of field devices make it difficult to have strong encryption of messages. This is similar to Secure Socket Layer/Transport Layer Security (SSL/TLS) encryption and decryption for secure Hyper Text Transport Protocol (HTTPS) that make it slower compared to HTTP protocol. Thus, strong cryptographic algorithms cannot be used for protection due to resource constraints [7].

An overview of sensor networking technologies for industrial applications is provided in [4]. Secure communications is an important requirement of the digital infrastructure and it is necessary to provide reliable communication despite presence of malicious users jeopardizing the normal flow of communications [8]. Modbus-RTU [9] was released in 1979 and is a communications protocol in widespread use in industrial applications [10]. Many security loopholes found in SCADA networks are in the communications protocols [7].

The attackers also know about the weaknesses and flaws in SCADA security [3]. Attacks on SCADA networks have increased and these systems have become attractive targets for malicious attackers [2]. It is critical to protect these systems due to the vulnerabilities and increased threats [2]. Thus it is important to provide security to the messages against eavesdroppers by using simple encryption schemes that provide requisite protection with an affordable level of processing available in low power devices.

Encryption encodes the messages such that it is unintelligible to an eavesdropper but authorized users can read it correctly [5]. Network coding was proposed by [12] and it allows robustness in data communications [13]. Instead of sending the source packets, linear combinations of packets are transmitted. The linear combinations are based on Exclusive-OR (XOR) operator, which is a simple operation to implement in hardware or software.

This paper proposes the use of network coding for securing the message transfers in SCADA networks and demonstrates the applicability through protecting Modbus protocol against man-in-the-middle (MITM) attack.

Rest of the paper is organized as follows: Section II describes related work. Section III covers the background information. Proposed protection methodology is described in Section IV. The results and discussion are provided in Section V and conclusion is in Section VI.

II. Related Work

A survey of protocols and challenges of Wireless Sensor Networks (WSNs) is provided in [14]. A review of SCADA components, communications protocols and security trends is provided in [15]. A summary of defensive measures against wireless industrial communications system using cryptographic techniques is described in [6]. Some SCADA protocols with increased security protection were realized for point-to-point, broadcast, and emergency channels [3].

Modbus protocol can be compromised to execute arbitrary requests [7]. An implementation of error detection and correction for Modbus-RTU serial protocol is described in [10]. This study overcomes the limitations of SCADA protocols by ensuring the integrity of the messages by using forward error correction.

Implementation of a secure framework for secure SCADA networks is proposed using moving target defence strategy [16]. The Internet Protocol (IP) address of each host is changed randomly so that the attacker cannot find it. The solution does not incur packet loss as compared to other solutions and zero packet loss was demonstrated during hand-off [16]. The IP based SCADA protocols considered were Modbus/TCP, Distributed Network protocol version 3 (DNP3), Profinet and Ethernet/IP [16].

A secure authentication for Distributed Network protocol version 3 (DNP3) is proposed for broadcast transmissions between master and multiple stations in [7]. The proposed scheme is validated against common attacks such as modification, injection and replay [7].

A discussion on security issues and sSCADA protocol suite was proposed to overcome some of the limitations of SCADA protocols in point-to-point, broadcast and emergency channels [3].

IEC 60870-5-101 communications protocol is used in SCADA systems for communications between a master device and remote devices in electric power industry. The protocol architecture does not protect the sensitive exchange of data between the master and slave devices [2]. An implementation of security for protocol is described by incorporating a secrecy layer between the physical and link layers of the protocol [2]. Variable length frames use encryption to hide the message. Three XOR and three transposition blocks were used in the cipher sublayer [2]. A simulation testbed was used to confirm that the proposed enhancement meets the temporal deadlines of electric substations [2].

A rateless application for evaluating the efficiency of network coding for secure transmissions is proposed in [13]. It was shown that the efficiency parameters need to be matched to the communications requirements to outperform routing.

