A Survey of Security in SCADA networks:Current Issues and Future Challenges

Sagarika Ghosh, Student Member, IEEE ,
sagarika.dal.ca

Srinivas Sampalli, Member, IEEE, Srini@
cs.dal.ca

***Abstract*—**Supervisory Control and Data Acquisition (SCADA) systems are used for monitoring industrial devices. However, their security faces the threat of being compromised due to the increasing use of open access networks. To secure the communication between nodes of SCADA networks, various security standards have been developed by different organizations. Researchers have proposed various security schemes to overcome the weaknesses of SCADA standards. The primary objective of this survey paper is to provide a study of the impact of possible attacks on SCADA systems. The paper addresses the future challenges that SCADA networks may face from quantum attacks. Furthermore, it outlines directions for further research in the field

***Keywords*—**Asymmetric cryptography, binary tree, intrusion detection system, key managementprotocol, n-ary tree, quantum, qubit, symmetric cryptography, SCADA networks.

I. Introduction

SCADA systems are used as control systems for monitoringindustrial, infrastructural, and facility processes such as oil mining, electric grids, traffic system control, water treatmentsystems, and space station systems. Modern SCADA systemshave been exposed to a range of attacks since they use openaccess networks to leverage efficiency. Failure to secure SCADA systems can be catastrophic [1]. For example, a malicious user can take control of the power supply to a city,shut down the water supply system, or cause malfunction ofa nuclear reactor.

Modern SCADA systems have a number of added features which increase the system complexities and are thus difficult to maintain. Some of the added features include control logic,communication protocols, user interfaces, and security. For example, many organizations do not tolerate data delay or dataloss. Added features like firewall function and anti-virus software processes can lead to delayed delivery of data [2]. The systems must operate continuously and in tight timing [3].Moreover, the communications are vulnerable to various threats. In the past few years, the number of cyber-attacks, ingeneral, is rising and has been affecting the power station, water, gas, and plants control systems. The pattern of cyber attacks has also evolved beyond the simple attacks such as Denial of Service or Man-in-the-Middle [3].

The paper has two major contributions as follows.

- It provides a study of the impact of possible attacks on SCADA systems.
- The paper addresses the future challenges that SCADA networks may face from quantum attack.

II. Traditional Attacks on scada networks

In December 2015, due to a successful cyber-attack on SCADA, 230,000 people were left without power for hours in Ukraine. After a year, another similar attack hit the country. This attack was launched by using spear phishing emails and is still in practice against industrial organizations.According to the U.S. Department of Justice, there was an attack on a small dam in Rye Brook, New York in 2013. Thehackers gained access to the core command-and-controlsystem by using a cellular modem. Although the breach occurred in 2013, it remained unreported until 2016. Furthermore, according to FBI and Homeland Security last year's joint report [4], there have been cyber-attacks on nuclear power plants throughout the U.S. The main motive and severity of the attacks are not known, but the method used for the attack was spear phishing. The hackers targetedthe control systems of the plant.

SCADA networks also comprise of resource-constrained devices such as Remote Terminal Units or Programming Logic Units which requires lightweight ciphers. Traditional intrusion detection systems (IDSs) such as firewalls are nowunable to protect from the new threats [5]. Robust security schemes involving machine learning to detect intrusions andencryption algorithms are essential to ensure a secure encrypted communication between nodes in SCADA networks. These threats and attacks have motivated researchers and organizations to develop different robust andimmune system for SCADA networks.

Although there are several survey papers on the security threats, key management schemes, and intrusion detection systems in SCADA networks [6][7][8], the reviews do not specify a contrast of the various schemes. Furthermore, Sajid et al.[9] have provided an excellent survey on the security and challenges of the SCADA systems. However, the papers do not address the future challenges of the SCADA networks.

III. Possible attack using quantum computing

A. Quantum Computer

Traditional computers are the digital electronic computers which encode information in bits. Each bit can be 0 or 1. They execute algorithms on bits using simple digital logic operations such as AND, XOR, OR, and NOT [11].

Instead, quantum computers encode information in qubits which are generated using atoms as digital bits [12]. The valueof qubits is based on the rules of modern physics: superposition and entanglement principle. According to the superposition principle, each qubit can represent 0 or 1 or both at the same time. Entanglement occurs when two superposed qubits are allied with each other [13][12]. Therefore, the

number of qubits is directly proportional to the number of states held by the set of qubits [12][14]. These two principles make quantum computing way faster than traditional computing.

A quantum algorithm was proposed to solve a binary maze problem[15]. Each line has one input and two outputs. The quantum algorithm attempted all the paths at the same time,and therefore, it solved the problem at extreme speed. Whereas, solving the maze problem was hard for a traditional computer since the size of the problem was doubling each time. For example, a 1000 step binary maze may have 2^{1000} outcomes, and this took more time in the case of traditional approach [15].

