SCADA Vulnerabilities and Existing Security Approaches Towards Industrial Protection

Daniel José Franco, Abdullah Muhammed, Shamala K. Subramaniam, Azizol Abdullah

Abstract**: *Attackers, spread all around the world, have become a major threat to SCADA systems, since they started using opened-standard networks, integrated to corporate networks and accessing the Internet. It is true that there are also many different security solutions and techniques available, such as firewalls, encryption, network traffic analysis and a few others, though, intruders still managed to gain access and control delicate systems. Pointed as a non-invasive solution, intrusion detection systems (IDS) are able to monitor and report activities of any anomaly or strange patterns. However, due to the lack of SCADA network traffic data, such IDS solutions are still primitive and based on just well-known vulnerabilities and attacks, where a dedicated IDS is necessary to properly protect SCADA in water distribution systems. This study highlights SCADA vulnerabilities and security issues, through a qualitative approach, using known attacks and examples in security as case studies and aiming to present scenarios on this issue, as well, an overview of today's SCADA vulnerabilities and main threats. Results show that the identification of Intrusion Detection Systems (IDS), with their approaches and types, also widely implemented in regular IT networks, help on providing a higher security level and identifying abnormal traffic data. Such systems have indeed shown a good success rate on identifying malicious traffic in SCADA networks, mainly because of their evolution to Ethernet and open communication protocols. Based on these singular characteristics, studying SCADA networks and their communication protocols is seen as a major factor to properly develop robust security mechanisms and tolls.***

Keywords : Intrusion Detection Systems, SCADA Networks, SCADA Security Tools, Variabilities, SCADA Communication Protocols, SCADA for Water Distribution Systems.

Revised Manuscript Received on September 30, 2020.
* Correspondence Author

Daniel José Franco*, Department of Communication Technology and Network, University Putra Malaysia, Serdang, Malaysia. Email: daniel.franco@sapo.pt

Abdullah Muhammed*, Department of Communication Technology and Network, University Putra Malaysia, Serdang, Malaysia. Email: abdullah@upm.edu.my

Shamala K. Subramaniam, Department of Communication Technology and Network, University Putra Malaysia, Serdang, Malaysia. Email: shamala_ks@upm.edu.my

Azizol Abdullah, Department of Communication Technology and Network, University Putra Malaysia, Serdang, Malaysia. Email: azizol@upm.edu.my

I. INTRODUCTION

Attackers, spread all around the world, have become a major threat to SCADA systems (Supervisory Control and Data Acquisition), since they started using opened-standard networks. It is true that there are also many different security solutions and techniques available, such as firewalls, encryption and a few others, though, intruders still managed to gain access and control delicate systems. Pointed as a non-invasive solution, IDSs are able to monitor and report activities of any anomaly or strange patterns. However, due to the lack of SCADA network traffic data, such IDS solutions are still primitive and based on just well-known vulnerabilities and attacks, where a dedicated IDS is necessary to properly protect SCADA in water distribution systems [1]. A deeper approach to SCADA security risks and vulnerabilities, shows that such systems were mainly designed to give an answer to efficiency rather than security, where it was used closed networks with a really low risk of attack. Though these networks were initially developed and thought to be working in an isolated way from other communication networks, today's pictures show a total different scenario, where SCADA systems started to be integrated into corporation networks and the Internet, through the use of TCP/IP communication networks and open-standard protocols. This new reality, brought new vulnerabilities and attack vectors became available and easier to explore. Recent studies confirm that attacks have unfortunately increased over the years, where, before the year of 2000, nearly 70% of the reported events were related to attacked from malicious insiders. On the other hand, after 2001, the top 70% reported events were related to attacks executed from outside of the SACADA network. Cases where an attacker gains access to the system's network, since it may be possible to gain control over the entire system and devices, may result in serious damages, financial losses and, in a deeper approach to water systems, have also a high impact on human health, putting lives in danger[2]. Designed to maintain a high level of performance, SCADA communication protocols do not have strong security tools on their own, using just simple mechanisms that are not able to properly protect the communications, and, consequently, opening ways for attackers to succeed [3]–[5]. [6] state that the low SCADA security level is directly related to financial issues, where are based in less expensive TCP/IP, Ethernet and Microsoft Windows systems that have a large number of known vulnerabilities and security problems.

