IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Wireless Sensor Networks: Applications, Protocols And Security

Dimpi Dewangan[a], Raghavendra Prasad[b*]

[a, b] Amity University Chhattisgarh

Abstract

Wireless sensor networks (WSNs) are most important technology for large-scale monitoring, providing sensor measurements at high temporal and spatial resolution. The simplest application is sample and send where measurements are relayed to a base station. (Pathan & Lee, 2006). Wireless Sensor area is growing at an accelerated pace, attracting more and more people to its use, It is communication and digital electronic has led to the massive deployment of tiny size, low cost and power, multifunctional and high performance sensor nodes. . Thus, the network technologies of WSNs have become a global trend in communication (Cheour et al., 2011). WSNs is having a crucial role in enhancing the socio-economic aspects of the life by enhancing the quality of living by state of the art applications in the area of healthcare, atmospheric sciences and in various environment associated factors also. WSN functions similar to the existing wireless transporting medium additionally adding the flexibility and security paradigm (Belghith & Obaidat, 2016). In this review paper roll of machine learning (Alsheikh et al., 2014), IoT(Alsheikh et al., 2014), and impact so many areas Healthcare-(Alemdar & Ersoy, 2010). Environment -(Pavkovic et al., 2010).Protocol :- The protocol is a processed to select suitable path for the data to travel from source to destination. (Shabbir & Hassan, 2017). This is allows random deployment in inaccessible terrains or disaster relief operations. In order to meet the issues we confront in daily life, pervasive computing, artificial intelligence research, and wireless sensors and sensor networks have combined to create the interdisciplinary idea of ambient intelligence. A WSNs is a network of nodes which work cooperatively to monitor the surrounding environment. Moreover, widely used applications of WSNs are presented and the potential of WSNs for many other application areas is emphasized. The wireless sensor network is an infrastructure less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitors the system, physical or environment. It is a very useful for human beings. This review paper is to discuss some of the most relevant issues of WSNs, from the application, design and technology point of view. We covered also the techniques reducing the power consumption within the nodes(Cheour et al., 2011).

Key words:

Wireless Sensor Network, Applications, Technology, Network.

Introduction

Wireless sensor networks (WSNs) are most important technology for large-scale monitoring, providing sensor measurements at high temporal and spatial resolution. The simplest application is sampling and sending where measurements are relayed to a base station, WSNs recording the physical state of the environment**.** . (Pathan & Lee, 2006). WSNs are useful in a wide range of crucial fields, including the military, homeland security, healthcare, the environment, education, agriculture, and industry, among others. One can envision in the future the deployment of large- scale sensor networks where hundreds and thousands of small sensor nodes form self-organizing wireless networks. Providing security in sensor networks is not an easy task (Khemapech et al., n.d.). WSNs have recently been a key study area. They have a significant long-term economic potential, the power to change how we live, and provide several new system-building challenges and duties (Arampatzis et al., 2005). Sensor networks also pose a number of new conceptual and optimization problems. Some of them, such location, deployment, and tracking, are fundamental problems since so many applications depend on them for vital data. Can be provided by a particular sensor network. The integration of multiple types of sensors such as seismic, acoustic, optical, etc. (Ramson

& Moni, n.d.). The earliest WSNs studies from a decade ago demonstrated the technology's potential for a wide range of monitoring applications, including forests, waterways, buildings, security, and the battlefield, as well as how it might revolutionized the way we do business and science (Steele et al., 2009). The availability of low-cost, low-power, feature-rich microcontrollers and single-chip radio transceivers set off a hype cycle for WSN technology (Buratti et al., 2009). Our colleagues, who are mostly scientists, have high expectations of something that pretends to be an instrument, and this expectation is not irrational, according to an early claim that WSNs are a novel instrument for obtaining data about the natural world. They demand in particular a high level of system performance, productivity, and integration (Networks, n.d.).

Sensor networks history

Sensor components have developed to build more powerful applications at a lower cost, starting with specific research goals that contributed to military applications. Any development's major goal is to reduce a sensor node's size so that it can be dispersed widely across a target area. The power supply unit of each node is unlikely to be replaced or recharged throughout the course of its operating lifetime, unlike a laptop or PDA (Roundy et al., 2004). Therefore, the main problem in today's sensor development is energy. Sensors are smaller and less expensive thanks to MEMS technology. More civilian applications have been noted as a result. Applications and components of sensor networks are covered in this section (Khemapech et al., n.d.).

