International Journal of Technology (2018) 4: 828-839
ISSN 2086-9614

IMPROVING THE RESILIENCE OF WIRELESS SENSOR NETWORKS AGAINST SECURITY THREATS: A SURVEY AND OPEN RESEARCH ISSUES

Saqib Ali[1,3*], Taiseera Al-Balushi[1], Zia Nadir[2], Omar Khadeer Hussain[3]

[1]*Department of Informations System, College of Economics and Political Science,Sultan Qaboos University, Al Khoudh,Muscat 123, Oman*
[2]*Department of Electrical and Computer Engineering, College of Engineering,Sultan Qaboos University, Al Khoudh,Muscat 123, Oman*
[3]*The School of Business, University of New South Wales, Canberra, Northcott Dr, Campbell ACT 2612, Australia*

(Received: January 2018 / Revised: March 2018 / Accepted: April 2018)

ABSTRACT

Wireless Sensor Network (WSN) technology has gained importance in recent years due to its various benefits, practicability and extensive utilization in diverse applications. The innovation helps to make real-time automation, monitoring, detecting and tracking much easier and more effective than previous technologies. However, as well as their benefits and enormous potential, WSNs are vulnerable to cyber-attacks. This paper is a systematic literature review of the security-related threats and vulnerabilities in WSNs. We review the safety of and threats to each WSN communication layer and then highlight the importance of trust and reputation, and the features related to these, to address the safety vulnerabilities. Finally, we highlight the open research areas which need to be addressed in WSNs to increase their flexibility against security threats.

Keywords: Countermeasures; Reputation; Security; Threats; Trust; Vulnerabilities; Wireless sensor network

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a system composed of devices and actuators to monitor and control any tasks associated with operations in certain environments when connected wirelessly (Yang, 2014). The generic architecture of a WSN is based on sensors placed over a specified field to sense and collect information on a specific task and to communicate back to its base station, often referred to as a data sink. The base station utilizes either public or dedicated communication links connected to a sensor network task manager (Boukerch et al., 2007; Chen et al., 2007b; Khalid et al., 2013; Sarobin & Ganesan, 2016). WSNs possess many benefits, including their low-cost, low-power, robustness, durability, small size, ease of deployment and multi-function ability (Yang & Cao, 2008; Yick et al., 2008; Li & Gong, 2008; Lasol & Pornpromlikit, 2016). Due to their extensive utilization and benefits, these sensors are frequently deployed in places such as deep water, battlefields, forests, airports and extreme temperature environments, which were very difficult to monitor in the past.

Over a period of time, the WSN concept has laid down the foundations for networks of distributed nodes that can communicate wirelessly (Estrin et al., 1999; Byers & Nasser, 2000).

*Corresponding author's email: saqib@squ.edu.om, Tel. +968 2414 2928, Fax. +968 2441 4043
Permalink/DOI: https://doi.org/10.14716/ijtech.v9i4.1526

The Institute of Electrical and Electronic Engineers (IEEE) initially issued the Smart Transducer Networking standard (Lee, 2000); the transducers were soon referred as smart sensors due to the specification of their desired functions (Lewis, 2004), and later the term Wireless Sensor Network was introduced. Subsequently, IEEE set ZigBee as the WSN standard for wireless communication (Kinney, 2003; Egan, 2005; Yang, 2014).

WSNs, like any other communication technology, are vulnerable to security attacks and possess their own security objectives. Security breaches and attacks on WSNs may lead to disastrous events and losses. The widespread application of WSNs makes them a target for attackers and hackers. Hacking into the WSN of government, military, industrial or healthcare organizations may lead to economic collapse, defeat in war, threats to nationwide security and loss of human lives. Consequently, it is extremely important to safeguard and raise the flexibility of WSN security and privacy aspects. This paper presents a literature review of the security issues and attacks on WSNs in order to improve their flexibility. Security attacks have been grouped in terms of physical, data-link, network, transport and application layers. We then move our emphasis to discussion of trust and reputation, and how their application and organization in WSNs could help ease the recognized security concerns. Finally, we highlight the open research issues that need to be addressed to improve the flexibility of WSNs with regard to security issues. The organization of the paper is as follows. Section 2 presents the research methodology adopted, while section 3 explores the different types of vulnerability which impact WSNs. Section 4 discusses in-depth the concept of trust and reputation in WSNs, which is one of the latest and most effective security measures. Section 5 presents the open research issues in relation to increasing WSN resilience, followed by the conclusion and suggestions for future research.

