Systematic literature review on designing trust-based security for WSNs

Raja Waseem Anwar[1], Anazida Zainal[2], Saleem Iqbal[3]
[1,2]Department of Communication, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
[3]Department of Computer Science, ARID Agriculture University, Pakistan

Article Info

Article history:

Received Oct 15, 2018
Revised Nov 17, 2018
Accepted Dec 31, 2019

Keywords:

Design
Networks
Security
Trust
Wireless

ABSTRACT

The study assessed the design and development of trust-based security for wireless sensor networks. A qualitative approach was opted by employing systematic review analysis, which was assessed using secondary data collection. The design and development of trust-based security were mainly targeted, and 140 publications were randomly reviewed, from which 24 studies were finalized after excluding irrelevant data and studies that only contained abstracts. The results were analyzed focusing on the designs, applications and protocols and trust factors. Different studies have been evaluated, which have suggested that proper design and development of trust-based security should be the foremost aim to be applied in user environments. The study suggested that designing the trust management models based on the taxonomy of routing applications and relevant algorithms could be a part of future investigations.

Corresponding Author:

Raja Waseem Anwar,
Department of Communication,
Faculty of Computing,
Universiti Teknologi Malaysia,
Skudai, 8130, Johor Darul Takzim, Malaysia.
Email: rajawaseem@gmail.com

1. INTRODUCTION

Wireless Sensor Network (WSN) possesses various potential applications, which include emergency response, battlefield surveillance, accident detection, and healthcare monitoring. These networks are susceptible to many security threats; however, recently, a trust management model has been suggested as an effective security mechanism for WSNs [1], [2]. Within an unattended and hostile environment, WSNs are often deployed. The sensor network formulates an ideal medium for attackers to perform vicious tasks through a wireless and resource-constrained nature. Therefore, the acceptance and deployment of WSN require adequate security. However, achieving an acceptable level of security for WSN is difficult owing to limited resources and bandwidth. Different safety mechanisms, including confidentiality, authentication, and message integrity have been proposed for incorporation in WSNs. Although these mechanisms are effective to outsider attacks, network insider attacks cannot be defended against. WSNs have proven to be a cost-effective solution for different domestic and war field applications. The networks possess sensor nodes that are known as autonomous sensing and communication units, which possess limited resource, energy, and processing [3-5].

WSNs are an emerging technology used to monitor and sense the environment. WSNs are regarded as an important issue because they are associated with mission-critical tasks. Security can be deliberated as one essential factor when the nodes are deployed in an open-access environment. The integrity, confidentiality, and authentication can be ensured by the cryptography techniques. However, WSN also requires controlling internal and external attackers. Trust management factors have been essential factors of the present study of WSNs. For security management, trust management systems can be applied in several different applications, including a selection of secure cluster heads, access control, data aggregation, and routing [6].

Different types of solutions have been provided by different researchers for the security-based applications concerned with trust management. Granting, all the relevant information is essential to be incorporated in a single node of the network for designing and developing a trust management system. The design must consider different applications and aspects of the WSN. As a consequence, a study by [7] emphasized proposing a trust factor and parameter-based framework and design of secure communication for WSN. The main contribution of the study was to recognize several parameters that influence trust in WSNs.

Many routing techniques of the sensor networks require location knowledge, which is offered effectively by the location finding system. Sometimes, a mobilizer may be required to move the sensor node; this depends on the application [6]. Although much research has been done on trust-based wireless sensor networks [8, 9], there is still a need to develop and design an easy and approachable trust management system that uses fewer resources of nodes in the management and evolution of trust among or between nodes. The trust management of WSNs must be kept as simple as possible.

This study was aimed at examining and comprehending the design and development process of the trust-based security for wireless security networks. The systematic review approach has been focused on assessing the importance of the design and development of the study. The security issues in WSN remain a challenge for researchers. The cross-layer encryption techniques and traditional cryptography techniques can mitigate insider attacks but are not suitable for all situations. The implementation of security systems in WSN has become cumbersome in understanding the lack of unity in the design of existing schemes [10]. The system specifications can be implemented effectively by presenting a systemic design of security management.

Trust management systems for wireless sensor networks can be very helpful for detecting interfering nodes and for assisting with the decision-making criteria. Particularly for WSN, lack of trust management studies has been observed [3, 11]. Most of the work in this area has been emphasized in recent years [12-14] with some relevant approaches adopted to imitate the peer-to-peer P2P and ad hoc networks for WSN. Although, this cannot be possible because of the differences in the network's features [15].