Typical assumptions

Since wireless communications are used by sensor nodes, radio links are typically unsecure. Attacks on the network include eavesdropping, injection, replay, and other methods. The adversary can introduce malicious nodes into the network or takes control of some trustworthy nodes. The majority of articles written about sensor network security in the literature do not address (Ko et al., 2010)me that sensor nodes are tamper resistant since the corresponding investment adds significant per-unit cost to sensor nodes (Estrin et al., n.d.). Base station security and reliability are frequently taken for granted. A compromised base station might make the entire sensor network unusable because it serves as the gateway for sensor nodes to communicate with the outside world. As a result, it is presumed that base stations in sensor networks are secure (Ko et al., 2010). i. Other typical assumptions on sensor networks are: ii. Sensor nodes are densely and statically deployed in the network. One common presumption is that base stations Nodes of sensors are conscious of their own locations. In many sensor networks, location awareness is a fundamental requirement for sensor nodes because most sensing data needs to be linked to the places where it is created. There is no need for a GPS receiver at each sensor because the network can estimate the locations of individual nodes using localization services. Other specific presumptions made in certain works may restrict the applicability of the suggested methods (Mainwaring et al., n.d.).

Protocols

There are several protocols proposed for WSNs the MAC (Medium Access Control) layer reacts to this probabilistic reception information by adjusting the number of acknowledgments and/or retransmissions. An optimal route discovery protocol cannot, it is noticed, be based on a single retransmission by each node because such a search may not be successful in reaching the destination or identifying the best path. Next It is discussed how using "hello" packets to learn about your neighbours is not a simple procedure (Radi et al., 2012). The main goal of routing in WSNs is to carry out data communication when trying at the same time to prolong the network lifetime and provide high quality of service during data delivery .Data Centric Based, Location Based Routing, Group Based Routing, Hierarchical Based Routing (Sambo et al., 2019).

Application categorization

There have been several attempts to categories sensor network applications. All of them traditionally focus on the field of the application being used such as several monitoring. Eight different sorts of applications are categorized traditionally. This kind illustrates how sensor networks are used for various purposes. Objective-Oriented categorization – Five groups of application; Military, Public Security/Warning, Education, Business Competitiveness (BC) Improvement, and Quality-of-Life (QOL) Improvement are also provided. Some traditional applications can be placed into more than one category (In, 2008). WSNs components - The main components of WSNs is processing unit, transceiver, power unit (Networks, n.d.).