D-wave, a quantum computing company, launched its first commercial quantum computer named D-Wave One in 2011, which is being used by National Aeronautics and Space Administration (NASA) of the U.S. for in-depth space exploration. By 2013, they increased the number of qubits and published the D-Wave Two system. Google is alsoplanning to use a quantum computer for big data mining [13].

B. Brute Force Attack by using a Quantum Computer

The capacity and speed of quantum computer solving mathematical problems make them a threat to traditional security scheme. All the encryption schemes are derived from mathematical logic. Cracking these schemes may be possible for quantum computers [16][17]. One such problem is Elliptic curve cryptography (ECC or ECDSA). Using Shor's algorithm, a quantum computer can launch a brute force attack and crack ECC in a brief time [17].

Shor's algorithm is a quantum algorithm for factorizing a number [18]. It implies that any public key cryptography can be easily cracked. The algorithm has two sections as follows [19].

- The classical computer can compute section 1. It reduces the factoring problem to Order Finding Problem using the Euclidean algorithm. The Euclidean algorithm is a fast scheme to calculate the greatest common divisor (gcd) of two integers [20].
- Section 2 is the quantum part which used Order Findingalgorithm. It finds the period of the function using the Quantum Fourier Transform (QFT). The Table 1 shows the steps in each section [19].

Table 1: Steps in Shor's Algorithm

Section 1: CLASSICAL PART	
Step 1:	Select a random positive integer m such that m<n. Then, calculate gcd(m,b) using the Euclidean algorithm. If gcd is not equal to 1, a non-trivial factor is obtained. Thus, the algorithm ends. Otherwise, go to Step 2.
Section 2: QUANTUM PART	
Step 2:	Calculate the period P of the sequence: x mod n, x^2 mod n, x^3 mod n, …
Step 3:	If p is odd, return to step 1. If p is even, go to step 4.
Step 4:	$\left(m^{p/2}-1\right)^2 = m^p - 1 = 0 \bmod n$, since p is even. If $m^{p/2}+1 = 0 \bmod n$, then return to step 1. Else, go to step 5.
Step 5	Calculate $result = gcd\left(m^{p/2}-1,\ n\right)$ using the Euclidean algorithm.

In step 2, to calculate the period of the function based on theseries, Quantum Fourier Transform (QFT) is used. Using QFT, it increases the speed of the algorithm by evaluating the function at all points simultaneously [19]. The QFT is a linear operator when applied to any state of qubit transforms it into another state. In other words, it is applied to the vector of amplitudes of a quantum state[21]. For example, if QFT operates on a quantum state X, then it transforms it into a quantum state Y.

X: $|x> = \sum_{i=0}^{\cdot\cdot} x_i |i>$

Y: $|y> = \sum_{i=0}^{N-1} y_i |i>$

The QFT refers to (1).

$$y_{k} = 1/\sqrt{N} \sum_{j=0}^{N-1} x_j \omega_n^{jk} \ , \ k = 0, 1, 2, 3, \ldots\ldots, N-1 \qquad (1)$$

Where, $\omega_n = e^{\frac{2\pi i}{N}}$ and is a primitive N^{th} root of unity, N is thelength of vectors such that $N := 2^n$[21].

IV. CONCLUSION

The existing security standards and schemes are based on traditional cryptography: Advanced Encryption System (AES), Elliptic-curve cryptography (ECC), and traditional hashing algorithm: Secure Hash Algorithm (SHA). So, they are vulnerable to quantum computer attacks. The transformation of quantum computing from theory to practice in the recent past has not only brought with its potential advantages but also increasing threats. The current cryptography schemes may remain at stake unless they are modified[16][17].

As a future direction, the article provides Table 2 that will provide a course for further research and assist an organization to decide on a suitable standard and scheme.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support in part by the Natural Sciences and Engineering Research Council (NSERC) and industry partners Cistel Technology Inc. and Technologie Sanstream, through a Collaborative Research

Table 2: Comparative analysis of prevention schemes of SCADA attacks.

Prevent SCADA attacks	Cost	Confidentiality	Integrity	Non-repudiation	Availability	Authenticate	Broadcast Interaction	Self-Heal	Prone to QC attack
SKE	High	Yes	No	No	No	No	No	No	Yes
SKMA	Low	Yes	No	No	No	No	No	No	Yes
LKH	High	Yes	No	No	No	No	Yes	No	Yes
ASKMA	Low	Yes	No	No	No	No	Yes	No	Yes
HKMA	Low	Yes	No	No	Yes	No	Yes	No	Yes
AHSKMA	Low	Yes	No	No	Yes	No	Yes	No	Yes
LiSH+	Low	Yes	No	No	Yes	No	Yes	Yes	Yes
ID-based KMP	Low	Yes	No	Yes	No	Yes	Yes	No	Yes
NTRU	Low	Yes	Yes	Yes	No	Yes	Yes	No	No

Grant. The authors also thank the anonymous reviewers for their valuable feedback and comments, which have substantially improved the quality of the paper.