In recent years, WSN has gained much attention in facilitating the development of smart sensors. Drastic improvements have been observed in the healthcare industry because of the involvement of WSNs. As compared to traditional sensors, these sensors are inexpensive, small, and possess limited processing resources [16, 17]. Many types of wireless sensor applications have been designed and developed based on current state-of-the-art sensor technology. A study conducted by Lopez et al. [18] considers WSNs as living beings who are born in a controlled environment. The nodes tend to work selflessly to achieve a common goal. The inherent security problems hinder the emerging importance of sensor networks.

The paper is organized in such a way that Section 2 discusses the method applied to conduct the study. Section 3 descibes the process of systematic literature review while results and discussions are provided in Section 4 and finally Section 5 concludes the study and provies the future direction.

2. RESEARCH METHODOLOGY

In this study, we conducted a SLR for designing trust-based security for WSNs.The study cosists of research design, procedure, search strategy, data collection, research questions and selction process or relevant studies.

2.1. Research Design

Qualitative research design includes a systematic approach that has been used to evaluate the design and development of trust-based security for WSNs. To execute the evaluation of a trust-based wireless sensor network, secondary data collection has been used. The nature of the topic permits implementing a systematic review analysis for understanding the development and design of trust-based WSN.

2.2. Research Procedure

The main aim of the systemic review analysis is to reduce the potential bias of the researcher and permit future replication of the review. A trial search has also been performed to verify the quality of the search string. The presentation of empirical data has been considered as the main criterion for inclusion of the primary data. The systematic review assisted in evaluating the procedures and objectives of secondary data for comprehending the design and development of WSNs considering trust in a broader perception. The systematic review analysis has been observed as effective in evaluating the secure application-based security management process, frameworks for the trust management systems, and different factors of trust that may impact WSNs.

2.3. Search Strategy

The keywords were derived for searching the relevant data from the research questions (Table 1). The terms representing the interventions and populations were composed by the search string. The following search terms: ("Wireless Sensor Network" OR "Wireless Network" OR "Design of Wireless Network") AND ("Design" OR "Trust" OR "Security") were used to carried out to collect data. Associated publications were manually searched relevant to the design and development of trust-based security for WSNs and compared with each other. Figure 1 shows a flow chart of search strategy.

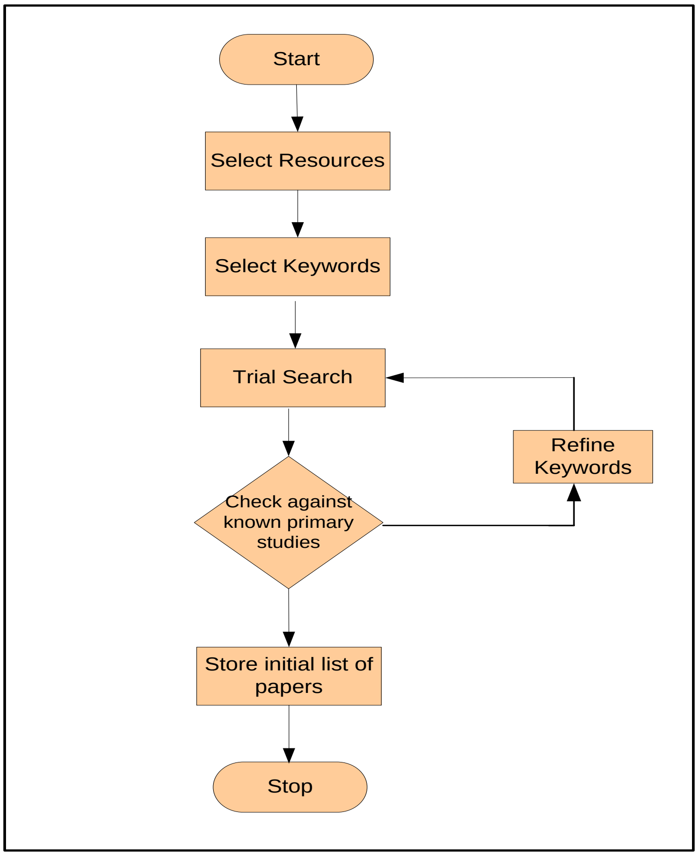

Figure 1. Search strategy

2.4. Data Collection

The results of the study are based on designing and developing trust-based security for a WSN. Therefore, the data has been collected relevant to the proposed nature of the study. A well-planned security mechanism needs to be designed for the successful deployment of wireless applications. The study presented the challenges faced in implementing a secure wireless sensor network through systematic analysis and comparing secondary research, which reflect the fact that technology is safe. It would not be impractical to use WSN technology. Figure 2 shows a databases that were used to search for relevant data.