Previous studies

The first wireless network that can be defined as modem WSN is known as the Sound Surveillance System (SOSUS). SOSUS was developed to detect Soviet submarines by the U.S. Military in the 1950s. SOSUS network is designed to have submerged sensors and hydrophones which are scattered in the Atlantic and Pacific Oceans (Cui et al., 2005). For widespread monitoring, wireless sensor networks (WSNs) are the most significant and practical technology because they provide sensor measurements with high temporal and spatial precision (Pathan & Lee, 2006). The deployment of massive sensor networks, made up of tens of thousands of tiny sensor nodes, is something that is conceivable for the future (Khemapech et al., n.d.). Wireless sensors have seen a significant evolution recently, primarily due to advancements in sensor hardware technology (miniaturization of components, increased ROM and RAM capacities, more energy capacity etc (Martínez et al., 2007). The position of sensor nodes need not be engineered or pre-determined. This is allows random deployment in inaccessible terrains or disaster relief operations (Portillo et al., 2018). In order to meet the issues we confront in daily life, pervasive computing, artificial intelligence research, and wireless sensors and sensor networks have combined to create the interdisciplinary idea of ambient intelligence (Alemdar & Ersoy, 2010). The industrial Internet of Things (IoT) was created at the same time as the deep integration of industrialization and information technology made it possible to gradually connect different parts of industrial production (Alemdar & Ersoy, 2010). As all data can be gathered and processed centrally, WSNs monitoring offers continuous and nearly real-time data acquisition as well as autonomous data acquisition (no supervision is necessary); increased monitoring frequency compared to manual inspection; and better data accessibility, management, and use compared to non-networked systems (Hodge et al., 2015). With a wide range of applications, including environmental, industrial, military, and health applications, WSNs have been a prominent research area for the past 20 years. The random deployment of WSNs in inhospitable locations where it is frequently impractical to replenish a node's energy source is one of their fundamental characteristics (Kosunalp, 2015). The main responsibility of the sensor nodes in each application is to sense the target area and transmit their collected information to the sink node for further operations (Radi et al., 2012). A large number of autonomous nodes with limited processing and energy resources, wireless communication interfaces, and sensing capabilities make up wireless sensor networks. WSNs are employed for the distributed and collaborative sensing of interesting physical phenomena and events (Saleem et al., 2011). Typically, a military force or other authority will place sensor nodes in a predetermined area, and these nodes will then automatically form a wireless network (Zhou et al., 2008). WSNs consist of small nodes that sense their environment, process data, and communicate through wireless links. They are expected to support a wide variety of applications, many of which have at least some requirements for security(Amin et al., 2008).As the name implies, preventative measures work to stop attacks or, at the very least, significantly hinder them. This is the area with the most study and uses fairly common cryptographic primitives to ensure confidentiality, integrity, and authentication (Healy et al., 2009). WSNs typically consist of sensor devices that are powered by batteries and have computation, data processing, and communication components. The sensors may be used in an uncontrolled environment or in a regulated setting where monitoring and surveillance are essential. Security for sensor networks becomes crucial in uncontrolled contexts (Kumar et al., 2014).Wireless transceivers are used in wireless sensor networks to facilitate communication in between sensors. Numerous researchers have been drawn to investigate on various problems relating to these kinds of networks by their appealing properties. However, despite the popularity of routing techniques and wireless sensor network design, security concerns have not yet received significant attention (Portillo et al., 2018). Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities (Boyle & Newe, 2008).When developing a security system for a WSN, it is crucial to make sure that all known attacks are guarded against. The stability and resilience of the application against assault will be key factors in determining its success (Das & Thampi, 2015). Thousands of sensor nodes make up a large-scale sensor network, which may be spread out over a huge region. Typical sensor nodes are battery-powered, compact, and have constrained communication and computing capabilities. These tiny sensor nodes are vulnerable to a variety of assaults(In, 2008).Security goals in sensor networks depend on the need to know what we are going to protect. We determine four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (Pathan & Lee, 2006). A number of economic and technological developments, such as Moore's Law, have made sophisticated electronics accessible to the general public. These technologies have the potential to enhance our daily lives with true ambient intelligence when combined with WSNs (Baker et al., 2007). The combination of wireless sensors and sensor networks with computing and artificial intelligence research have built a cross-disciplinary concept of ambient intelligence in order to overcome the challenges we face in everyday life (Darwish & Hassanien, 2011).

Sensors

Conventional integrated circuit naturally have the ability to sense a few phenomenon in a small space, like light and temperature, but micromachining has allowed researchers to compress many different types of sensors into small spaces while frequently maintaining or even improving performance levels over those of conventional transducers. Detectors of radiation, magnetic sensors, flow sensors, chemical and biological sensors, accelerometers, gyroscopes, pressure sensors, microphones, and thermal sensors are a few examples. There are most common architecture for WSN follows the OSI Model. Basically in sensor network we need five layer: application layer, transport layer, network layer, data link layer and physical layer (Jindal DAV College, 2018).

Security and Attacks in Wireless Sensor Networks

Security of WSNs is an important issue, especially if they have mission-critical task. Attacks against the security of WSNs can be grouped into two branches as; active and passive. In active attacks, an attacker actually affects the operations badly in the targeted network. Passive attacks can be grouped into eavesdropping attack, node tampering attack, node malfunctioning attack, node destruction attack and finally, traffic analysis attack (Cui et al., 2005). Broadly speaking, there are two levels of viewpoints that can be used to analyse attacks on wireless sensor networks. One is an assault on the security mechanisms, while the other is an assault on the fundamental mechanisms like routing mechanisms (Kumar et al., 2014).

Applications

As it is known, WSNs provide sensing, monitoring and controlling, managing options. Therefore, they have vast amount of application fields such as military applications, environmental applications, and industrial applications. In military applications, monitoring friendly forces or battlefield surveillance are realized by WSNs. In environmental application, air and water quality that all can be monitored by WSNs (Cui et al., 2005).