2. METHODOLOGY

A Systematic Literature Review (SLR) is conducted on the specified topic. The protocol for conducting such a review was given by Kitchenham in 2004 and in 2007 (Kitchenham, 2004; Kitchenham & Charters, 2007). According to Kitchenham, the SLR is a systematic procedure of identification, interpretation and evaluation of relevant studies that pertain to a given research topic or area of interest (Kitchenham & Charters, 2007). The SLR is a well-defined and stringent procedure with an unbiased research outlook, which makes it very different to the traditional literature review and helps make a significant contribution to the research and add to the scientific value. The SLR procedure of Portocarrero et al. (2014) and Pa et al. (2015) basically consists of three major steps, namely planning, conducting and reporting. In this case, the research questions, the search plan, and the organizational plan were set during the planning stage. Once the questions had been hypothesized, the search strategies were created. Some of the most well-known and efficient journal search engines, such as Springer, IEEE, ACM, Scopus, ScienceDirect, ProQuest and Google Scholar were selected. Once the initial data gathering and the selection process were complete, the database needed to be further screened and organized. Papers were initially prearranged based on the possibility of answering one or more of the planned research questions. During the screening process for each research question, the papers were further scrutinized by analyzing their organization, topics and subtopics. The organized papers were read and studied very carefully to obtain the understanding and trends in the various aspects of WSNs. The studies clearly show that there has been a drastic rise in the research into and the application of WSNs, due to its huge advantages and usefulness. It has also been observed among researchers that security concerns have at the same time increased; this is because vulnerabilities and threats have increased as the implementation of WSNs has advanced.

3. SECURITY - DIFFERENT TYPES OF VULNERABILITY IMPACTING WSNS

The WSN field is growing at an enormous speed, which fascinates many stakeholders, including governments, engineers and researchers, but also attackers. WSN wireless communication links are considered to be less secure than wired networks due to their broadcast nature, which can be easily tapped into by cyber enemies (Sarma & Kar, 2006). Attackers can easily interrupt wireless communication and replace valid packets with malicious ones. Without any acceptable safety measures, WSNs are vulnerable to various cyber-attacks. The vulnerabilities and sensor node limitations associated with wireless media pose particular security challenges. Security is normally achieved through a trusted and controlled atmosphere (Undercoffer et al., 2002; Zia & Zomaya, 2006; Ali et al., 2018). Existing security procedures aim to improve the security of WSNs from two aspects, namely security and reliability. Security aims to protect the WSN from outside attacks (Li & Gong, 2008; Lopez et al., 2009; Yu et al., 2012), whereas reliability guarantees the system output based on its specifications. Data packet detection, monitoring, sensing, transmission and event occurrence are some of the known issues with regard to reliability (Willig & Karl, 2005; Hsu et al., 2007; Mahmood et al., 2015).

The diverse set of WSN cyber-attacks can be divided into different categories; from the attackers' perspective, these are normally categorized into internal and external attacks (Yu et al., 2012; Ali et al., 2018). When an attacker is able to access a node by infringement through the cryptographic procedures, this normally occurs through an internal attack. On the other hand, external attacks are carried out through snooping and injecting fractional data into wireless networks. These attacks are further classified into logical network layers (application, transport, network, data link and physical layers) depending upon the type of attack made (Yang, 2014). The number of attacks which targeted the application layer, and the total number of attacks suffered by WSNs, are classified by Li and Gong (2008), López and Zhou (2008), Araujo et al. (2012), Lopez et al. (2010), Ali et al. (2015). Based on the survey carried out for this study, Figure 1 gives a brief overview of the various WSN layers and cyber-attacks involved.

