17th International Computing & Control for the Water Industry Conference
1-4 September 2019, Exeter, United Kingdom

Cyber-Physical System Security Open Challenges in Smart Water Networks

Haitham Hassan M. Mahmoud and Wenyan Wu
School of Engineering and Built environment, Birmingham City University
[1]*Haitham.mahmoud@bcu.ac.uk*

Keywords: Cyber-Physical System; Cyber-Physical System Security; Water 4.0; Smart Water Networks.

EXTENDED ABSTRACT

Introduction

Cyber Physical Systems (CPSs) are at the core of Water 4.0. As water networks are upgraded to Smart Water Networks (SWNs), however, the number of potential entry points for malicious attackers grows. Therefore, there is a pressing need for mitigating the related risks using cyber and physical security frameworks. This pressing need is evidenced by the fact that Cyber-Physical System Security (CPSS) has attracted a lot of research attention in recent years. Examples of reported CPSs attacks are the ransomware attack in the city of Atlanta in March 2018 and the Ukraine attack in December 2015. Bearing this in mind, there are many other attacks that are expected to occur in SWNs such as compromising remote sites, hot pivots, cell-phone WIFI, Stuxnet, etc. [1]. A recent study [2] reported that, every sixty seconds, the cyber-crime costs more than $1.1 million and impacts more than 1,800 people along with affecting infrastructures and the services.

SWNs are complex systems consisting of a physical layer of reservoirs, valves, pumps and pipes, among the others. According to the SWAN forum, the other SWN layers are: 1) sensing and control, 2) collection and communication, 3) data management and display and 4) data fusion and analysis. This paper reviews the potential attacks and prevention approaches with focus on each layer of the SWN architecture. The attacks and possible countermeasures are explained and references to relevant literature that has attempted to deal with these issues are provided. Moreover, the impact of these attacks on SWNs is discussed and recommendations for security procedures to be followed by water utilities are proposed.

Cyber-Physical System Security Threats and Countermeasures for Smart Water Networks

Different CPS threats and potential countermeasures are discussed in this section with focus on each layer of the SWN architecture (see Figure1) to provide guidance for water utilities when upgrading the current water infrastructure.

In the physical and sensing and control layers, many attacks can occur that are directed to the physical devices (i.e., smart meters, water quality sensors, hydraulic sensors, PLC, etc.) and/or to the process of collecting the data from such devices. These attacks include, device tampering, fake (virtual) node injection, malicious code injection, sleep denial attacks and node jamming. Device tampering may occur when an attacker is physically close to the device and can replace part of the hardware to manipulate the data or to get the information inside the device (e.g., data, cryptographic key, communications channels, etc.). This threat can be mitigated by implementing secure and reliable physical design with alarming systems that can notify a water utility in the case of any tampering attempt [3]. Fake node injection may occur when an attacker succeeds in injecting a virtual node in the network which, in turn, enables the attacker to gain access to the network and control the flow of data. This threat can be mitigated by implementing a secure booting scheme which involves a lightweight physical layer authentication such as unclonable function [3] and weighted hash function cryptographic algorithms [4]. Malicious code injection may occur when the attacker can gain access to the network by attacking one of the nodes by Denial of Service (DoS) attacks of a virus which can expose the network resources. This threat cannot be easily mitigated as some of the nodes may not have the power and computational capabilities to stand against such attacks. However, putting the nodes in sleep mode in case of these attacks and intrusion detection technologies have been proposed for this threat. Sleep denial attacks may occur when the attacker manages to prevent the nodes from going sleep when not in service, which may result in shutting the nodes down. This threat can be mitigated by maintaining authentication and trust between devices in the node. Finally, node jamming may occur when the sensor get DoS following transmission of noise signals. This threat can be mitigated by implementing a Internet Protocol security (IPsec) channel which is a network protocol that can provide authentication and encryption of the transmitted data along with identifying the sender [5].