The WSNs applications are given in the figure 1 below-

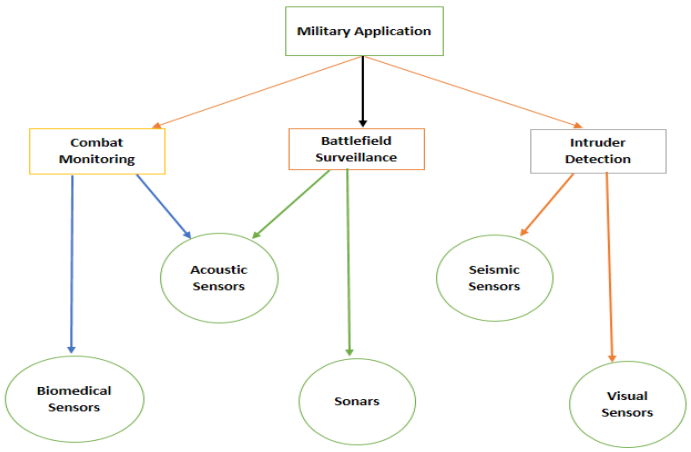

Fig. 1, Wireless Sensor Network Applications

WSNs protocol in IoT, Role and challenges of WSNs, Machine Learning in WSNs

Today Internet is migrating from connecting people to connecting things, leading to the new concept of Internet of thing (IoT). It is predicted that 212 billion devices will be installed by 2020 (Kuo et al., 2018). This presented system provided farmers with useful information in a user-friendly and easy to access way with real-time data communications through IoT about saltwater intrusions, the moisture of soil, level of water, wet conditions, temperature and the general state of the land (Gulati et al., 2021). Challenges - Real time management, Security and privacy, Security, Quality of service, Configuration, Data integrity(Gulati et al., 2021). However, machine learning experts recognize it as a rich field with very large themes and patterns. Understanding such themes will be beneficial to those who wish to apply machine learning to WSNs. Existing machine learning algorithms can be categorized by the intended structure of the

model. Most machine learning algorithms fall into the categories of supervised, unsupervised and reinforcement learning (Alsheikh et al., 2014).

Wireless Sensor Network Design and Server implementation

Due to the abundance of features, designing WSNs entails a variety of factors and considerations and frequently necessitates taking into account a number of related concerns at once, including connection, channel access, signal processing methods, etc. Nodes are arranged in a cluster-based topology with the assumption that they are dispersed over the region using a Poisson point process (Buratti et al., 2009). Server layer of implements the role of mediator between users and WSNs. The interaction with the long-range communication modules has to be carefully designed (Boyle & Newe, 2008).

Area of WSNs uses area of WSNs uses, User interface

Wireless sensor networks have grown substantially over the years and have a momentous potential in diverse applications in areas healthcare (Alemdar & Ersoy, 2010), security(Huo et al., 2009)**,** technology(Buratti et al., 2009)., environment , telecommunication, education services, agriculture, surveillance, military services etc (Buratti et al., 2009). At this regard, in the SEA project architecture, two solutions have been implemented to allow data transfers between modem and server:-1.Socket TCP/IP; 2.SMS. (Longhi et al., 2012).

The whole system provides two ways to allow a user to interact with it:

i. A custom software client.
ii. A WEB browser (Longhi et al., 2012).

Clustering algorithms for WSNs, Localization WSNs, Convergecast WSNs, Fuzz logic in WSNs

WSNs often comprise a sizable sensor network with hundreds or even thousands of sensors. Clustering is a useful tool for managing such a large node population. We give a literature review of distributed techniques for clustering WSNs in this part. Given that scalability is regarded as the main advantage of network clustering, the surveyed algorithms are grouped according to their convergence rate into two subsections for variable and constant convergence time algorithms, respectively (Abbasi & Younis, 2007). Localization is extensively used in WSNs to identify the current location of the sensor nodes. A WSN consist of thousands of nodes that make the installation of GPS on each sensor node expensive and moreover GPS will not provide exact localization results in an indoor environment (Pal, 2010). A WSNs consists of sensor nodes deployed in an environment for collecting and transmitting data regarding changes in the environment In Wireless Sensor Networks the process of dissemination of data among various sensor nodes is called broadcast and collection of data from all sensor nodes is called convergecast are common communication operations (Rathnayaka & Potdar, 2013). The use of fuzz logic in WSNs is shown to be a promising technique since it allows combining evaluating diverse parameters in an efficient manner. Fuzz logic is a good approach due to the execution requirement can be easily supported by sensor nodes, while it is able improve the overall network performance (Taylor et al., 2012)**.**