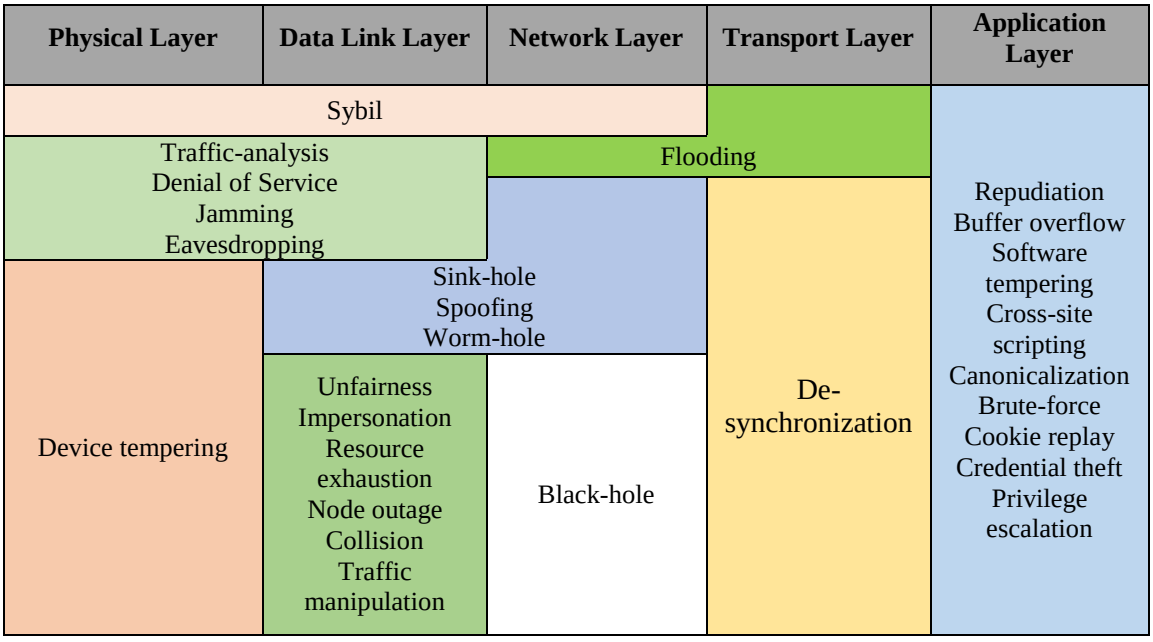

Figure 1 Attacks on various WSN layers

Trust and reputation in WSNs will be discussed in the following section. Analysis of the literature is also presented to discuss advances in WSN technology in relation to security concerns in order to improve its resilience.

4. TRUST AND REPUTATION –IMPROVING THE RESILIENCE OF WSN

Yu et al. (2010) explained that the characteristics of trust are that it is context sensitive, subjective, unidirectional and transitive. Noting this kind of behavior in humans, scholars have also attempted to apply trust to the information technology context, and during the mid-2000s the concepts of trust and reputation were first introduced into the WSN field. Trust is calculated based on the previous experience of a particular node and its degree of belief (Boukerch et al., 2007), whereas reputation is the overall perception of one node among other network nodes (Boukerch et al., 2007).

There are two main trust parameters: trust qualification and trust computation (Pirzada & McDonald, 2004; Ali et al., 2018). Trust qualification defines the numerous levels of trust, while trust calculation describes the means of measuring the trust value between nodes. It is also important to note that Trust and Reputation Management (TRM) is a system which defines the different steps that manage trust. The basic phases in TRM are to collect the facts, update the trust values and activate the creation of choices. The approach adopted in this research paper is twofold: a survey, and diverse proposals on trust and reputation.

4.1. Brief Survey of Trust and Reputation vital

WSNs have the vital property of being distributed in nature. This is evident in Sorniotti et al.'s (2007) survey. Data processing within a network in a distributed manner makes the communication and data sync considerably simpler. For group detection and self-diagnosis methods, a Sensor Node Failure Recognition (SNFR) scheme was introduced. Ganeriwal et al. (2008) discuss the reputation systems which help to create trust among sensor nodes through the integrated approach of different domains, including economics, data analysis and cryptography. They also discuss the use of Bayesian & beta distribution probability, cryptographic material and public key authentication trust-based frameworks for non-critical sensor networks. Various WSN issues and standards are discussed by Yick et al. (2008). In addition to this, localization, the coverage area of sensors, security and synchronization are some important issues also discussed. An extensive literature on trust and reputation systems is provided by Srinivasan et al. (2009) and Reshmi and Sajitha (2014). Lopez et al., (2010) focused on a WSN trust management system survey, while Khalid et al. (2013) applied the concepts of trust and reputation seen in human behavior in daily life into the WSN field for the purpose of node interactions.

A survey presented by Han et al. (2014) discusses the detection of unusual nodal behavior by focusing on the nature and applications of WSN trust models. Srivastava and Johri (2012) and Reshmi and Sajitha (2014) conducted surveys on WSNs, which are of great importance in the field and highly considered. Both surveys present an expanded overview of indirect and direct methods to measure trust in various trust management structures. Based on the surveys, it is evident that both the notions of Quality of Service (QoS) and social trust parameters are vital for trust.

4.2. Trust and Reputation Management

Managing the trust of the nodes and modules in a WSN is a process known as Trust and Reputation Management (TRM). Pirzada and McDonald (2004) recommended a trust model composed of trust deviation, qualification, functions and computation. Momani et al., Jsang and Isamil (Momani et al., 2007a; Momani et al., 2007b; Jsang & Ismail, 2002) used the Beta Reputation System (BRS) concept to enhance the trust level in the e-commerce environment.

Momani et al., (2007a) further enhanced their work on trust and reputation management by adopting the recursive Bayesian approach. This research was further investigated by Momani and Challa (2008), who found that a mischievous node may still be considered trusted if it behaves normally during communication. This leads to the introduction of data trust and communication trust to avoid any false data injection into the system. Later, in another study (Momani et al., 2008) compare their work with other models to draw a comparative conclusion.

Chen et al. (2007a) believe that employing tools from different domains such as probability, statistics and mathematical analysis in the trust management framework enhances the security implemented in WSNs. Following their research, they discuss the issue that sensor node trust and reputation is based on an amount of certainty in the values of that particular node. On the other hand, Fernandez-Gago et al. (2007) stress that WSNs in Ad-hoc and P2P lack proper trust management solutions.