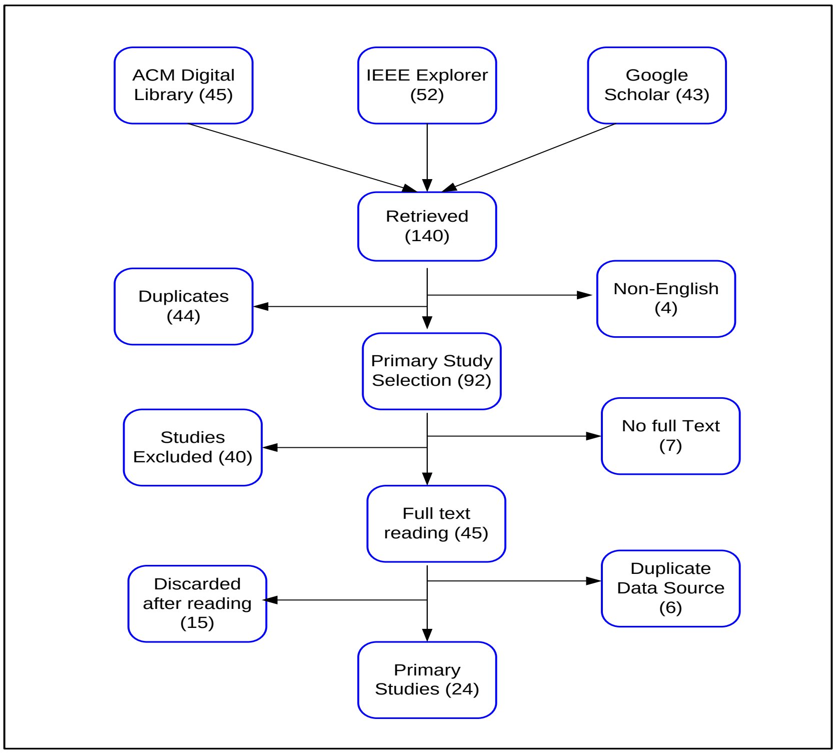

Figure 2. Selection of studies from databases

2.5. Research Questions

Table1, represents the research questions which were identified in the designing of trust-based security for WSNs.

Table 1. Research Question (RQ'S) Along with The Objectives

Research Question	Focus
RQ1: What types of designs have been used for trust-based security for WSN?	The designs have focused on using wireless networks and the issues present in the existing applications of WSNs.
RQ2: Where the trust management system can be implemented for security management purposes?	As an open environment is used to deploy the nodes, security is one factor that is essential.
RQ3: What are the secure routing processes in WSNs?	The protocols for the trust evaluation for secure routing in WSNs have been focused.
RQ4: What are the security-related problems and what is the importance of trust-based security in WSNs?	Different parameters and trust factors have been emphasized presenting the importance of trust in WSNs.

2.6. Study Selection Process

The systematic review process was executed in a manner that has been illustrated in Figure 2. The study has considered articles/studies that have been published in 2005-2017. Initially, 45, 52, and 43 studies were analyzed from ACM Digital Libraries, IEEE explorer, and Google Scholar, out of which 140 publications were randomly retrieved from the field of advanced technology of wireless sensor networks (WSNs). All the studies were reviewed based on literature and study outcomes to be included in the systematic analysis.

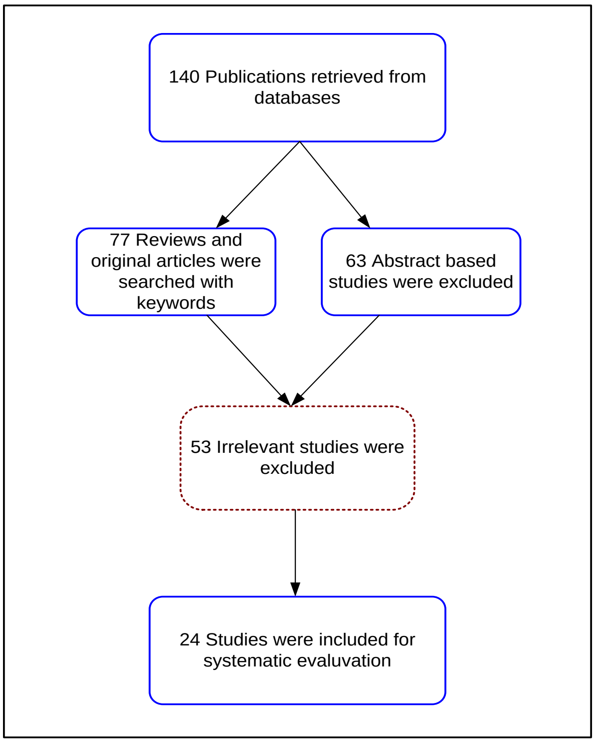
140 Publications retrieved from databases
77 Reviews and original articles were searched with keywords
63 Abstract based studies were excluded
53 Irrelevant studies were excluded
24 Studies were included for systematic evaluvation