Aggregation in WSNs, Energy consumption in WSNs, Cryptographic Frameworks for WSNs

In WSNs data aggregation is a process of collecting and combining the useful information in a particular region of interest. The effective of the communication among nodes depend on the data aggregation technique being used (Ozdemir & Xiao, 2022). Energy Consumption Approach Based on Ant Colony in wireless Sensor network. It is the amount of energy consumed during the packets transmission by each node and calculates the overall energy of the whole network (Pavkovic et al., 2010). In this part of cryptograph framework we covered frameworks that have been specifically created and put into use to secure wireless sensor networks. We categories the existing frameworks based on the shared key's nature, or whether it is private or public. Asymmetric cryptographic frameworks, ECC-based cryptographic frameworks, and pairing-based cryptographic frameworks are further categorized (Sharma & Verma, 2012).

Discussion

The methods for reducing congestion described above concentrate on channel monitoring to dynamically modify the data forwarding rate. The installed sensors and their data rate correspond to two categories of problems that CODA is intended to address. It does not, however, offer any queue occupancy monitoring. Even sending a tiny amount of ACK in situations of ongoing congestion could make the situation worse. Additionally, this system needs feedback signalling, which raises the cost. A WSN is a network of nodes which work cooperatively to monitor the surrounding environment. It is necessary to provide an interaction between people and nodes' environment. In this paper, WSNs are described in a compact manner and technical details of their characteristics are provided. Moreover, widely used applications of WSNs are presented and the potential of WSNs for many other application areas is emphasized. Protocol Stacks, advantages and disadvantages of WSNs are listed. Wireless sensor networks have been widely used in many areas. They provide endless opportunities, but at the same time pose several challenges, such as the fact that energy is a scarce and usually non-renewable resource. Flexibility of WSNs - The architecture of WSN is not fixed. Rather it varies from application to application which justifies that the protocols and algorithms have the characteristics of self-organization.

Conclusion

Wireless sensor networks (WSNs) have attracted significant attention over the past few years. Wireless sensor networks make it possible to monitor the physical environment effectively. The primary operational restriction is energy availability. We suggest a sensor network organization in which the nodes are divided into mutually incompatible sets in order to maximize the effective usage of batteries by randomly arranged sensors. Such a set always has one active set. Recent advanced hardware technologies result in more powerful sensors as small as a few millimetres volume. The main drawback is still energy constraints. Additional strategies aiming at extending sensor lifetimes have also been studied along with pre-processing or data aggregation prior to transmission, and the optimal positions to place sensors. WSNs provides several types of application providing comfortable and smart-economic life. This paper reviews the wireless sensor network applications which focus mainly on the monitoring process system. These systems has low power consumption, low cost and is a convenient way to control real-time monitoring for unprotected agriculture and habitat. As future works, we plan to classify the optimized clustering in terms of WSNs types. We would talk about clustering parameters used to WSNs which locations are non-terrestrial or not above the ground but rather under the water or under the ground. In addition to future work, we would discuss about the spectrum-awareness or spectrum-efficient clustering studies in practical large wireless sensor networks.

Reference

Abbasi, A. A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, *30*(14–15), 2826–2841. https://doi.org/10.1016/j.comcom.2007.05.024

Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks*, *54*(15), 2688–2710. https://doi.org/10.1016/j.comnet.2010.05.003

Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. (2014). *Machine Learning in Wireless Sensor Networks : Algorithms , Strategies , and Applications*. *c*, 1–24. https://doi.org/10.1109/COMST.2014.2320099

Amin, F., Jahangir, A. H., & Rasifard, H. (2008). Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. *Engineering and Technology*, *31*(July), 530–535. http://www.akademik.unsri.ac.id/download/journal/files/waset/v41-91.pdf

Arampatzis, T., Lygeros, J., & Manesis, S. (2005). A survey of applications of wireless sensors and wireless sensor networks. *Proceedings of the 20th IEEE International Symposium on Intelligent Control, ISIC '05 and the 13th Mediterranean Conference on Control and Automation, MED '05*, *2005*, 719–724. https://doi.org/10.1109/.2005.1467103