Retrieval Number: 100.1/ijitee.J76340891020
DOI: 10.35940/ijitee.J7634.0991120
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

It is possible to identify two different categories of SCADA security issues, being the first one related to terrorist attacks and other direct security threats and the second one related to indirect security threats, including spyware, virus and other threats on the software level. Moreover, [7] points that on SCADA, security issues are mainly related to the legacy problem of outdated operating systems and other software, that is not always easy to update or patch, since the system must be in operation 24h a day, 7 days a week. Also, systems are not redesigned for many decades.

Their nature, controlling and monitoring critical industrial infrastructures makes it difficult to apply security patches, where a test environment is, apart from expensive, almost impossible to maintain and a simple patch, if not careful and properly applied may result in the disruption of the service or even ends opening more vulnerabilities or back doors. Such concerns make SCADA systems to still work on old and outdated software that are, most of the time, no longer supported by their developers and vendors. Countermeasures, similar to the ones implemented on regular IT systems, are not easy to apply. SCADA is a sensitive system where a simple break on the communication may result in grave danger and damages. Some of the existing countermeasures, such as cryptography algorithms, like [8], [9], require extreme caution and their implementation must be carefully followed. However, some mechanisms are indeed able to protect SCADA systems without putting them in a danger stage, including firewalls and intrusion detection systems. Also, VPN connections and dedicated lines are pointed in a way to promote SCADA security. Though, firewalls are not efficient when the attack vector is an authorized computer outside or inside the automation system that has already been corrupted [10]. Taking the example of an authorized engineer that can use his laptop connected to a SCADA LAN, if the laptop is infected by malware, may allow unauthorized access to the system [11].

As it was mentioned before, IDS systems are one of the countermeasures that can be applied to SCADA networks, however, current IDS techniques are still in their embryonic stage and far from achieving their maturity. Classical Signature-Based approaches are primitive for such critical systems [12], confirming the need of development of well-tailored and dedicated intrusion detected system to SCADA and automation systems in water distribution [10]. There are many different Model-Based intrusion detection techniques proposed for SCADA networks, however, almost none of them can actually be implemented in real systems [13].

A. Research Objectives

This paper highlights SCADA systems used on water distribution systems' (WDS) control ana management, aiming to answer the following questions and objectives:

1) To understand the different SCADA modules and characteristics;

2) To understand the different possible security approaches capable to protect SCADA systems without compromising their normal performance.

II. LITERATURE REVIEW

Many different attacks, including denial-of-service, flooding and code injection that were not an issue in old times, are now possible threats to SCADA networks using opened communication standards and protocols. The example of the Stuxnet that, in 2010, attacked the Iranian SCADA system controlling the uranium enrichment, came to give a warning that new SCADA networks are in need of a high level of security and protection. The malware damages all databases and infected not just the Iranian SCADA, in 2010, but also a larger number of other systems, since 2009, where more than 100.000 infections were registered also in Indonesia and India. Apart from destroying the system databases, no other major consequences were registered and no lives were put in danger. Though, this malware, came to alert the major risk that modern SCADA systems are facing, if robust precautions and countermeasures are not developed and properly implemented [14]. There are already a few studies focusing SCADA networks' security and privacy, including mechanisms such as fireworks and cryptography. The study developed by [15] is a good example on the analysis of some possible security solutions for SCADA systems, focusing on its unicast, multicast, broadcast and polling communications. The authors apply secure cryptographic algorithms, including the RSA, AES and SHA2 hash to the different communication types, in a way to protect the communications among the different SCADA devices. They declare that the experiment results presented a good efficiency of the system, while using cryptography, highlighting that unicast communications were able to achieve around 91% of the normal system performance, when no algorithm is applied. Though, the authors do not mention any information of the impact rate that those algorithms may cause to the communications neither to their possible application to wireless sensors and other low powered devices with low computational capabilities. Taking the lack of security in traditional SCADA communication protocols and standards as the study foundation, [16] described IEC62351 and AGA-12 as the new SCADA standards that offer a higher security level for the communications, however, such standards also show a lower system performance. Due to the use of cryptography that demands messages encryption and decryption, communications are performed in a much lower rhythm, decreasing the normal processing and communication time and, consequently, turning the system slower and with a lower performance. In a way to address this issue, authors propose a lightweight algorithm, using a public key structure (NTRU), to allow end-to-end security. Their results declare a better system performance, when compared to the traditional RSA and ECC algorithms, included on these new SCADA standards, and faster encryption and decryption process.