Figure 3. Evaluvation process

2.7. Study Inclusion and Exclusion Criteria

The aim of this step is to narrow down the search and to find those articles which fulfils the criteria as per the research questions. The studies that were available with abstracts only were excluded from the randomly selected sample of 140 publications (Figure 3). Finally, 24 studies were recruited for the systematic review analysis as secondary data, based on which the outcomes have been analyzed and concluded.

3. SYSTEMATIC LITERATURE REVIEW (SLR)

This section describes the process of systematic literature review which is based on the research questions (RQ's). There are a significant number of aspects, which are directly associated with wireless sensor networks. During the development and design of wireless sensor networks, trust-based security is always identified as a foremost aspect to consider. Han et al. [3] have conducted a comprehensive study that has mentioned the development of wireless sensor networks by considering the trust factor. WSNs have been identified as an emerging technology that is needed for the purpose of battlefield, emergency response, healthcare, and surveillance. The development of the trust factor among individuals related to WSNs is extremely effective in enhancing the reliability of the entire system. Moreover, another study has mentioned that providing security to the WSNs is a major requirement for the deployment along with the acceptance of WSNs [19, 20]. Therefore, it can be said that the development and design of trust-based security for wireless sensor networks are extremely significant. Table 2, has reviewed different studies, which focused on different designs of wireless sensor networks.

3.1. Research Question 1 (RQ1)

The intention of this research question was to explore the types of designs used for trust-based security for WSN. The designs were characterized according to their features and 13 different types of designs (Table 2) were found. The most dominant design found was the trust-aware secure routing framework. The designs are explicitly discussed in the following section. For efficient collaboration and security improvement, trust and security are considered as the most important factors of a wireless sensor network. Trust management can make sure that all the nodes of communication are trustworthy during the authorization time and key management system. It can eventually enhance the traditional security systems efficiency and reliability.

Trust management factors can enhance the cooperation of the nodes, which is effective for the system’s performance and associated enhancement. Trust management and estimations can be highly challenging matters owing to the distinct features and exposure of wireless sensor networks to various attacks. Therefore, the aim of the study by Ishmanov et al. [21] was to gain the conceptual design framework of trust management in wireless sensor networks and, to achieve the targeted goal, the study opted trust management and computation schemes in wireless sensor networks.

Wireless sensor networks are vulnerable to various threats concerning security issues. Owing to computation, communication, and delayed restrictions of wireless networks the security mechanisms are useless. Trust management models have been recommended recently as an effective security mechanism, more particularly for wireless sensor networks [3]. Various applications have been evaluated regarding trust models which are categorized as: routing, malicious attacks, secure node selection, localization, and secure data aggregation. Additionally, different types of malicious attacks against the trust models and trust-based practices have been listed which are essential for the development of effective wireless sensor networks [3]. Considerable research has been conducted on managing and modeling the trust [22-25].

Wireless sensor networks have distinct categorization that includes a limited power supply and low bandwidth transmission with a small memory size and data storage and capacity. Because of the limited and restricted operating conditions of wireless sensor networks, many of the techniques devised the conventional wireless or wired networks, including the intrusion detection approach, which is directly pertinent to a wireless network environment. It is a very big challenge to design an efficient and effective intrusion detection technique [26]. Information extraction from the environment can be convenient through wireless sensor networks by using small nodes that are more effectively deployed in unattended and sensitive hostile territories. Further, the cryptographic technique is widely used to provide WSN security. However, owing to insecure and unattended deployment, the sensor node can be captured physically by an adversary that attains the underlying secrets or a subset to access the nodes and other critical data in the network; although, a node cannot work because of deficient resources on issues in the link of a particular network. Different reputation and trust models have been applied to monitor transforming the behavior of nodes to a WSN in a network. The study by Khalid et al. [22] explored the recent advancements of trust and reputation and included an accurate comparison of several trust and reputation factors. A comprehensive discussion was made concerning the challenges and the issues experienced in the implementation of most of the trust-based systems.