Baker, C. R., Armijo, K., Belka, S., Benhabib, M., Bhargava, V., Burkhart, N., Der Minassians, A., Dervisoglu, G., Gutnik, L., Haick, M. B., Ho, C., Koplow, M., Mangold, J., Robinson, S., Rosa, M., Schwartz, M., Sims, C., Stoffregen, H., Waterbury, A., … Wright, P. K. (2007). Wireless sensor networks for home health care. *Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW'07*, *1*, 832–837. https://doi.org/10.1109/AINAW.2007.376

Belghith, A., & Obaidat, M. S. (2016). Wireless sensor networks applications to smart homes and cities. *Smart Cities and Homes: Key Enabling Technologies*, 17–40. https://doi.org/10.1016/B978-0-12-803454-5.00002-X

Boyle, D., & Newe, T. (2008). Securing wireless sensor networks: Security architectures. *Journal of Networks*, *3*(1), 65–77. https://doi.org/10.4304/jnw.3.1.65-77

Buratti, C., Conti, A., Dardari, D., & Verdone, R. (2009). An overview on wireless sensor networks technology and evolution. *Sensors*, *9*(9), 6869–6896. https://doi.org/10.3390/s90906869

Cheour, R., Lahmar, K., & Abid, M. (2011). Evolution of wireless sensor networks and necessity of power management technique. *2011 Faible Tension Faible Consommation, FTFC 2011*, 75–78. https://doi.org/10.1109/FTFC.2011.5948923

Cui, L., Ju, H., Miao, Y., Li, T., Liu, W., & Zhao, Z. (2005). Overview of wireless sensor networks. *Jisuanji Yanjiu Yu Fazhan/Computer Research and Development*, *42*(1), 163–174. https://doi.org/10.1360/crad20050121

Darwish, A., & Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, *11*(6), 5561–5595. https://doi.org/10.3390/s110605561

Das, A. P., & Thampi, S. M. (2015). Secure communication in mobile underwater wireless sensor networks. *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, *00*(c), 2164–2173. https://doi.org/10.1109/ICACCI.2015.7275937

Estrin, D., Giro, L., Pottie, G., & Srivastavat, M. (n.d.). *INSTRUMENTING THE WORLD WITH WIRELESS SENSOR NETWORKS Department of Computer Science Department of Elecrical Engineering*. 2033–2036.

Gulati, K., Kumar Boddu, R. S., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2021). A review paper on wireless sensor network techniques in Internet of Things (IoT). *Materials Today: Proceedings*, *51*(xxxx), 161–165. https://doi.org/10.1016/j.matpr.2021.05.067

Healy, M., Newe, T., & Lewis, E. (2009). Security for wireless sensor networks: A review. *SAS 2009 - IEEE Sensors Applications Symposium Proceedings*, 80–85. https://doi.org/10.1109/SAS.2009.4801782

Hodge, V. J., O'Keefe, S., Weeks, M., & Moulds, A. (2015). Wireless sensor networks for condition monitoring in the railway industry: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *16*(3), 1088–1106. https://doi.org/10.1109/TITS.2014.2366512

Huo, H., Xu, Y., Yan, H., Mubeen, S., & Zhang, H. (2009). An elderly health care system using wireless sensor networks at home. *Proceedings - 2009 3rd International Conference on Sensor Technologies and Applications, SENSORCOMM 2009*, 158–163. https://doi.org/10.1109/SENSORCOMM.2009.32

In, O. (2008). *S ECURITY IN W IRELESS S ENSOR N ETWORKS*. *August*, 60–66.

Jindal DAV College, V. (2018). History and Architecture of Wireless Sensor Networks for Ubiquitous Computing. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *7*(2), 2278–1323.

Khemapech, I., Duncan, I., & Miller, A. (n.d.). *A Survey of Wireless Sensor Networks Technology*.

Ko, B. J., Lu, C., Srivastava, M. B., Stankovic, J. A., Ieee, F., Terzis, A., & Welsh, M. (2010). *for Healthcare*. *98*(11).