Another important cryptographic approach is presented by [8]. The authors take advantage of the Elliptic Curve concept of the Diffie-Helman to develop an algorithm that uses sessions keys in the master station. This study uses a decentralized key distribution model, taking into consideration the low computational capabilities of slave stations and remote devices. Results show a comparison between this solution and other similar ones, where, in this case, it was achieved a lower delay time and energy consumption. Early SCADA IDS solutions were basically monitoring techniques able to detect abnormal behavior of the system and most studies used to focus on lightweight model algorithms and fuzzy techniques to detect such abnormal symptoms. According to those studies, intrusion patterns in SCADA networks are needed and may be developed through traffic correlation and system configuration for man-in-the-middle attack monitoring.

Among the existing studies in this field, the major research methods highlight the use of white and blacklist rules, the need of real industrial network traffic analysis and the need of automated rules production to given an answer to large networks [17].

[18] stated that installation of a dedicated and up to date IDS system in SCADA networks perimeter or intersection may significantly increase the protection and security levels not just in the network, but also to the entire system.

III. METHODOLOGY

This study is performed in a qualitative way, focusing on known attacks and examples of SCADA security mechanisms as case study. A qualitative approach makes it easier to achieve results and answer the initial objectives and research questions, using international documents, articles and books as may data source. The study provides an overview of todays' SCADA threats and vulnerabilities, highlighting some countermeasure and cryptographic solutions, through a qualitative analysis [19]–[25].

IV. RESULTS AND FINDINGS

Intrusion detection system, as mentioned by [7], is a mechanism that can be applied to improve SCADA systems security. Recently, intrusion detection systems, or IDS, are being proposed to help network administrators to analyze the security risks and detect attacks against their SCADA networks and SCADA systems [13], [26].

Like on SCADA, IDS systems are widely implemented in regular IT networks, in order to identify abnormal traffic data. Such systems have indeed shown a good success rate on identifying malicious traffic in SCADA networks, mainly because of their evolution to Ethernet and open communication protocols. Though, there are also weak points related to this type of security mechanism, where specific attacks to communication protocols and devices are not correctly identified. To address this issue, an effective IDS system must be able to inspect and analyze SCADA message payloads [13].

Most SCADA systems have already included a firewall device, protecting the system and network by specific actions and rules. Analogically speaking, a firewall can be seen as a protecting wall, providing a secure access to and from outside. On the other hand, an IDS system can be seen as cameras and sensors that constantly monitor the place. It is usually composed by a management console, to manage and report intrusions, and the sensors that work as agents, monitoring network devices in real-time [11].

Historically speaking, there are different types of intrusion detection systems, classified according to their nature and way of working [27]. [13] classify IDS systems into two main categories: Signature-Based and Anomaly-Based. Signature-Based approaches are designed based on known attack patterns and are used as rule sets, such as the ones used by Snort IDS. Incoming traffic is then compared to these rules, in order to identify abnormal traffic among the normal one [13], [27].

Contrasting with the previous category, Anomaly-Based methods are based on the idea of normal behavioral profiles, flagging divergent profiles during intrusion detection. This type of approach often returns a high false alarm rate, when detecting new attacks [13], [27]. It is also common to find IDS systems categorized as Host-Based (HIDS) and Network-Based (NIDS). When compared, a Host-Based IDS system assumes the responsibility of monitoring the behavior of a single host, while a Network-Based IDS system collects evidences through network traffic data analysis [11], [12]. [28] consider the combination of these two IDS categories as the best way to protect SCADA networks against cyber-attacks, though, they are still too immature to be widely deployed. Also, it is possible to identify a weak point in HIDS that must be improved, when it may fail to correctly detect an intrusion in case the host is compromised. In conventional IDS systems, the paradigm of denying access to malicious packets by dropping them or their root is entirely accepted. However, due to their critical nature, such paradigm is not acceptable in SCADA networks. SCADA systems require regular and constant communications among devices and controllers, where an unavailable root or packet may compromise the entire system, resulting in catastrophic consequences [18].

In their study, [12] highlighted the existing weaknesses and singular characteristics of SCADA systems that must be taken into consideration before the implementation of an IDS system. SCADA main components, such as PLCs and RTUs have usually low computational and memory capabilities, making them not suitable to allocate a HIDS that must be installed on the host itself for it to be analyzed. On the other hand, NIDS sensors can be installed in a separated machine connected to the network to be monitored. Such approach can be easily integrated with the SCADA system, where it is necessary to understand and analyze communication protocols. However, in their current implementations, SCADA communication protocols, which were initially designed to work in serial communications, are embedded into TCP packets' payloads. Traditional NIDS, such as Snort and Suricata [13], have no capability to understand well those protocols and only recently a set of ad-hoc rules and pre-processing modules have been turned available for SCADA attacks detection. Such approach misses the most significant potential threats to SCADA networks as they do not analyze SCADA protocol messages. [29] state that the performance of current IDSs is still too poor when compared to the increasing number of existing vulnerabilities. Many IDS are based on expert rules that are manually designed and created, describing only known attack signatures.