To provide faster trust evaluation of clustered WSNs of a grouping nature, a lightweight group for trust computation based on a trust management scheme was proposed by Shaikh et al. (2009). To overcome the problem of using high end resources in implementing a group trust management scheme, an agent based trust calculation scheme was introduced by Reddy and Selmic (2011).

An approach to simplifying the comparison between trust and reputation management systems by building a simulator was introduced by Mármol and Pérez (2009). A particularly scalable cluster-based ordering trust management procedure was also introduced by Bao et al. (2011a; 2011b; 2012) after examining a wide range of trust and reputation management systems.

4.3. Frameworks and Trust Models

Numerous investigators have developed several models based on statistical methods, logical methods, nature inspired methods, fuzzy logic, etc. and various orientations such as individual and clustered distributed to present trust models and frameworks.

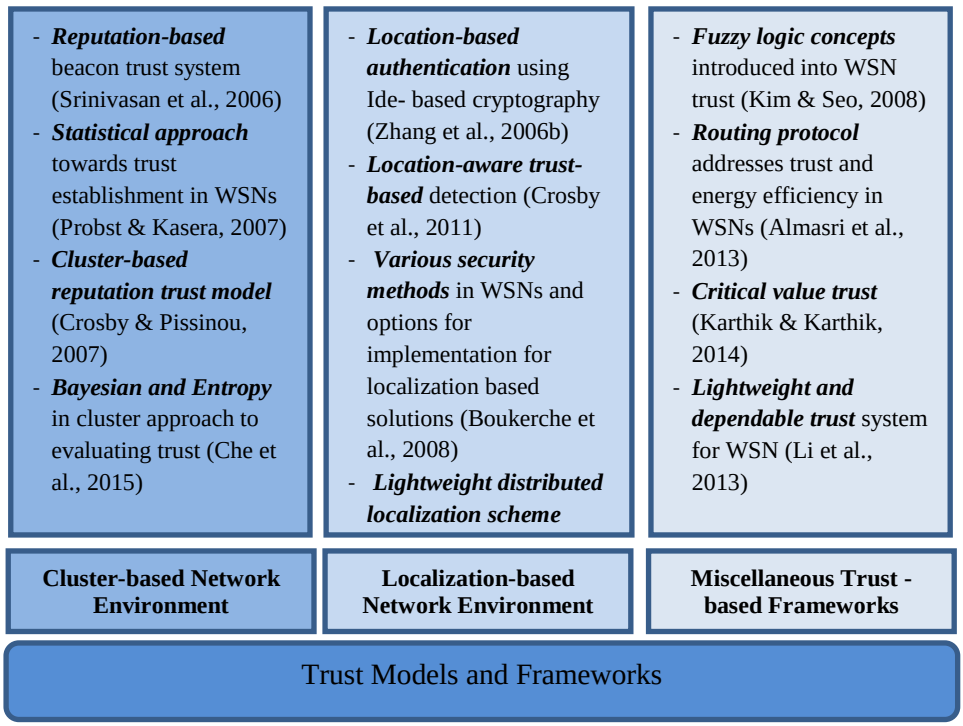

Figure 2 Trust models and frameworks overview

A cluster head in a cluster network is selected from the group, which is responsible for communication between the cluster and the base station. The Distributed Reputation-based Beacon Trust System (DRBTS) was proposed and recommended by Srinivasan et al. (2006), while Probst and Kasera (2007) study the trust establishment of WSNs by the application of statistical approaches. The direct and the indirect skills of the nodes are used to assess the confidence interval. Crosby and Pissinou proposed the Cluster-based Reputation and Trust model in (Crosby & Pissinou, 2007). The proposed model supports nodes with a good reputation which build their trust values over time, but disregards those which do not do this. This work was further developed by Shaikh et al. (2009).

Location-based authentication for WSNs using ID-based Cryptography (IBC) was introduced by Zhang et al. (2006), while several localization-based WSN security protocols are considered for application by Boukerche et al. (2008). Crosby et al. (2011) proposed a another location-aware trust-based detection model, which is an extension of their previous work in (Crosby & Pissinou, 2007). The research by Miao et al. (2015) proposes a distributed localization scheme that is lightweight; a localization method of three-step approach is proposed and implemented.

Kim and Seo introduced the fuzzy logic concept into WSN trust in 2008 (Kim & Seo, 2008). In addition, Zhan et al. (2009) introduced the Sensor Trust model to mitigate the problems associated with data integrity for the purpose of hierarchical WSN. Almasri et al.'s (2013) study focused on addressing the question of energy efficiency and proposed a routing protocol which is responsible for WSN trust and energy efficiency, called the Trusted and Energy Efficient Routing Protocol (TERP). Enhancement of the reliability of WSNs based on the critical value of the trust was demonstrated by (Karthik & Karthik, 2014).