Wireless sensor networks have gained much attention towards the wireless research sector as these networks are intended and focused towards supporting a large number of practical applications that are effective to be implemented. The security design for WSN is significantly stimulating, mainly because of the salient features of the sensor networks. The lack of timeliness and comprehensiveness was observed by Zin et al. [24] regardless of a good number of existing surveys and literature the study reviewed the state-of-the-art wireless sensor network routing protocols that portray the challenges and issues in terms of design matters.

3.2. Research Question 2 (RQ2)

The intention of this research question was to explore the implementation and to secure the WSNs. There are various important and essential issues present in the traditional trust-aware routing systems. These include trust metric compatibility by QoS metrics along with the control of overhead produced by the procedures of trust evaluation. A study by Duan et al. [25] proposed a trust-aware secure routing system and its framework with the categorization of high ability and light weight to resist different attacks. The features of common attacks were first analyzed to meet the requirements of a secure routing system. Trust derivation and computation schemes were proposed based on the results and analysis. Ultimately, the designs used the contrast of QoS and trust metric to present the optimized routing algorithm within the system.

Noteworthy benefits have been provided by WSN over the conventional techniques for different applications, which include smart homes, environmental monitoring, health care, and security. Wireless sensor networks have been found integrated with internet protocols to develop the internet of things for the connection of daily routine objects. The Internet of Things has been proven as one of the most powerful and effective wireless models of the 21st century. Owing to this fact, the Internet of Things has become more helpful and valuable in several different domains, such as assisted living monitoring, health monitoring, and smart home automation systems. Therefore, there are several main challenges in the designs of WSN. The challenges may include the ways to effectively use small, low-powered nodes for the implementation of security during data transmission processing among various nodes. The challenges and issues may also include security issues concerned with the complex and harsh environmental situations during the data transmission. A secure Internet of Things based smart home automation system has been developed by Pirbhulal et al. [27]. A triangle based security algorithm has been used by the study based on effective key development mechanisms. The proposed algorithm was included in a wireless sensor network to provide secure data transmission. The developed system had an outstanding performance, consuming less energy in comparison with some other already developed models. The outcomes of the study have also shown that the algorithm proposed in the system consumed less energy and fulfilled all the necessary security requirements of the WSN (Table 2).

3.3. Research Question 3 (RQ3)

The study has found the dominance of major applications of wireless sensor networks. These applications include routing, data aggregation, intrusion detection, clustering, and collection tree applications (Table 3). Routing and data aggregation are the most dominant applications identified in the study. Wireless sensor networks are susceptible to security threats. Therefore, traditional security mechanisms cannot be used owing to computation, delay constraints, and communication of WSNs. As Han et al. [3] stated, trust management models are recommended mostly as an appropriate and effective security mechanism for WSNs. In addition, using routing protocols as applications generate great trust towards WSNs. Empirically, the effectiveness of several trust-based applications such as secure routing, secure localization, secure node selection, secure data aggregation, and malicious attack detection. Thereby, the study has recommended that these trust-based applications are important for establishing a strong trust model for WSNs.

Butun et al. [26] have exemplified intrusion detection systems along with their design specifications, requirements, and their classifications for showing the effectiveness of WSNs. The study discussed that specific distinctive aspects might be relevant to WSNs in the selection of intrusion detections. For WSNs, conventional cryptography methods are not appropriate specifically for secure routing [10]. The vulnerability of these networks has been caused owing to processing and storage, lack of supervision, restrictions in view of resource and diverse applications. Therefore, the implication of trust-based applications, such as secure routing, can be effectual for providing better security to assist in routing protocols.

According to [25], a dominant role has been played by the trust-aware routing protocol in securing wireless sensor networks. In contrast, the study has examined that conventional trust-aware routing protocols comprise of several key issues and are yet to be resolved. The predominant issues include the control of overhead and the compatibility of a trust metric with QoS metrics generated by trust evaluation procedure. Thereby, WSN-based networks can be accomplished by high efficiency and the intended security of a trust-aware secure routing framework (TSRF) with the assistance of simulations.