The authors developed a framework to better analyze the technical challenges in general IDSs, based on machine learning, including the data acquisition and feature extraction, real-time detection and machine learning. Sharing SCADA traffic data is a vital factor to better improve IDSs, analyzing security risks and develop appropriate security solutions. However, privacy of communications is a big concern among SCADA owners, making difficult to obtain traffic data to be analyzed and, consequently, resulting in less robust IDSs.

A key challenge with SCADA traffic data is the large number of variables and attributes that must be analyzed, including categorical attributes with unranked nominal values, numerical byte counts, categorical protocols and hierarchically structured IP addresses [26]. Penetration attacks in SCADA systems are also rarely reported, due to the sensitive nature of these systems, therefore, network traffic and logged data are not turned publicly available for security experts to analyze and discover possible solutions.

In order to address the issue of the privacy in the communications, authors developed a framework (privacy preserving framework) capable of satisfying the privacy requirements while maintaining sufficient data utility. However, the research was limited due to the lack of proper modelling tools and had an issue related to the computational time problem, forcing the use of parallel computing with multi-core-CPUs and GPUs. Once again, [30] state that SCADA security is a major role to properly protect and manage critical industrial infrastructures and must be carefully implemented to avoid not just possible attacks, but also damages to the system that may cause catastrophic results. As so, authors focus their study on the use of Intrusion Detection System, highlighting their major importance and identifying them as major tools to properly find, track and control malicious events on the system and its networks. The authors developed an anomaly detection mechanism that uses traffic periodicity as base, where this periodicity is the key factor for any DoS and information gathering attacks (Fig. 1).

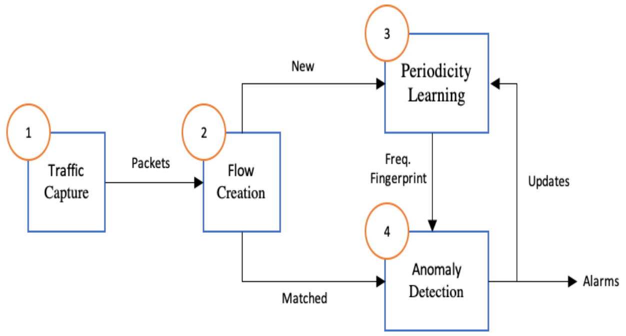

Fig. 1. Periodicity Based Anomaly Detection in SCADA Networks – Source: (Barbosa et al., 2012)

On their research, [31] wanted to address four attack categories (reconnaissance, response injection, command injection and denial of service) through the investigation of traffic periodicity and telemetry patterns on SCADA network traffic, because they state that the majority of SCADA network traffic presents periodic patterns. To fulfil their objectives, the authors started creating an analyzer algorithm, able to identify the periodicity characteristics and designed an auxiliary module to analyze telemetry patterns.

[32] state that intrusion detection in real-time is yet a problem without a concrete solution. For critical systems such as SCADA networks, the inexistence of a strong defense mechanism able to cooperate with another security mechanism for intrusion detection may result in false positive alarms or mistakes on the origin of the intrusion and, consequently, put the entire system in a high-security risk. The authors also state that the effect of the most known attacks may result in devastating costs on SCADA systems. Therefore, to properly address this issue, they identify the development of an IDS system specifically design to SCADA systems and networks, able to ensure adequate balance between high accuracy, low false alarm rate and reduced network traffic over-systems, as a must [32]. Protecting SCADA systems and networks against cyber-attacks and other types of threats is a pertinent theme with importance not just to smart water systems, but also to other types of industries [33].

A more recent study, done by [34] focus the use of Intrusion Detection Systems in wireless sensor networks used on industrial environment (WISN), namely the ones used on SCADA systems.

The authors state that WISN are seen as one of the main targets for attackers, suffering from the same type of security issues and security threats that affect classical wireless sensor networks (WSN). [34] also state that, in SCADA systems, due to their singular nature, controlling sensitive and critical infrastructures, attack consequences may result in simple network accesses, but also in a complete control and shutdown of the entire system.

This is a major concern, since it may affect many different areas, such as financial and economic and, in worse scenarios, human lives. In order to address this issue, the authors identify the need of Intrusion Detection Systems, associated to cryptographic and secure authentication mechanisms as main security features to be implemented.