The Lightweight and Dependable Trust System (LDTS) for WSNs was proposed by Li et al. (2013). In this model, energy efficiency is increased by removing the feedback of the cluster head. Wang et al. (2014) made the computations modest to reduce the energy consumption of WSNs. Later, a Lightweight Trust Model (LTM) was introduced by Singh et al. (2015), which has a dynamic trust building mechanism. Che et al. (2015) combined Bayesian and Entropy in their cluster approach to evaluating trust.

5. FINDINGS AND DISCUSSION

Based on the above literature overview and discussion, it is evident that the two main issues considered as key challenges to WSNs are security and reliability. According to Anand et al. (2006), the main tasks in securing WSNs comprise environment complications, topology complications, protected collections, privacy and trust management (Anand et al., 2006). Reliability concerns are associated with sensing/detection, transmission of data, event occurrence and data packets (Willig & Karl, 2005; Hsu et al., 2007; Mahmood et al., 2015). This paper has highlighted the importance of trust and reputation and the features related to them in order to better address security vulnerabilities. The areas that will be addressed by trust and reputation to benefit the overall aim of improving the security and reliability of WSNs are summarized in Table 1.

Table 1 Challenges and open research issues associated with WSN

Research domain	Known open research issues	Description
Security	Topology problems	If targeted nodes are attacked by an attacker then its apparent policy is to compromise both sensors and their keys, which logically reside in high value locations in the routing tree.
	Environment	Classification of cost-effective schemes in order to hide sensor network time; transport messages with periodic breaks; split and add random delay to messages broadcast; forged communication to deceive authentic send times.
	Assessing privacy	Different models and metrics for protocol logical level evidence, privacy and security attributes.
	Threatened cryptographic approaches	Employment of diverse cryptographic approaches for aggregation of messages.
	Ad-hoc network topology	Ad-hoc network topology is vulnerable to cyber-attacks by simplifying different types of link outbreaks, ranging from passive interfering to active snooping.
	Wireless media	Security systems for wired networks are not appropriate for WSNs due to wireless characteristics. The cost of implementing wireless media is also considered as a challenge.
Reliability	Package reliability	Transfer of data from resource-controlled sensor nodes to the sink in an efficient and reliable manner.
	Event reliability	Both in hop-by-hop and end-to-end mode of delivery of packets, receiving node held accountable for reliable transmission of information to the following node or to the destination.
	Link reliability	End-to-end packet loss ratio can be largely reduced through link reliability mechanisms. Some applications, such as intrusion detection applications, surveillance or applications used in battlefields or healthcare, require complete end-to-end reliability.
Trust and reputation	Trust models	Models that support nodes with a good reputation value to gain access to the WSN and disregard those which do not have it. By doing so, unreliable nodes can be avoided from entering the network, thereby enhancing its overall security.
	Risk assessment	Models that base their decisions on the risk of giving access to both cyber and physical realms. The risk assessment methodology consists of risk analysis and risk mitigation, which is more of a proactive approach towards managing security (Govindarasu et al., 2012).
Other challenges	Energy consumption, complexity and data reliability	There are numerous challenges associated with WSNs, mostly associated with the efficient use of energy resources, the complexities involved and data reliability, including data segregation, synchronization and classification.

One of the major security challenges to WSNs is associated with the nature of their error prone wireless links, reliable data transfer from resources to sensor nodes to the unreliable data transfer. These issues can be addressed by utilizing trust and reputation and combining them with an assessment of risk management to improve the resilience of WSNs. Researchers such as Mahmood et al. (2015) have highlighted the importance of trust in WSNs and have classified it into different stages at which it can be utilized. For example, they propose that trust can be applied in packets, at the event dependability level, or by hop-by-hop reliability. In hop-by-hop, the following hop is accountable for ensuring the reliable transmission of information to the destination, whereas in the scenario of end-to-end reliability, it is only the source and destination nodes of the end points which are responsible (Mahmood et al., 2015). However:

a) Trust as a measure can further be utilized to not only ensure reliability in transmission, but also to regulate the joining of nodes to the wireless sensor network. This will ensure an

additional tier in the process of improving security in WSNs and improve their resilience against malicious nodes.

b) Apart from utilizing trust, risk assessment can also be used as a complement to further enhance the security of WSNs. Risk management would enable one to ascertain beforehand the risk to the security of the WSN when it allow a node to join the network. This measure can then be used to assign access level tasks to nodes depending on their level of reliability. This will ensure that critical tasks are handled or assigned only to those nodes which have levels of risk below and of trust above a certain threshold.

Utilizing trust and risk also introduces the challenge of achieving reliable harmonization of measurements, minimization of human intervention in the network, and reliable delivery of a substantial number of measurements (Cinque et al., 2006).