3.4. Research Question 4 (RQ4)

In WSNs, the trust model has emerged significantly for malicious node detection. Many applications are assisted by the trust model, including secure data aggregation, secure routing, and trusted key exchange. Jiang et al. [8] have signified the need for a distributed trust model regardless of any central node for monitoring each neighbor node owing to WSNs wireless aspects. The findings of the study have shown that the efficient distributed trust model (EDTM) is an attack-resistant and efficient trust model for defining a threshold and selecting the appropriate value of the weight.

The research community has recently characterized the importance of multimedia wireless sensor networks. Various different types of multimedia data have been potentially provided by these networks to a base station or an end-user. Owing to the existence of resource-starving sensor nodes at the base of their architecture, these networks emerge as resource constrained in spite of their potential to monitor trust-based applications extensively. Usman et al. [28] have signified that multimedia sensor nodes execute in hostile and remote environments and, therefore, are vulnerable to a wide range of malicious attacks. In contrast, there are potential chances that data coming from legitimate nodes cannot be properly ensured as it transmits delay-sensitive authenticated and highly-critical data to the base station.

Lu et al. [29] have stated that secure data transmission is a crucial and important concern for WSNs. However, the system performance of WSNs is enhanced using an effective and practical trust-based application: clustering. The study has further analyzed that the computational overhead for protocol security is reduced by SET-IBOOS. The efficiency of the intended protocols is illustrated from the feasibility of the SET-IBOOS and the SET-IBS. Therefore, the study has shown that the intended protocols have better performance compared to the current security protocols for cluster-based wireless sensor networks with respect to energy consumption and security overhead.

Several researchers have evidently revealed the importance of contemporary trends in developing new applications for data clustering. According to Kavitha and Pushpalatha [30], the instigation of a secure and advanced data clustering pattern is emerged for WSNs to secure data clustering. For sustaining security and ignoring data from malicious nodes in the network, the generation of keys and exchange of keys emerged from a modified Diffie Hellman key exchange algorithm. The performance of the specific algorithm emerged for residual energy, energy consumption, and network lifetime.

The provision of better routing paths has been specified from the survey of the collection tree applications that transmits the source packets from the destination. In this regards, Devisri and Balasubramaniam [7] presented that the trust-aware routing protocol is used for improving the performance of WSNs and selecting an appropriate route for transmitting products. The study has indicated that these types of networks are important to be monitored for assuring confidence between each pair of interacting nodes. The use of WSNs has dominantly emerged in maintaining tracking, controlling, environmental control, and surveillance tasks. It is a fact that the factor of security has relatively higher significance as compared to other factors [31-34]. Therefore, security factors are viable for wireless sensor networks to enhance the abilities of a system effectively.

4. RESULTS AND DISCUSSION

In this section, findings and results are discussed which are based on the predefined research questions. The frequencies of each design in the reviewed studies have also been mentioned in the Table 2.

Table 2. Design of Wireless Sensor Network

Name	Studies	Frequency
Trust-based Cross-Layer Model (TCLM)	[3], [31], [22]	3
Mobile Ad-Hoc Networks	[26]	1
Trust Management System Design	[3], [23], [22], [24]	4
Intrusion Detection Systems	[26]	1
Trust-aware secure routing framework	[22], [23], [24], [25]	4
Efficient Distributed Trust Model	[8], [22], [24]	3
Cluster-based hierarchical data authentication approach	[23], [28]	2
Identity-based digital signature	[29]	1
Diffie Hellman Key Exchange algorithm	[32]	1
Service-oriented architecture	[30]	1
Vector AutoRegression (VAR)	[9]	1
Trust-aware routing	[33]	1
Triangle-Based Security Algorithm (TBSA)	[27]	1

Figure 4 describes the frequencies of the designs used for WSNs graphically. It has been observed that trust-based secure framework e design that was mostly employed. The higher frequency shows the higher level of utilization of designs.