However, such mechanisms and techniques cannot be applied to WSN in the same way they are used in classic wireless networks, as they have several characteristics, such as low processing power and low energy consumption needs, demanding primary adaptation.

An efficient Intrusion Detection System must be able to collect and analyze all exchanged packets in both local and end-to-end communications.

Based on this fundamental principle, [34] focused on the development of an IDS scheme, specially designed to networks used by SCADA systems, building a wireless backbone to increase the network security. The study held by [35], focuses, once again, on anomaly detection system applicable to SCADA networks and its communications, but, this time, not emphasizing intrusion detection systems in particular, but different anomaly detections applied within a resilience framework. Their results show, in 2014, an increase of 100% of SCADA's cyber-attacks, when compared to the previous year, concluding that this is due to a large number of vulnerabilities applied to new opened networks that are now being used by SCADA systems and that security mechanisms are still not robust enough as it was expected.

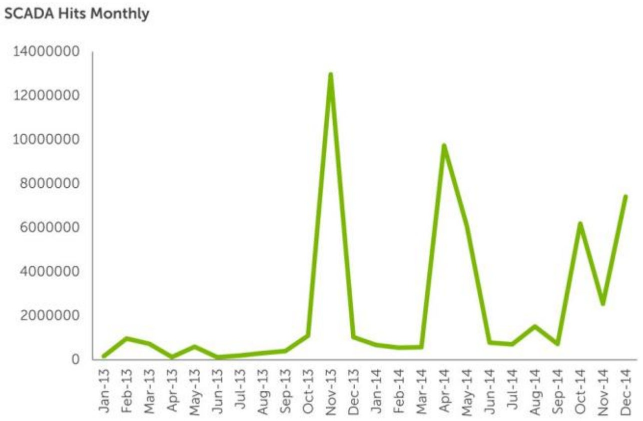

Fig. 2. Number of SCADA attacks over 2013 and 2014 – Source: automation.com

Specific devices, such as master terminal units and remote terminal units, are also threatened by possible vulnerabilities exploitation, taking advantage of the weak authentication mechanisms available on communication protocols (Modbus, DNP3 and Profibus). Therefore, [35] state that prompt anomaly detection in SCADA systems and its supporting communications infrastructure is a critical issue that must be addressed as soon as possible. This study, however, was performed in a laboratory environment, where datasets were obtained through the simulation of real anomalies and normal activities in gas pipeline, controlled by a SCADA system. Results may be different if the techniques are applied in real time systems.

Recent studies focus a State-Base approach to a dedicated SCADA IDS protection. As described by [10], [11] the normal devices state can be used to detect attacks and anomalies in the network. [17] states that a Status-Based IDS is capable of detecting a single Modbus packet attack by analyzing the normal operation of the system. Also, [28] states that this approach is more advanced than a Signature-Based NIDS, since it monitor the states of a SCADA system, detecting a complex attack through traffic analysis and keeping track of the system states, comparing them with the stored rules. Critical state rules represent the combination state of related control devices, where an attack is identified if this combinatorial state achieves a critical state for the system. A good example on this IDS approach was studied by [11], however, the author focused just SCADA systems for power grids.

The study performed by [12], focuses specifically on Modbus and DNP3 protocols and how a state-based intrusion detection system could be done. The authors state, once again, that classical signature-based IDS approaches are considered primitive, in relation to SCADA and other industrial systems, since they are able to protect against single packet-based attacks only, where protection related to more robust and strong attacks is still not enough. Moreover, authors also highlight the issues brought by the use of modern technologies to improve performance in SCADA systems, opening the systems to a large number of vulnerabilities and security issues. On their study, they present an approach to the design of a state-based IDS system to protect Modbus and DNP3 SCADA networks, aiming to protect them from more complex attacks than the ones approached with signature-based rules. The solution, however, uses a virtual representation of the real system, being in constant contact with it and updating its virtual database, not just based on the network traffic, but also from the real values of the system, which may result in a vulnerability by itself. Focusing on the same solution, [36]–[38] propose a special language for state-based IDS rules and packet capture, however, such rules must be manually created and do not respect system privacy, where data, such as IP addresses, are kept visible. In addition, authors do not use any type of database encryption, putting the system itself in a vulnerable level. Their solution requires a pre-design organization of rules, so all SCADA components are properly addressed.