6. CONCLUSION

In the paper, the authors have presented a review of WSN security concerns, with special attention paid to trust and reputation. The research was carried out by making a systematic literature review, which is the most suitable method of conducting a review. Issues related to the type of attacks, the features and vulnerabilities of attacks have been discussed. The notions of trust and reputation in WSNs have been debated and analysed. On the basis of the survey, the study concludes that security and reliability are the two main challenges faced by WSNs. Some shortcomings, challenges and open research issues associated with WSNs are also scrutinised. The paper provides an understanding of trust and reputation in WSNs. In the future, the authors plan to develop a secure, effective and efficient WSN mechanism.

7. ACKNOWLEDGEMENT

The research that produced these findings received Project Funding from The Research Council of the Sultanate of Oman, under Research Agreement No [ORG/SQU/ICT/13/011]. The authors would like to acknowledge and sincerely thank the research council and Sultan Qaboos University for all their managerial, administrative and financial support.

8. REFERENCES

Ali, S., Al Balushi, T., Nadir, Z., Hussain, O.K., 2018. *Cyber Security for Cyber Physical Systems.* Springer International Publishing, USA

Ali, S., Anwar, R.W., Hussain, O.K., 2015. Cyber Security for Cyber-physical Systems: A Trust Based Approach. *Journal of Theoretical and Applied Information Technology*, Volume 71(2), pp. 144–152

Almasri, M., Elleithy, K., Bushang, A., Alshinina, R., 2013. TERP: A Trusted and Energy Efficient Routing Protocol for Wireless Sensor Networks (WSNs). *In:* Proceedings of the 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications, pp. 207–214

Anand, M., Cronin, E., Sherr, M., Blaze, M., Ives, Z., Lee, I., 2006. Security Challenges in Next Generation Cyber Physical Systems. *In:* Beyond SCADA: Networked Embedded Control for Cyber Physical Systems. Pittsburgh, Pennsylvania, USA

Araujo, A., Blesa, J., Romero, E., Villanueva, D., 2012. Security in Cognitive Wireless Sensor Networks. Challenges and Open Problems. *EURASIP Journal of Wireless Communication and Networking*, Volume 2012(48), pp. 1- 8

Bao, F., Chen, I.-R., Chang, M., Cho, J.-H., 2011a. Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-based Routing. *In:* Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1732–1738

Bao, F., Chen, I.-R., Chang, M., Cho, J.-H., 2011b. Trust-based Intrusion Detection in Wireless Sensor Networks. *In:* 2011 IEEE International Conference on Communications (ICC), pp. 1–6

Bao, F., Chen, I.-R., Chang, M., Cho, J.-H., 2012. Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-based Routing and Intrusion Detection. *IEEE Transactions on Network and Service Management*, Volume 9, pp. 169–183

Boukerch, A., Xu, L., El-Khatib, K., 2007. Trust-based Security for Wireless Ad Hoc and Sensor Networks. *Computer Communications*, Volume 30(11–12), pp. 2413–2427

Boukerche, A., Oliveira, H., Nakamura, E.F., Loureiro, A.A., 2008. Secure Localization Algorithms for Wireless Sensor Networks. *In:* IEEE *Communications Magazine*, Volume 46(4), pp. 96–101

Byers, J., Nasser, G., 2000. Utility-based Decision-making in Wireless Sensor Networks. *In:* 2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC, pp. 143–144

Che, S., Feng, R., Liang, X., Wang, X., 2015. A Lightweight Trust Management based on Bayesian and Entropy for Wireless Sensor Networks. *Security and Communication Networks*, Volume 8(2), pp. 168–175

Chen, H., Gu, G., Wu, H., Gao, C., 2007a. Reputation and Trust Mathematical Approach for Wireless Sensor Networks. *International Journal of Multimedia and Ubiquitous Engineering*, Volume 2(4), pp. 23–32

Chen, H., Wu, H., Zhou, X., Gao, C., 2007b. Reputation-based Trust in Wireless Sensor Networks. *In:* 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp. 603–607

Cinque, M., Cotroneo, D., De Caro, G., Pelella, M., 2006. Reliability Requirements of Wireless Sensor Networks for Dynamic Structural Monitoring. *In:* Proceedings of International Workshop on Applied Software Reliability (WASR 2006), pp. 8–13

Crosby, G.V., Hester, L., Pissinou, N., 2011. Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks. *International Journal of Network Security*, Volume 12(2), pp. 107–117

Crosby, G.V., Pissinou, N., 2007. Cluster-based Reputation and Trust for Wireless Sensor Networks. *In:* 2007 4th IEEE Consumer Communications and Networking Conference, pp. 604–608

Egan, D., 2005. The Emergence of ZigBee in Building Automation and Industrial Controls. *Computing and Control Engineering Journal*, Volume 16(2), pp. 14–19

Estrin, D., Govindan, R., Heidemann, J., Kumar, S., 1999. Next Century Challenges: Scalable Coordination in Sensor Networks. *In:* Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking ACM, pp. 263–270

Fernandez-Gago, M.C., Roman, R., Lopez, J., 2007. A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks. *In:* Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, (SECPerU 2007), pp. 25–30