Use of network coding for protection of unicast bidirectional connections in optical networks is proposed in [17]. The use of preconfigured cycles is explained for generating the linear combinations of data units. It provides the advantage as explicit detection of failures and rerouting is not required [17].

A model for secure network coding and necessary conditions for its being secure are described in [8]. A method was proposed using precoding to transform an insecure network code to a secure code [8].

III. Background

In this section we provide relevant background on Modbus protocol, a common attack scenario being considered and basics of XOR and network coding techniques.

A. Modbus Protocol

The protocol was developed by Modicon Incorporated in 1979. It is a master-slave protocol in which all the communication is initiated by the master device. The slave devices only respond to a master query and do not initiate communication [9]. A summary of commands is provided in Table I.

Some of the common industrial protocols are described in [18]. In industrial applications, Modbus is the most commonly used protocol [18]. It transmits 16 bit integer data between the devices on the same network [18]. It is a well-known serial protocol used with PLC for controlling a large variety of applications such as, bar code readers, position sensors, vision sensors, speed controls, etc. [19]. Modbus protocol uses Cyclic Redundancy Check (CRC) for integrity check and error detection.

TABLE I. Modbus Commands

Code	Function	Reference
01 (01H)	Read Coil (Output) Status	0xxxx
03 (03H)	Read Holding Registers	4xxxx
04 (04H)	Read Input Registers	3xxxx
05 (05H)	Force Single Coil (Output)	0xxxx
06 (06H)	Preset Single Register	4xxxx
15 (0FH)	Force Multiple Coils (Outputs)	0xxxx
16 (10H)	Preset Multiple Registers	4xxxx
17 (11H)	Report Slave ID	Hidden

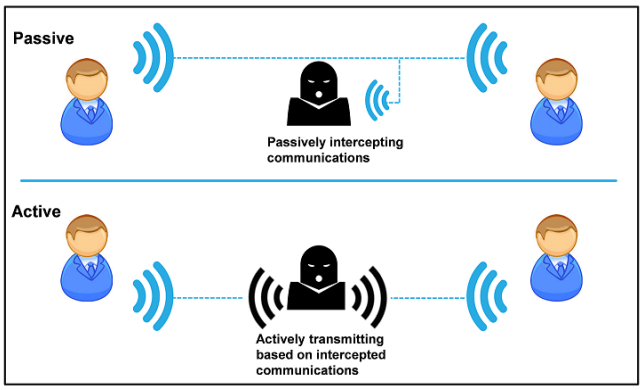

Fig. 2. *MITM attack.*

B. Attack Scenarios

In SCADA systems it is important that the source and destination of each method is identified [2] as otherwise potentially damaging commands could be issued causing damage or disruption to the physical system being controlled.

MITM attack scenarios are shown in Figure 2. Passive attacks are aimed at intercepting the messages and interpreting them to acquire more information about the system under attack. Such attacks can continue over a longer period of time and can be difficult to detect. In an active attack the eavesdropper not only intercepts the message but also tries to discard, modify or delay the message with a view to compromise the system.

C. XOR and Network Coding

The XOR operation is similar to logical OR except that the result with both input bits as 1, will be 0. XOR operation can be efficiently implemented in hardware and software.

Network coding combines the packets in a linear combination and the simplest combination operator used is XOR. The receiving node by applying the XOR operation again is able to extract the original message [20].

Network coding is simple to implement and as a packet level error correction solution, performs as near-optimal erasure codes for sufficiently large finite field used for creating linear combinations of source symbols [21]. The complexity is acceptable for short lengths of the source messages [21].

The XOR is a lightweight operation that can easily be performed on a low power device. It is used in conjunction with other transformations in many encryption algorithms, such as Wired Equivalent Privacy (WEP) [6] and Advanced Encryption Standard (AES) protocols. XOR is also used for transforming message payload of each message sent from browsers to WebSocket servers [22].