V. CONCLUSION

Based on many different scholars, it is possible to highlight some of the main issues SCADA systems are facing, due to their evolution to TCP/IP networks. Not just the number of vulnerabilities is higher, by the no existence of security mechanisms on its communication protocols and the lack of patching and updating of operating systems that work 24h a day, 7 days a week, the systems are constantly put in a great danger. Security mechanisms are still primitive and not robust enough to protect such sensitive systems. The use of traditional security tools does not properly protect SCADA and the use of cryptography must be applied with special care, since they may disrupt communication among system's components. Also, sensors are not powered enough to deal with robust cyphers, neither algorithms, making cryptography a difficult solution. Moreover, the lack of network traffic data, due to privacy issues, turns it difficult to properly develop and design security solutions dedicated to SCADA, where the study of traditional anonymization algorithms and their combination into a dedicated anonymization tool may increase privacy level and give SCADA owns a better comfort on providing their systems' network traffic data to be used on research. Existing IDS rules for SCADA systems are still not robust enough and based on known attack signatures. IDS is pointed as one of the best possible solutions to increase SCADA networks security.

REFERENCES

1. T. Bradley, "What is an IDS and Why Do You Need It?," *Alert Logic*, 2018. .
2. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security Issues in SCADA Networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, 2006, doi: 10.1016/j.cose.2006.03.001.
3. D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations," *CSI Trans. ICT*, vol. 1, no. June, pp. 135–141, 2013, doi: 10.1007/s40012-013-0013-5.
4. D. J. Franco, R. M. Silva, A. Muhammed, O. K. Akram, and A. Graça, "Network Security Evaluation and Training Based on Real World Scenarios of Vulnerabilities Detected in Portuguese Municipalities' Network Devices," in *Advances in Intelligent Systems and Computing(AISC)*, vol. 942, A. M. Madureira A., Abraham A., Gandhi N., Silva C., Ed. Springer, Cham, 2019, pp. 288–297.
5. D. J. Franco, A. Muhammed, S. Subramaniam, A. Abdullah, R. M. Silva, and O. K. Akram, "A Review on Current and Old SCADA Networks Applied to Water Distribution Systems," in *First International Conference of Intelligent Computing and Engineering (ICOICE)*, 2019, pp. 1–11, doi: 10.1109/ICOICE48418.2019.9035134.
6. J. Gao *et al.*, "SCADA Communication and Security Issues," *Secur. Comm. Networks*, vol. 7, pp. 175–194, 2014, doi: 10.1002/sec.698.