Kosunalp, S. (2015). MAC protocols for energy harvesting wireless sensor networks: Survey. *ETRI Journal*, *37*(4), 804–812. https://doi.org/10.4218/etrij.15.0115.0017

Kumar, V., Jain, A., & Barwal, P. N. (2014). Wireless Sensor Networks: Security Issues, Challenges and Solutions. *International Journal of Information & Computation Technology*, *4*(8), 859–868. http://www.irphouse.com

Kuo, Y. W., Li, C. L., Jhang, J. H., & Lin, S. (2018). Design of a Wireless Sensor Network-Based IoT Platform for Wide Area and Heterogeneous Applications. *IEEE Sensors Journal*, *18*(12), 5187–5197. https://doi.org/10.1109/JSEN.2018.2832664

Longhi, S., Marzioni, D., Alidori, E., Di Buò, G., Prist, M., Grisostomi, M., & Pirro, M. (2012). Solid waste management architecture using wireless sensor network technology. *2012 5th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2012 Conference and Workshops*. https://doi.org/10.1109/NTMS.2012.6208764

Mainwaring, A., Polastre, J., Szewczyk, R., & Culler, D. (n.d.). *Wireless Sensor Networks for Habitat Monitoring*. 88–97.

Martínez, J. F., García, A. B., Corredor, I., López, L., Hernández, V., & Dasilva, A. (2007). QoS in wireless sensor networks: Survey and approach. *Euro American Conference on Telematics and Information Systems - Proceedings of the 2007 Euro American Conference on Telematics and Information Systems, EATIS 2007*. https://doi.org/10.1145/1352694.1352715

Networks, S. (n.d.). *Efficient Organization of Wireless*. 472–476.

Ozdemir, S., & Xiao, Y. (2022). Secure data aggregation in wireless sensor networks : A comprehensive overview q. *Computer Networks*, *53*(12), 2022–2037. https://doi.org/10.1016/j.comnet.2009.02.023

Pal, A. (2010). *Localization Algorithms in Wireless Sensor Networks : Current Approaches and Future Challenges*. *2*(1), 45–74.

Pathan, A. K., & Lee, H. (2006). *Security in Wireless Sensor Networks : Issues and Challenges*. 1043–1048.

Pavkovic, B., Theoleyre, F., Barthel, D., & Duda, A. (2010). Experimental analysis and characterization of a wireless sensor network environment. *PE-WASUN'10 - Proceedings of the 7th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Co-Located with MSWiM'10*, 25–32. https://doi.org/10.1145/1868589.1868595

Portillo, C., Martinez-Bauset, J., & Pla, V. (2018). Modelling of S-MAC for Heterogeneous WSN. *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, *2018-Janua*, 1–6. https://doi.org/10.1109/NTMS.2018.8328705

Radi, M., Dezfouli, B., Bakar, K. A., & Lee, M. (2012). Multipath routing in wireless sensor networks: Survey and research challenges. *Sensors*, *12*(1), 650–685. https://doi.org/10.3390/s120100650

Ramson, S. R. J., & Moni, D. J. (n.d.). *Applications of Wireless Sensor Networks – A Survey*. *978*, 325–329.

Rathnayaka, A. J. D., & Potdar, V. M. (2013). Wireless sensor network transport protocol: A critical review. *Journal of Network and Computer Applications*, *36*(1), 134–146. https://doi.org/10.1016/j.jnca.2011.10.001

Roundy, S., Steingart, D., Frechette, L., Wright, P., & Rabaey, J. (2004). *Power Sources for Wireless Sensor Networks*. 1–17.

Saleem, M., Di Caro, G. A., & Farooq, M. (2011). Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions. *Information Sciences*, *181*(20), 4597–4624. https://doi.org/10.1016/j.ins.2010.07.005

Sambo, D. W., Yenke, B. O., Förster, A., & Dayang, P. (2019). Optimized clustering algorithms for large wireless sensor networks: A review. *Sensors (Switzerland)*, *19*(2). https://doi.org/10.3390/s19020322

Shabbir, N., & Hassan, S. R. (2017). Routing Protocols for Wireless Sensor Networks (WSNs). *Wireless Sensor Networks - Insights and Innovations*. https://doi.org/10.5772/intechopen.70208

Sharma, G., & Verma, A. K. (2012). *Security Frameworks for Wireless Sensor Networks-Review*. *6*, 978–987. https://doi.org/10.1016/j.protcy.2012.10.119

Steele, R., Lo, A., Secombe, C., & Wong, Y. K. (2009). Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. *International Journal of Medical Informatics*, *78*(12), 788–801. https://doi.org/10.1016/j.ijmedinf.2009.08.001

Taylor, P., Singh, A. K., Purohit, N., & Varma, S. (2012). *Fuzzy logic based clustering in wireless sensor networks : a survey*. *April 2013*, 37–41.

Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials*, *10*(3), 6–28. https://doi.org/10.1109/COMST.2008.4625802