Ganeriwal, S., Balzano, L.K., Srivastava, M.B., 2008. Reputation-based Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks (TOSN)*, Volume 4(3), pp. 15

Govindarasu, M., Hann, A., Sauer, P., 2012. Cyber-physical Systems Security for Smart Grid. *In:* Future Grid Initiative White Paper, PSERC

Han, G., Jiang, J., Shu, L., Niu, J., Chao, H.-C., 2014. Management and Applications of Trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*, Volume 80(3), pp. 602–617

Hsu, M.-T., Lin, F. Y.-S., Chang, Y.-S., Juang, T.-Y., 2007. The Reliability of Detection in Wireless Sensor Networks: Modeling and Analyzing. *In:* Embedded and Ubiquitous Computing. Springer, pp. 432–443

Jsang, A., Ismail, R., 2002. The Beta Reputation System. *In:* Proceedings of the 15th Bled Electronic Commerce Conference, pp. 41–55

Karthik, N., Karthik, J. 2014. Trust Worthy Framework for Wireless Sensor Networks. *International Journal of Computer Science & Engineering Technology (IJCSET)*, Volume 5(5), pp. 478–480

Khalid, O., Khan, S.U., Madani, S.A., Hayat, K., Khan, M.I., Min-Allah, N., Kolodziej, J., Wang, L., Zeadally, S., Chen, D., 2013. Comparative Study of Trust and Reputation Systems for Wireless Sensor Networks. *Security and Communication Networks*, Volume 6(6), pp. 669–688

Kim, T.K., Seo, H.S., 2008. A Trust Model using Fuzzy Logic in Wireless Sensor Network. *International Journal of Electronics and Communication Engineering*, Volume 2(6), pp.1051–1054

Kinney, P., 2003. Zigbee Technology: Wireless Control that Simply Works. *In:* Communications Design Conference, pp. 1–20

Kitchenham, B., 2004. *Procedures for Performing Systematic Reviews*. Keele University, UK

Kitchenham, B., Charters, S., 2007. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Version 2.3, Technical Report. Keele University and University of Durham, UK

Lasol, W., Pornpromlikit, S., 2016. Broadcast-based Skew Correction Technique for Wireless Sensor Networks. International Journal of Technology, Volume 7(7), pp. 1232–1238

Lee, K., 2000. IEEE 1451: A Standard in Support of Smart Transducer Networking. *In:* Proceedings of the 17th Instrumentation and Measurement Technology Conference, pp. 525–528

Lewis, F.L., 2004. Wireless Sensor Networks. *Smart Environments: Technologies, Protocols, and Applications*, pp. 11–46

Li, X., Zhou, F., Du, J., 2013. LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks. *In:* IEEE Transactions on Information Forensics and Security, Volume 8(6), pp. 924–935

Li, Z., Gong, G., 2008. Survey on Security in Wireless Sensor. *Special English Edition of Journal of KIISC*, Volume 18, pp. 233–248

Lopez, J., Roman, R., Agudo, I., Fernandez-Gago, C., 2010. Trust Management Systems for Wireless Sensor Networks: Best Practices. *Computer Communications*, Volume 33(9), pp. 1086–1093

Lopez, J., Roman, R., Alcaraz, C., 2009. Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks. *In:* Foundations of Security Analysis and Design V., Springer, pp. 289–338

López, J., Zhou, J., 2008. *Wireless Sensor Network Security*, Ios Press, Netherlands

Mahmood, M.A., Seah, W.K., Welch, I., 2015. Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead. Computer Networks, Elsevier, Volume 79, pp. 166–187

Mármol, F.G., Pérez, G.M., 2009. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. *In:* IEEE International Conference on Communications, pp. 1–5

Miao, C.-Y., Dai, G.-Y., Chen, Q.-Z., 2015. Cooperative Localization and Location Verification in WSN. *In:* Human Centered Computing. Springer, pp. 139–205

Momani, M., Aboura, K., Challa, S., 2007a. RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks. *In:* 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information

Momani, M., Challa, S., 2008. GTRSSN: Gaussian Trust and Reputation System for Sensor Networks. *Advances in Computer and Information Sciences and Engineering*, pp. 343–347

Momani, M., Challa, S., Aboura, K., 2007b. Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective. *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, pp. 317–321

Momani, M., Challa, S., Alhmouz, R., 2008. Can We Trust Trusted Nodes in Wireless Sensor Networks? *In:* 2008 International Conference on Computer and Communication Engineering, pp. 1227–1232

Pa, N.C., Anthony, B.J., Nor, R.N.H., Murad, M.A.A., 2015. Risk Assessment of IT Governance: a Systematic Literature Review. *Journal of Theoretical and Applied Information Technology*, Volume 71(2), pp. 184–193

Pirzada, A.A., Mcdonald, C., 2004. Establishing Trust in Pure Ad-hoc Networks. *In:* Proceedings of the 27th Australasian Conference on Computer Science, Volume 26, pp. 47–54