7. Y. Cherdantseva *et al.*, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2015, doi: 10.1016/j.cose.2015.09.009.
8. A. Rezai, P. Keshavarzi, and Z. Moravej, "Secure SCADA Communication by Using a Modified Key Management Scheme," *ISA Trans.*, vol. 52, no. 4, pp. 517–524, 2013, doi: 10.1016/j.isatra.2013.02.005.
9. A. Tesfahun and D. L. Bhaskari, "A SCADA Testbed for Investigating Cyber Security Vulnerabilities in Critical Infrastructures," *Autom. Control Comput. Sci.*, vol. 50, no. 1, pp. 54–62, 2016, doi: 10.3103/S0146411616010090.
10. F. Schuster and A. Paul, "A Distributed Intrusion Detection System for Industrial Automation Networks," *Proc. 2012 IEEE 17th Int. Conf. Emerg. Technol. Fact. Autom. (ETFA 2012)*, pp. 1–4, 2012, doi: 10.1109/ETFA.2012.6489703.
11. H. Waagsnes, "SCADA Intrusion Detection System Test Framework," University of Agder, 2017.
12. I. N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta, and M. Masera, "Modbus/DNP3 state-based intrusion detection system," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 729–736, 2010, doi: 10.1109/AINA.2010.86.
13. J. Nivethan and M. Papa, "Dynamic Rule Generation for SCADA Intrusion Detection," *2016 IEEE Symp. Technol. Homel. Secur. HST 2016*, pp. 1–5, 2016, doi: 10.1109/THS.2016.7568964.
14. M. Ozturk and P. Aubin, "SCADA Security : Challenges and Solutions," 2011.
15. Aa. Shahzad, Z. Guangzhi, H. Chae, M. Lee, and M. Irfan, "The Approximate Approaches in Addressing of SCADA Security Issues," *J. IT Econ. Dev.*, vol. 6, no. 2, pp. 31–35, 2015.
16. A. P. Premnath, J. Y. Jo, and Y. Kim, "Application of NTRU Cryptographic Algorithm for SCADA Security," *ITNG 2014 - Proc. 11th Int. Conf. Inf. Technol. New Gener.*, pp. 341–346, 2014, doi: 10.1109/ITNG.2014.38.
17. S. J. Kim, B. H. Kim, S. S. Yeo, and D. E. Cho, "Network anomaly detection for m-connected SCADA networks," *Proc. - 2013 8th Int. Conf. Broadband, Wirel. Comput. Commun. Appl. BWCCA 2013*, pp. 351–354, 2013, doi: 10.1109/BWCCA.2013.61.
18. C. Valli, "Snort IDS for SCADA Networks," *Management*, no. 2009, pp. 618–621, 2009, [Online]. Available: http://ro.ecu.edu.au/ecuworks/529/.
19. O. K. Akram, D. J. Franco, and S. Ismail, "Development Phases from Heritage Buildings to Smart Buildings," *Int. J. Eng. Technol. Manag. Appl. Sci.*, vol. 4, no. 4, pp. 6–13, 2016, doi: https://www.researchgate.net/publication/299994273_Development_Phases_from_Heritage_Buildings_to_Smart_Buildings.
20. O. K. Akram, N. F. Mohammed Jamil, D. J. Franco, S. Ismail, and A. Graça, "The Preservation of Significant Islamic Architectural Heritage of Al-Mustansiriya School, Baghdad City, Iraq," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 7S2, pp. 1–7, 2019.
21. D. J. Franco, R. M. Silva, A. Muhammed, O. K. Akram, and A. Graça, "Network Security Evaluation and Training Based on Real World Scenarios of Vulnerabilities Detected in Portuguese Municipalities' Network Devices," in *Advances in Intelligent Systems and Computing(AISC)*, vol. 942, A. M. Madureira A., Abraham A., Gandhi N., Silva C., Ed. Springer, Cham, 2020, pp. 288–297.
22. O. K. Akram, S. Ismail, N. F. Mohammed Jamil, D. J. Franco, A. Graça, and A. R. Carvalho, "Classification of International Policies of Tangible Heritage for Historic Sites," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 7S2, pp. 13–21, 2019, [Online]. Available: https://www.researchgate.net/publication/333561986_Classification_of_International_Policies_of_Tangible_Heritage_for_Historic_Sites.
23. O. K. Akram, D. J. Franco, N. F. Mohammed Jamil, A. Graça, and S. Ismail, "How to Guide your Research using ONDAS Framework," Beja, Portugal, 2018.
24. O. K. Akram, N. F. Mohammed Jamil, S. Ismail, D. J. Franco, and A. Graça, "The importance of the heritage values of Al-Ukhaidhir palace, Karbala city, Iraq," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 401, no. 1, pp. 2–3, 2018, doi: 10.1088/1757-899X/401/1/012030.
25. O. K. Akram, D. J. Franco, S. Ismail, A. Muhammed, and A. Graça, "Promoting Heritage Management in New Smart Cities: Évora City, Portugal as a Case Study," *Int. J. Eng. Technol. Manag. Appl. Sci.*, vol. 4, no. 9, pp. 148–155, 2016, doi: https://www.researchgate.net/publication/321442902_Promoting_Heritage_Management_in_New_Smart_Cities_Evora_City_Portugal_as_a_Case_Study.
26. A. Fahad, Z. Tari, A. Almalawi, A. Goscinski, I. Khalil, and A. Mahmood, "PPFSCADA: Privacy Preserving Framework for SCADA Data Publishing," *Futur. Gener. Comput. Syst.*, vol. 37, pp. 496–511, 2014, doi: 10.1016/j.future.2014.03.002.
27. C. E. Texas, "BLOOM FILTER BASED INTRUSION DETECTION FOR SMART GRID SCADA Saranya Parthasarathy and Deepa Kundur," no. May, 2012.
28. M. Anisheh, D. Lindskog, P. Zavarsky, and R. Ruhl, "SCADA Full State Network Intrusion and Malfunction Detection System," pp. 1–9, 2010.
29. D. P. Vinchurkar and A. Reshamwala, "A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique," *Int. J. Eng. Sci. Innov. Technol.*, vol. 1, no. 2, pp. 54–63, 2012.
30. R. R. R. Barbosa, R. Sadre, and A. Pras, "Towards Periodicity Based Anomaly Detection in SCADA Networks," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, pp. 0–3, 2012, doi: 10.1109/ETFA.2012.6489745.
31. J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion Detection in SCADA Systems by Traffic Periodicity and Telemetry Analysis," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Augus, pp. 318–325, 2016, doi: 10.1109/ISCC.2016.7543760.
32. L. A. Maglaras, J. Jiang, and T. Cruz, "Integrated OCSVM Mechanism for Intrusion Detection in SCADA Systems," *Electron. Lett.*, vol. 50, no. 25, pp. 1935–1936, 2014, doi: 10.1049/el.2014.2897.
33. Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. F. Wang, "Rule-Based Intrusion Detection System for SCADA Networks," *Renew. Power Gener. Conf. (RPG 2013), 2nd IET*, pp. 1–4, 2013, doi: 10.1049/cp.2013.1729.
34. L. Bayou, N. Cuppens-Boulahia, D. Espes, and F. Cuppen, "Towards a CDS-based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks," *2016 11th Int. Conf. Availability, Reliab. Secur.*, pp. 157–166, 2016, doi: 10.1109/ARES.2016.48.
35. S. N. Shirazi *et al.*, "Evaluation of anomaly detection techniques for SCADA communication resilience," *Proc. - 2016 Resil. Week, RWS 2016*, pp. 140–145, 2016, doi: 10.1109/RWEEK.2016.7573322.
36. I. Nai Fovino, A. Carcano, A. Coletta, M. Guglielmi, M. Masera, and A. Trombetta, "State-based firewall for industrial protocols with critical-state prediction monitor," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6712 LNCS, pp. 116–127, 2011, doi: 10.1007/978-3-642-21694-7_10.
37. I. Nai Fovino, A. Coletta, A. Carcano, and M. Masera, "Critical state-based filtering system for securing SCADA network protocols," *IEEE Trans. Ind. Electron.*, vol. 59, no. 10, pp. 3943–3950, 2012, doi: 10.1109/TIE.2011.2181132.
38. I. N. Fovino, M. Masera, M. Guglielmi, A. Carcano, and A. Trombetta, "Distributed intrusion detection system for SCADA protocols," *IFIP Adv. Inf. Commun. Technol.*, vol. 342 AICT, pp. 95–110, 2010, doi: 10.1007/978-3-642-16806-2_7.