In the collection and communication (i.e. network) layer, there are several attacks that do not require the attacker to be physically at the location where the attack will take place. These attacks include: traffic analysis attack, sinkhole attack and Man In The Middle (MITM) attack. Traffic analysis attacks may occur when the attacker is able to obtain confidential information such as an employee’s authentication information. This threat can be mitigated by using secure

routing procedures such as routing through several paths. Sinkhole attacks involve the manipulation of one of the nodes to redirect the transmission signal to a different destination that can invalid data safety and result in dropping the information packets. The attacks that comes from outside the network can be secured using different techniques whilst attacks from inside the network can be secured using security aware ad-hoc routing protocol (SAR) [6]. Finally, MITM attacks may occur when the attacker can intercept restricted information. This threat can be mitigated using point-to-point encryption techniques such hash functions [7] to ensure data integrity.

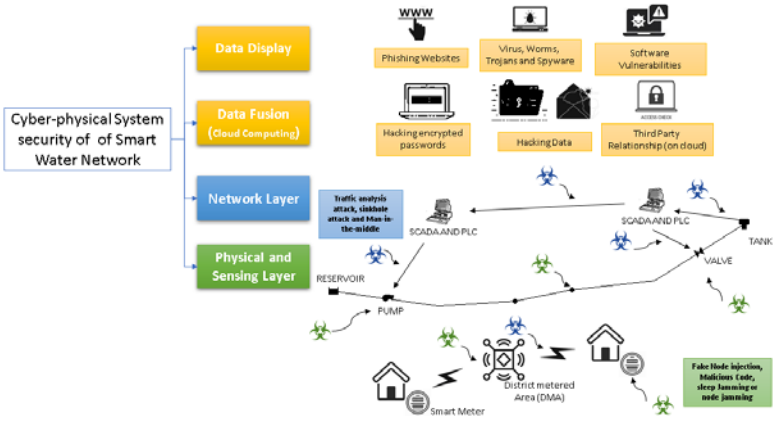

Figure 1 Smart Water Network layers with the potential CPS attacks

There are many other attacks and prevention techniques that focus on the data management and display and data fusion and analysis layers. Cloud application security, cloud data security, underlying IT infrastructure security, virtualization threats, phishing attacks, virus, worms, malicious attacks, software vulnerabilities are just a few examples. The majority of these threats/countermeasures are actively been mitigated/investigated using/by third parties such as google cloud, IBM, android things, and Microsoft azure. Therefore, third-party relationships require particular attention from water utilities to reduce the entry points for the attackers. High-level encryption such as advanced encryption standards [8] should be considered when storing or sending data.

Recommendations and Conclusions

CPSS is fundamental to enable Water 4.0 and SWNs. This paper has presented a brief review of the potential attacks and prevention approaches with focus on each layer of the SWN architecture. Based the these and on the impact of these attacks on SWNs it is possible to state that lightweight encryption and anomaly detection techniques need further investigation as the commercial Internet of Things (IoT) nodes may not be able to use the normal encryption and anomaly detection techniques due to the low processing and power capabilities.

REFERENCES

[1] A. Ginter, “The Top 20 Cyber Attacks Against Industrial Control Systems, Waterfall security Solutions, 2017.
[2] RiskIQ Evil Internet Minute 2.0 report, 2018.
[3] J. R. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, pp. 99-106, 2016.
[4] G. Avoine, M. A. Bingo, X. Carpent, S. Berna, O. Yalcin, and S. Member, “Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography,” EEE Trans. Mob. Comput., vol. 12, no. 10, pp. 2037–2049, 2013.
[5] D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui,and M. Laurent, “E2E: An Optimized IPsec Architecture for Secure And Fast Offload,” in Seventh International Conference on Availability, Reliability and Security E2E:, 2012.
[6] S. Sharmila, “Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms,” IEEE, pp. 0–5, 2011.
[7] C. Chen, Y. Lin, Y. Lin, and H. Sun, “RCDA□: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks,” IEEE Trans. PARALLEL Distrib. Syst., vol. 23, no. 4, pp. 727–734, 2012.
[8] D. Koo, J. Hur, and H. Yoon, “Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage q,” Comput. Electr. Eng., vol. 39, no. 1, pp. 34–46, 2013.