Irish Interdisciplinary Journal of Science & Research (IIJSR)
Volume 8, Issue 2, Pages 71-77, April-June 2024

A Survey on Computational Techniques in WSN Networks

Anand Karuppannan[1*] & Mekala Rathinam[2]

[1,2]*Assistant Professor,* [1]*Department of Electronics and Communication Engineering,* [2]*Department of Information Technology,* [1,2]*Gnanamani College of Technology, Namakkal, India. Email: anandped2012@gmail.com*[*]

DOI: https://doi.org/10.46759/IIJSR.2024.8208

Article Received: 07 March 2024 *Article Accepted: 09 May 2024* *Article Published: 13 May 2024*

ABSTRACT

A network made up of many tiny, inexpensive sensors that use wireless communications is now technically and economically possible because to considerable advancements in hardware manufacturing technology and the creation of effective software algorithms, this is known as a wireless sensor network. The use of sensor networks in mission-critical environments like conflict zones as well as in more commonplace security and business applications like building and traffic surveillance, habitat monitoring, and smart homes, among others, has considerable promise. Wireless sensor networks, however, provide particular security difficulties. Because WSNs are used for so many security-sensitive applications, security is now a top issue for protocol designers working on WSNs. We have attempted to list all known security flaws in wireless sensor networks in this study, which also examines a broad range of WSN attacks and their categorization processes. The various security measures that may be used to counter them, as well as the difficulties encountered. In this paper, we've taken up the problem and put forward a proposal for an integrated, all-encompassing security that would provide security services for all sensor network services. It is lucrative to be utilised in significant quantities in the future incorporating the wireless connectivity, computational power, and sensor technologies it combines. There are several different security risks associated with wireless communication technologies

Keywords: WSN; Wireless communication technologies; Security; WSN attacks; Connectivity; Computational power.

1. Introduction

A WSN is a sizable network of sensor nodes with limited resources that perform a variety of programmed tasks, including sensing and processing, to meet various application goals. The base stations and sensor nodes are the two main components of a WSN. In fact, they may be conceptualised as the network's "brain" and "sensing cells," respectively. Typically, an authority deploys sensor nodes in a predetermined region, and the nodes then automatically create a wireless network. A deterministic strategy may be used to deploy homogeneous or heterogeneous type sensor nodes at random or at pre-selected places. In contrast to mobile nodes, which may be deployed in accordance with application needs, sensor nodes are typically static. The network is installed together with one or more base stations (BSs), either static or mobile. After being installed, sensor nodes continue to watch over the network region [1]-[5].

If many nearby nodes identify the same event, collaboration may be possible. In this instance, one of them works with the other nodes to provide a final report. The report may be processed by the BS, who can then transmit it over high-quality wired or wireless lines to the outside world for further processing. A BS broadcasts orders and inquiries that the WSN authority sends to it across the network. As a result, a BS serves as a conduit between the WSN and the outside world. Evidently, the needs of the application are a deciding factor when selecting the hardware for a wireless sensor node. Hardware and software for sensing, data processing, and communication are integrated in a sensor node. They use wireless channels to send information to and receive information from other nodes. Since the battery life greatly affects the lifespan of a sensor node, it is crucial to use energy-efficient information processing techniques. Every intelligent control system must have sensors. One of the information technologies that is growing the fastest is wireless sensor networks, which have a wide range of potential uses in

Next Generation Networks, the Internet of Things, and for applications that are both mission-critical and safety-related. One of the most crucial characteristics of such systems is reliability. A Markov model is suggested in the study for reliability evaluations of sensor nodes in wireless sensor networks. It has been shown that the sensor node's dependability relies on its monitoring approach and is a unimodal function of the test time. One of the information technologies that is growing the fastest is wireless sensor networks (WSNs), which have a number of potential uses in next-generation networks (NGNs) and cyber-physical systems (CPS) [6]-[10].