REFERENCES

[1] D. J. Kang, J. J. Lee, S. J. Kim, and J. H. Park, "Analysis on cyber threats to SCADA systems," *Transm. Distrib. Conf. Expo. Asia Pacific, T D Asia2009*, pp. 1–4, 2009.

[2] Trihedral, "Managing SCADA Complexity- Minimizing Risk Balancing System GrowthAgainst Destabilizing Uncertainty," 2016.

[3] S. Nazir *et al.*, "Autonomic Computing MeetsSCADA Security," pp. 498–502.

[4] US CERT, "Russian Government Cyber Activity Targeting Energy and Other Critical InfrastructureSectors," *Us Cert*, vol. TA18–074A, pp. 1–19, 2018.

[5] P. Nader, P. Honeine, and P. Beauseroy, "Lp-norms in one-class classification for intrusion detection in SCADA systems," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2308–2317, 2014.

[6] A. Rezai, P. Keshavarzi, and Z. Moravej, "Key management issue in SCADA networks: A review,"*Eng. Sci. Technol. an Int. J.*, vol. 20, no. 1, pp. 354–363, 2017.

[7] R. J. Robles, M. Balitanas, R. Caytiles, Y. Gelogo, and T. H. Kim, "Comparison of encryption schemesas used in communication between SCADA components," *Proc. - 2011 Int. Conf. Ubiquitous Comput. Multimed. Appl. UCMA 2011*, pp. 115– 118, 2012.

[8] R. Lopez Perez, F. Adamsky, R. Soua, and T. Engel, "Machine Learning for Reliable Network Attack Detection in SCADA Systems," *Proc. - 17thIEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 633–638, 2018.

[9] A. Sajid, H. Abbas, and K. Saleem, "Cloud- Assisted IoT-Based SCADA Systems Security : AReview of the State of the Art and Future Challenges," *IEEE Access*, vol. 3536, no. c, 2016.

[10] M. Endi, Y. Z. Elhalwagy, and A. Hashad, "Three-layer PLC/SCADA system architecture in process automation and data monitoring," *2010 2nd Int. Conf. Comput. Autom. Eng. ICCAE 2010*, vol. 2, pp. 774–779, 2010.

[11] L. Chang, "How secure is today's encryption against quantum computers?," *Betanews*, 2017. [Online]. Available: https://betanews.com/2017/10/13/current- encryption-vs-quantum-computers/. [Accessed: 21-Oct-2018].

[12] Pedram Khalili Amiri, "Quantum Computers," *IEEE Potentials*, vol. 21, no. 5, pp. 6–9, 2002.

[13] X. Zhang, Z. Y. Dong, Z. Wan, C. Xiao, and F. Luo, "Quantum cryptography based cyber-physical security technology for smart grids," *IEEE Xplore*,2017.

[14] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantumcryptography for IoT: APerspective," *IEEE Int. Conf. IoT its Appl. ICIOT 2017*, 2017.

[15] N. Kumar and D. Goswami, "Quantum Algorithm to Solve a Maze: Converting the Maze Problem intoa Search Problem," Kanpur, India, 2013.

[16] S. Castellanos, "Nascent Quantum Computing Poses Threat to Cybersecurity - CIO Journal. - WSJ," *Sep 13, 2017*. [Online]. Available: https://blogs.wsj.com/cio/2017/09/13/nascent- quantum-computing-poses-threat-to-cybersecurity/. [Accessed: 21-Oct-2018].

[17] R. Dennis, "Quantum Computers Are the Most Powerful Tech Threat to Cryptocurrency.," *ICO ALERT*. [Online]. Available: https://blog.icoalert.com/quantum-computers-are- the-most-powerful-tech-threat-cryptocurrency-will- face-9b271e76edda. [Accessed: 21-Oct-2018].

[18] Quantiki, "Shor's Factoring Algorithm," *Quantiki*, 2015. [Online]. Available: https://www.quantiki.org/wiki/shors-factoring- algorithm. [Accessed: 05-Nov-2018].

[19] J Stephanie Blanda, “Shor’s Algorithm – Breaking RSA Encryption _ AMS Grad Blog”, American Mathematical Society, 2014.

[20] I. S. Ben Lynn, “Number Theory - Euclid’s Algorithm,” Standford University. [Online]. Available: https://crypto.stanford.edu/pbc/notes/numbertheory/ euclid.html. [Accessed: 05-Nov-2018].

[21] F. X. Lin, “Shor ’ s Algorithm and the QuantumFourier Transform,” pp. 1–16.