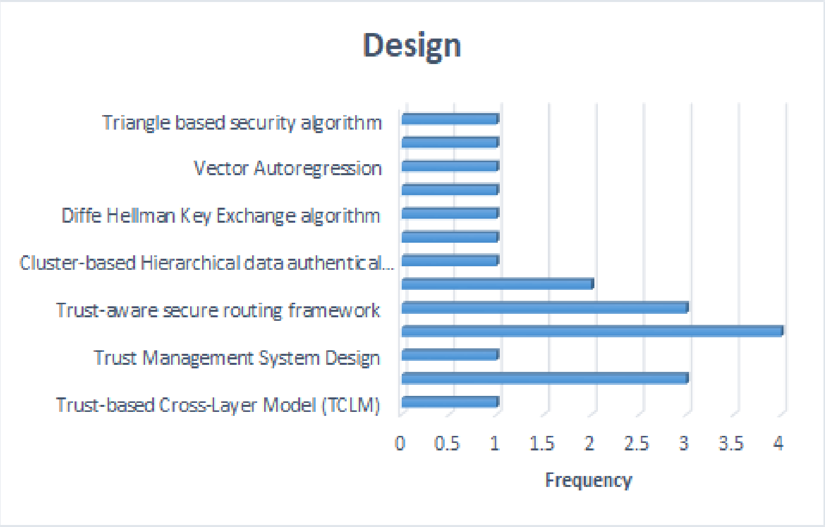

Figure 4. Design frequencies

The following Table 3, summraizes the the frequencies of the applications, where trust-related factors are employed. The highest frequency was observed regarding the trust-aware secure routing framework, which was found to be used in four studies. Similarly, Table 3, shows the frequencies of the applications that were adopted by the studies regarding wireless sensor networks. It has been observed that mostly the routing application has been used by 13 studies on WSNs. Secondly, a data aggregation application was used by 10 studies.

Table 3. Applications

Name	Studies	Frequency
Routing	[3], [4], [25], [8], [28], [32], [30], [31], [23], [22], [33], [34], [27]	13
Data aggregation	[22], [3], [27], [28], [32], [30], [31], [23], [24], [32],	10
Intrusion detection	[23], [28], [3], [22], [33],	5
Clustering	[28], [22], [33], [3], [4], [33], [34]	7
Collection tree applications	[9], [27]	2

Figure 5 shows the frequencies of applications and protocols employed in the studies.

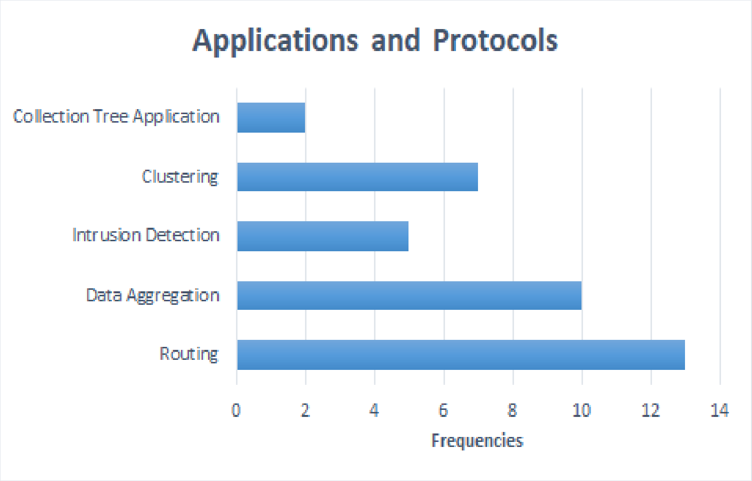

Figure 5. Frequencies of applications and protocols

It is observed that majority of the WSN applicactions prefer to implement trust-based secure routing as it shows the higher occurrence frequency. Data aggregation has been found as the second highest used preferred method by researchers for WSN.

5. CONCLUSION

This study has effectively contributed to portraying the security aspect of WSNs that should be addressed in terms of the previously recognized integration approaches and the communication technologies that assist in contributing to the field. The security mechanism has been reviewed to analyze the security mechanism and structured to secure and protect the communication system by using the technologies. It has been assumed that the survey conducted along with such aims and objectives may provide a significant contribution to readers in this important field. Hybrid and scalable security solutions are required in order to provide trustworthy and secure routing environment for WSNs.

REFERENCES

[1] Prabhu, B., N. Balakumar, and A. Antony, Wireless Sensor Network Based Smart Environment Applications. 2017.

[2] Anwar, R.W., et al., Security in Wireless sensor network: Approaches and Issues. Indonesian Journal of Electrical Engineering and Computer Science, 2015. 15(3): p. 584-590.

[3] Han, G., et al., Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 2014. 80(3): p. 602-617.

[4] Can, O. and O.K. Sahingoz. A survey of intrusion detection systems in wireless sensor networks. in Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on. 2015. IEEE.

[5] Yassine, S. and N. El Kamoun, Attacks and Secure Geographic Routing In Wireless Sensor Networks. Indonesian Journal of Electrical Engineering and Computer Science, 2017. 5(1): p. 147-158.