Sensor technologies, signal processing, computing, and wireless networking are all combined in one system by wireless integrated network sensors. The term "cyber-physical system" refers to the tight interactions and feedback controls between cyber components and physical components, where cyber components are typically systems for sensing and communication and physical components are typically any number of systems in use. A key topic of study in recent years has been the effective design of wireless sensor networks. A sensor is a machine that reacts to and picks up input from environmental or physical factors, such as pressure, heat, light, etc. An electrical signal is often transferred from the sensor's output to a controller for further processing. A network of gadgets that can wirelessly transmit the data obtained from a monitored field is known as a wireless sensor network. Multiple nodes are used to forward the data, and a gateway is used to link it to other networks like wireless Ethernet.

A wireless network called a WSN is made up of base stations and several nodes (wireless sensors). These networks are used to cooperatively send data to a central location while simultaneously monitoring physical or environmental factors including sound, pressure, and temperature. A wireless sensor network is a collection of geographically scattered, specialised sensors that are used to monitor environmental variables, record them, and organise the information at a central point [11]-[15].

2. Challenges in Wireless Sensor Networks

The future of Zigbee wireless communication technology is bright. In a few years, Zigbee will be utilised for home networks, building automation, medical equipment control, mine safety, and more. Home automation and industry control will be the two primary application areas. Families use Zigbee wireless communication. Home temperature management, remote control of interior lighting systems, and curtain auto-adjustment are all easily accomplished. In order to read metres using Zigbee wireless communication technology, the monitoring centre just has to examine and compute data collected from customers and determine their power use.

After then, the user's energy account is debited for the monthly electric bill. Workers are then required to read the metre at the user's house, and it is avoided if users aren't there. It is more crucial to employ safety than working quickly for the sake of the workforce. introduces an experimental Zigbee-based home security monitoring and alarming system that can monitor door and window magnetic contact, smoke, gas leaks, flooding, and other events while also offering basic controls like shutting off valves and transmitting alarms to a residential area security network. In factories or businesses, Zigbee wireless communication technology is used.

It is used in the information systems of coal preparation firms, where all of the drawbacks of the conventional cable network system are eliminated. This significantly increases the degree of information automation, information management, aa well as automation.

In the ARM NC system network, Zigbee wireless communication technology is used. The results of the experiments shown that the enhanced approach can ensure the processing effectiveness of the NC system with satisfactory accuracy and data transmission rate. A cutting-edge Zigbee-based laser alarm system is suggested in with the goal of improving substation perimeter safety. It comprises of a data central monitoring subsystem and a laser railing security subsystem, and because the two subsystems communicate through Zigbee wireless technology, workers may access a real-time human-machine interface.

In mining, Zigbee wireless communication is used. The Miner's Lamp Monitoring uses Zigbee technology with the goal of enhancing worker and production safety. This system can facilitate staff orientation underground, monitor and manage the miner's lamp's charge level, and effectively manage and regulate the usage of the miner's light. The improved method has been researched in Zigbee and has been widely used in many areas due to the advantage of low power consumption and low cost, making it suitable for large-scale application.

The system also can be more easily increased with the humidity, gas, and other sensors, to achieve mine environmental monitoring, ensure safety in production. However, there are some issues right now, including the coordinator carrying too many nodes, which is necessary to cause bad real-time, data packet loss, and stability decrease; additionally, there are some locations where it is challenging for humans to change the batteries of nodes, or there are a sizable number of nodes which is difficult to change presents an improved design, the coordinator only deal with the task on the Zigbee network, the coordinator only deals with the task on the Zigbee network; and finally, there are Zigbee routing protocol was created with the key purpose of extending the lifespan of the Zigbee network. It introduces the EA-AODV energy-aware routing method, which may increase the efficiency of the Zigbee network while reducing energy consumption. Container uses Zigbee wireless connectivity technology. In order to maintain energy load balancing between network nodes and successfully extend node and network lifespan, the information system in the study proposes networking and routing technique.