Portocarrero, J.M., Delicato, F.C., Pires, P.F., Gámez, N., Fuentes, L., Ludovino, D., Ferreira, P., 2014. Autonomic Wireless Sensor Networks: A Systematic Literature Review. *Journal of Sensors*, Volume 2014, pp. 1- 13

Probst, M.J., Kasera, S.K., 2007. Statistical Trust Establishment in Wireless Sensor Networks. *In:* 2007 International Conference on Parallel and Distributed Systems, pp. 1–8

Reddy, Y., Selmic, R., 2011. Agent-based Trust Calculation in Wireless Sensor Networks. *In:* SENSORCOMM 2011, the Fifth International Conference on Sensor Technologies and Applications, pp. 334–339

Reshmi, V., Sajitha, M., 2014. A Survey on Trust Management in Wireless Sensor Networks. *International Journal of Computer Science & Engineering Technology*, Volume 5(2), pp. 104–109

Sarma, H.K.D., Kar, A., 2006. Security Threats in Wireless Sensor Networks. *In:* Proceedings 2006 40th Annual IEEE International Carnahan Conferences Security Technology, pp. 243–251

Sarobin M., V.R., Ganesan, R. 2016. Bio-inspired, Cluster-based Deterministic Node Deployment in Wireless Sensor Networks. International Journal of Technology. Volume 7(4), pp. 673–682.

Shaikh, R.A., Jameel, H., D'auriol, B.J., Lee, H., Lee, S., Song, Y.-J., 2009. Group-based Trust Management Scheme for Clustered Wireless Sensor Networks. *In:* IEEE Transactions on Parallel and Distributed Systems, Volume 20(11), pp. 1698–1712

Singh, M., Sardar, A.R., Sahoo, R.R., Majumder, K., Ray, S., Sarkar, S.K., 2014. Lightweight Trust Model for Clustered WSN. *In:* Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, 2015. Springer, pp. 765–773

Sorniotti, A., Gomez, L., Wrona, K., Odorico, L., 2007. Secure and Trusted In-network Data Processing in Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security*, Volume 2, pp. 189–199

Srinivasan, A., Teitelbaum, J., Wu, J., 2006. DRBTS: Distributed Reputation-based Beacon Trust System. *In:* 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 277–283

Srinivasan, A., Teitelbaum, J., Wu, J., Cardei, M., Liang, H., 2009. Reputation-and-Trust-based Systems for Ad Hoc Networks. *Algorithms and Protocols for Wireless and Mobile Ad hoc Networks*, Volume 375, pp. 375-404

Srivastava, S., Johri, K., 2012. A Survey on Reputation and Trust Management in Wireless Sensor Network. *International Journal of Scientific Research Engineering & Technology*, Volume 1(3), pp. 139–149

Undercoffer, J., Avancha, S., Joshi, A., Pinkston, J., 2002. Security for Sensor Networks. *In:* CADIP Research Symposium, pp. 25–26

Wang, N., Gao, L., Wu, C., 2014. A Light-Weighted Data Trust Model in WSN. *International Journal of Grid & Distributed Computing*, Volume 7(2), pp. 33–40

Willig, A., Karl, H., 2005. Data Transport Reliability in Wireless Sensor Networks. A Survey of Issues and Solutions. *Praxis der Informationsverarbeitung und Kommunikation*, Volume 28(2), pp. 86–92

Yang, S.-H., 2014. *Wireless Sensor Networks*, Springer

Yang, S.-H., Cao, Y., 2008. Networked Control Systems and Wireless Sensor Networks: Theories and Applications. *Journal International Journal of Systems Science*, Volume 39(11), pp. 1041–1044

Yick, J., Mukherjee, B., Ghosal, D., 2008. Wireless Sensor Network Survey. *Computer Networks*, Volume 52(12), pp. 2292–2330

Yu, H., Shen, Z., Miao, C., Leung, C., Niyato, D., 2010. A Survey of Trust and Reputation Management Systems in Wireless Communications. *In:* Proceedings of the IEEE, Volume 98(10), pp. 1755–1772

Yu, Y., Li, K., Zhou, W., Li, P., 2012. Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. *Journal of Network and Computer Applications*, Volume 35(3), pp. 867–880

Zhan, G., Shi, W., Deng, J., 2009. Sensor Trust: A Resilient Trust Model for WSNs. *In:* Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, pp. 411–412

Zhang, Y., Liu, W., Fang, Y., Wu, D., 2006. Secure Localization and Authentication in Ultra-Wideband Sensor Networks. *In:* IEEE Journal on Selected Areas in Communications, Volume 24(4), pp. 829–835

Zia, T., Zomaya, A., 2006. Security Issues in Wireless Sensor Networks. *In:* 2006 International Conference on Systems and Networks Communications (ICSNC'06)