Simple XOR operation can be used to create very robust encryption by applying a technique known as one-time pad, in which the source message is XOR with a random key of same length as the source message. This would require generating a new completely random key for the next message to be encrypted to prevent the eavesdropper from guessing the key. The full-length keys could also be based on a shorter key that generates a truly random longer bit sequence. The idea is similar to network coding wherein a seed or key value is used to generate the sequence of linear combinations.

The application of XOR operation can be understood through a small example:

Source message	: 0 1 1 0	1 0 1 0
XOR Key	: 1 0 1 0	1 0 1 0 (XOR)
Cipher text	: 1 1 0 0	0 0 0 0

The same key can be applied again to the encrypted text for retrieving the original source symbol:

Cipher text	: 1 1 0 0	0 0 0 0
XOR Key	: 1 0 1 0	1 0 1 0 (XOR)
Original message	: 0 1 1 0	1 0 1 0

IV. Methodology

A. Attack Scenario

We consider an attack scenario where an eavesdropper is able to intercept the Modbus protocol messages between the master and slave devices in the SCADA network. The attacker could thereby inject a valid message of its own in order to change the system state to jeopardise the system operation.

B. Proposed Encryption Technique

Network coding is based on XOR operation which can be efficiently implemented in hardware and the operation executes at much higher speed and low-cost compared to other encryption algorithms that might be considered.

We propose use of a secret key or seed for network coding to generate the linear combinations. This short key can be used to generate a truly random bit sequence equal in length to the message to be encrypted. The security of this key is important to preserve the security of XOR coded messages.

The robust security provided by the above scheme can fully secure the message against any eavesdropper provided that (i) the short key remains a secret; (ii) the random bit sequence generated using the short key is truly random (iii) the key is not re-used.

An interesting feature of the XOR coding is that applying the XOR sequence used for encoding to the encrypted sequence will yield the original plain text message. Thus, the intended recipients in the SCADA network can recover the actual message quite easily.

Normally the key used for the random network coding is sent along with the message for ease. We instead propose key sequences to be either available at both the sender and receiver or these could be dynamically sent by the master device over another secure communications channel.

V. Results and Discussion

We consider the problem of protecting the SCADA Modbus protocol traffic. As described above, we illustrate the efficacy of XOR operation through a simplified operation; however, it is straightforward to extend it to the full length of source message to be protected.

A. *Passive Attack on Modbus Communications*

In a passive attack, the eavesdropper can access the ongoing communication but does not change it. This might be to gain more information about the SCADA network to launch a more serious and involved attack.

Modbus messages could be of different lengths based on the number of slave devices and the particular function type. For illustration, consider a source message of length 32 bits as,

01101011 00101010 10111100 10101010

Using a 32 bit secret key,

11010001 11001100 01111000 01011011, the encrypted message would be,

10111010 11100010 11000100 11110001

It can be seen that if the key is not known to the eavesdropper then it is highly unlikely to decipher the message. The seed of length 32 for a random number generator has 2^{32} possible values giving 4 billion combinations. Although this can be broken in finite time by trying all possible combinations but that would require that eavesdropper has requisite processing power and more information about the network. Also, as the next Modbus command would use a different key, the eavesdropper cannot infer the plain text message conveniently, and at best can infer information about the Modbus network devices.

B. *Active Attack on Modbus Communications*

In an active attack the eavesdropper can not only access the ongoing communication but also proceeds to duplicate, distort, or replace it.

As illustrated in the Section above, once the eavesdropper is able to decipher and understand the ongoing Modbus commands and responses flowing in the network, it will be too late to make any use of this information as next time around a new key will be used. Thus, it is no longer possible to modify these in any meaningful way without it being detected.

The only possibility remaining for the attacker is to replay an intercepted encrypted message. However, as described, this would also be caught as an invalid message due to the updated key and will not be decoded to a valid command and hence ignored.