[6] Sujatha, V. and E.M. Anitha, Immensely Discriminate Routing in Wireless Networks. Indonesian Journal of Electrical Engineering and Computer Science, 2017. 8(3): p. 712-714.

[7] Devisri, S. and C. Balasubramaniam, Secure routing using trust based mechanism in wireless sensor networks (WSNs). International Journal of Scientific & Engineering Research, 2013. 4(2): p. 1-7.

[8] Jiang, J., et al., An efficient distributed trust model for wireless sensor networks. IEEE Transactions on Parallel & Distributed Systems, 2015(1): p. 1-1.

[9] Venkataraman, R., et al., Trust–based backpressure routing in wireless sensor networks. International Journal of Sensor Networks, 2015. 17(1): p. 27-39.

[10] Vamsi, P.R. and K. Kant. Systematic design of trust management systems for wireless sensor networks: A review. in Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on. 2014. IEEE.

[11] Chen, H., et al. Reputation-based trust in wireless sensor networks. in Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on. 2007. IEEE.

[12] Fang, W., et al., BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. Journal of Network and Computer Applications, 2016. 59: p. 88-94.

[13] Lee, Y.k., et al., A study of vulnerabilities of wireless sensor network. International Journal of Sensor Networks, 2014. 16(1): p. 23-31.

[14] Wang, J., S. Jiang, and A.O. Fapojuwo, A protocol layer trust-based intrusion detection scheme for wireless sensor networks. Sensors, 2017. 17(6): p. 1227.

[15] Román, R., et al., Trust and reputation systems for wireless sensor networks. Security and Privacy in Mobile and Wireless Networking, 2009: p. 105-128.

[16] Kumar, P. and H.-J. Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey. sensors, 2011. 12(1): p. 55-91.

[17] Yick, J., B. Mukherjee, and D. Ghosal, Wireless sensor network survey. Computer networks, 2008. 52(12): p. 2292-2330.

[18] Lopez, J., et al., Trust management systems for wireless sensor networks: Best practices. Computer Communications, 2010. 33(9): p. 1086-1093.

[19] Raje, R.A. and A.V. Sakhare. Routing in wireless sensor network using fuzzy based trust model. in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. 2014. IEEE.

[20] Virmani, D., M. Hemrajani, and S. Chandel, Exponential trust based mechanism to detect black hole attack in wireless sensor network. arXiv preprint arXiv:1401.2541, 2014.

[21] Ishmanov, F., et al., Trust management system in wireless sensor networks: design considerations and research challenges. Transactions on Emerging Telecommunications Technologies, 2015. 26(2): p. 107-130.

[22] Khalid, O., et al., Comparative study of trust and reputation systems for wireless sensor networks. Security and Communication Networks, 2013. 6(6): p. 669-688.

[23] Rani, V.U. and K.S. Sundaram, Review of trust models in wireless sensor networks. Int. J. Comput. Inf. Syst. Control Eng, 2014. 8: p. 371-377.

[24] Zin, S.M., et al., Routing protocol design for secure WSN: Review and open research issues. Journal of Network and Computer Applications, 2014. 41: p. 517-530.

[25] Duan, J., et al., TSRF: A trust-aware secure routing framework in wireless sensor networks. International Journal of Distributed Sensor Networks, 2014. 10(1): p. 209436.

[26] Butun, I., S.D. Morgera, and R. Sankar, A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 2014. 16(1): p. 266-282.

[27] Pirbhulal, S., et al., A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors, 2017. 17(1): p. 69.

[28] Usman, M., et al. Data sharing in secure multimedia wireless sensor networks. in IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2016. IEEE.

[29] Lu, H., J. Li, and M. Guizani, Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE transactions on parallel and distributed systems, 2014. 25(3): p. 750-761.

[30] Kavitha, H. and K. Pushpalatha, Secure Authentication Technique for Wireless Sensor Networks with Load-Balancing Routing Protocol. Traffic, 2015. 3(6).

[31] Han, G., et al., Secure communication for underwater acoustic sensor networks. IEEE communications magazine, 2015. 53(8): p. 54-60.

[32] Ozdemir, S. and Y. Xiao, Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks, 2009. 53(12): p. 2022-2037.

[33] Geetha, V. and K. Chandrasekaran, A distributed trust based secure communication framework for wireless sensor network. Wireless Sensor Network, 2014. 6(09): p. 173.

[34] Ren, Y., et al., A novel approach to trust management in unattended wireless sensor networks. IEEE Transactions on Mobile Computing, 2014. 13(7): p. 1409-1423.