AUTHORS PROFILE

Daniel José Franco received the B.Sc. degree in computer engineering from Polytechnic Institute of Beja, Portugal, in 2007 and the M.Sc. degree in computer security engineering from Polytechnic Institute of Beja, Portugal, in 2014. He is currently pursuing the Ph.D. degree in computer networks at University Putra Malaysia, Malaysia. From 2008 to 2011, he was a network engineer with the City Hall of Beja, Portugal and from 2011 to 2013, he was a lecturer with the Department of Engineering at Superior School of Technology and Management, Polytechnic Institute of Beja, Portugal. His research interest includes computer networks, computer security, Internet of things, smart cities and smart urban development, being author and co-author of about 10 scientific publications and co-founder of ONDAS Group. Since 2014 he is the head of the IT department at the City Hall of Alcácer do Sal, Portugal. Mr. Franco's awards and honors include the first place in the Summer School on Information and Communication Technologies and Law, Istanbul Kemerburgaz University, Turkey.

Abdullah Muhammed is an Associate Professor at the Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia. He received the Bachelor degree in Computer Science from Universiti Putra Malaysia in 1998, the Master degree in Computer Science from Universiti Malaya in 2004 and the PhD degree in Computer Science from University of Nottingham, United Kingdom, in 2014. His research interests include grid/cloud computing, Wireless Sensor Network/IoT, heuristic and optimization. For more information please email him at abdullah@upm.edu.my.

Shamala K. Subramaniam is a Professor in the Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. Presently she also serves as the Director of the Sports Academy, Universiti Putra Malaysia. She serves as the Chairman for Ph.D. and Master's Thesis Supervisory Committee. She has a high number of cited publications in reputed high impact and indexed journals.
She has authored Chapter(s) in book and lecture series. She has been recognized as a Member of Editorial Advisory Board in national and international journals. She addresses key note in several national and international forums. She is the Director of National Olympic Academy of the Olympic Council of Malaysia, an Executive Board member of the OCM, a board member of the National Sports Institute, Deputy President of the Malaysian Hockey Confederation and an Executive Member of the Asian Hockey Federations.

Azizol Abdullah obtained his Master of Science in Engineering (Telematics) from the University of Sheffield, UK in 1996 and his PhD in Parallel and Distributed System from Universiti Putra Malaysia, Malaysia in 2010. He is an Associate Professor at Department Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia. He is a member of Information Security Research Group and; Network, Parallel and Distributed Computing Research Group. He is also has been appointed as Fellow Researcher for ITU-UUM Asia Pacific Centre of Excellence For Rural ICT Development (ITU-UUM). His main research areas include cloud and grid computing, network security, wireless and mobile computing and computer networks.