VI. CONCLUSION

The protection of message interchanges between SCADA system and its devices has assumed more importance with the SCADA interconnectivity with Internet of Things devices and the Internet. The low power devices are not capable of strong cryptographic algorithms and such techniques which might also violate the timing constraints of SCADA system. This paper has proposed a simple technique for message protection based on network coding and key management that can effectively counter and limit the actions of an eavesdropper.

In our future work we will extend this work to other SCADA protocols and communications scenarios to illustrate a wide applicability of the proposed scheme.

REFERENCES

[1] S. Nazir, S. Patel, and D. Patel, "Assessing and Augmenting SCADA Cyber Security-A Survey of Techniques," *Computers & Security*, 70, July 2017

[2] T. Cherifi, L. Hamami, "A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol," *International Journal of Critical Infrastructure Protection,* 20 (2018) 68–84.

[3] Y. Wang, "sSCADA: securing SCADA infrastructure communications," *Int. J. Communication Networks and Distributed Systems*, vol. 6, no. 1, 2011.

[4] A. Flammini, P. Ferrari, D. Marioli, E. Sisinni, A.Taroni, "Wiredandwirelesssensornetworksforindustrialapplications," MicroelectronicsJournal40(2009)1322–1336.

[5] K. Finnan, P. Willems, "Benefits of Network Level Security at RTU Level," *Pipeline & Gas Journal*, Feb 2014;241,2.

[6] T. Ondrasina, M. Franekova, "Attacks to Cryptography Protocols of Wireless Industrial Communication Systems," *Information and Communication Technologies and Services,* vol. 8, no. 3, 2010.

[7] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, August 2016.

[8] N. Cai and T. Chan, "Theory of Secure Network Coding," in Proceedings of the IEEE, vol. 99, no. 3, pp. 421-437, March 2011. doi: 10.1109/JPROC.2010.2094592.

[9] modbus-tcp: http://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

[10] C. Urrean, C. Morales, and J. Kern, "Implementation of error detection and correction in the Modbus-RTU serial protocol," *International Journal of Critical Infrastructure Protection*, 15(2016), pp. 27–37.

[11] D. McMillan, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent," 2016. https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

[12] Ahlswede, Rudolf; N. Cai; S.-Y. R. Li; R. W. Yeung (2000). "Network Information Flow," *IEEE Transactions on Information Theory*, 46 (4): 1204–1216. doi:10.1109/18.850663.

[13] E. Franz, S. Pfennig, T. Reiher, "Efficiency of rateless secure network coding," *Procedia Technology*, 17, 2014, pp. 162-169.

[14] A. A. Kumar S., K. Øvsthus, and L. M. Kristensen, "An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges," *IEEE Communications Survey and Tutorials*, vol. 16, no. 3, third quarter, 2014.

[15] A. Shahzad, A. S. Musa, Aborujilah and M. Irfan, "The SCADA Review: System Componenets, Architecture, Protocols and Future Security Trends," *American Journal of Applied Sciences* 11 (8): 1418-1425, 2014.

[16] V. Heydari, "Moving Target Defense for Securing SCADA Communications," *IEEE Access*, vol. 6, 2018.

[17] A. E. Kamal, M. Mohandespour, "Networkcoding-basedprotection," *Optical Switching and Networking*, 11(2014), pp.189–20.

[18] C. Wilson, "Common Industrial Communications Protocols," *Process Control*, 2013.

[19] D. Jones, "Industrial network communications products contribute to lower cost operating systems," *Control Engineering*; Barrington, 2015.

[20] B. Li, and Y. Wu, "Network Coding," vol. 99, 2011 IEEE no. 3, March 2011.

[21] S. Nazir, D. Vukobratović and V. Stanković, "Performance evaluation of Raptor and Random Linear Codes for H.264/AVC video transmission over DVB-H networks," *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague, 2011, pp. 2328-2331. doi: 10.1109/ICASSP.2011.5946949.

[22] V. Wang, F. Salim, and P. Moskovits, "The definitive guide to HTML5 WebSocket," Apress, 2013.