The need for study in these areas is very important. After Bluetooth, ZigBee technology has become the new norm in wireless personal area. A new wireless metre reading system based on the ZigBee protocol is feasible when this technology is introduced. This system, which is made up of a database management system and a ZigBee network, offers numerous significant benefits, including cheap cost, low power consumption, and low data rate.

As a new wireless protocol in personal area, ZigBee has its unique characteristics including low cost, low data rate, and low power consumption which corresponds to a large market. This paper provides an application in the field of building automation. The fusion of two emerging technologies - WSN and RFID that can give full play to the advantages of both technologies complement each other. It provides more reliable technique protection on the coal mine environmental monitoring and has great significance in China Mine safety. In this paper wireless sensor network technology is discussed along with application and it is clear that WSN proves to be emerging technology. ZigBee is a brand-new wireless protocol for use in personal areas. It stands out for its cheap price, low data rate, and low power consumption, all of which equate to a sizable market. In the area of building automation, this article offers an application. Combining two cutting-edge technologies—WSN and RFID—that may fully exploit the benefits of both technologies complements one another. It offers more trustworthy method protection for

monitoring the environment in coal mines and is very important for China Mine safety. This study discusses wireless sensor network technology and applications, and it is evident that WSN is an emerging technology.

Wireless sensor network (WSN) technological advancements have made compact, inexpensive sensor nodes with the capacity to analyse data, communicate wirelessly, and sense a variety of physical and environmental variables available. There are a wide range of applications due to the diversity of sensing capabilities. The peculiarities of wireless sensor networks, however, call for more efficient approaches to data processing and forwarding. The sensor nodes of a WSN have a constrained transmission range, constrained processing and storage, and constrained energy resources. In these circumstances, routing systems for wireless sensor networks must enable reliable multi-hop communication while still preserving the network's pathways. In this article, we provide an overview of wireless sensor network routing techniques and contrast their advantages and disadvantages.

The majority of sensor networks have various application needs and are application-specific. The following primary design goals are thus all or partially taken into account when designing sensor networks: Small node size: Since sensor nodes are often deployed in large numbers in a hard or hostile environment, lowering node size helps ease node deployment.

Additionally, it will lower the price and power use of sensor nodes. Low node cost: Since sensor nodes are often deployed in large numbers in hostile or harsh environments and cannot be reused, lowering the cost of sensor nodes is crucial and will lower the cost of the whole network. Low power consumption: Since sensor nodes are battery-powered and it is frequently very difficult or even impossible to charge or recharge their batteries, it is essential to minimise the power consumption of sensor nodes in order to extend their lifespan as well as the lifetime of the entire network.

Scalability: Network protocols created for sensor networks should be adaptable to varied network sizes given that the number of sensor nodes in these networks is on the range of tens, hundreds, or thousands.

Reliability: To assure dependable data transmission across noisy, error-prone, and time-varying wireless channels, network protocols built for sensor networks must include error control and repair procedures.

Self-configurability: Sensor nodes in sensor networks should be able to autonomously arrange themselves into a communication network after they are deployed and reconfigure their connection in the case of topology changes and node failures.

Adaptability: Changes in node density and network architecture may occur in sensor networks as a consequence of a node failing, joining, or moving. Network protocols created for sensor networks should thus be adaptable to such variations in density and structure.

Channel utilisation: Since sensor networks have a certain amount of bandwidth, communication protocols created for them should effectively utilise the available bandwidth.

Fault tolerance: Because of their unsupervised operations and harsh deployment conditions, sensor nodes are susceptible to failure. As a result, sensor nodes need to be fault tolerant and capable of self-calibration, self-testing, self-repair, and self-recovery.

Security: A sensor network should have strong security measures to guard against unauthorized access to or malicious assaults on the network's or a sensor node's data.

The development of wireless communication technology is still advancing quickly. The field of wireless sensor networks has seen a sharp increase in research over the last several years (WSNs). WSNs use autonomous, geographically dispersed sensor nodes that are configured to perceive certain data to facilitate communication. Worldwide, WSNs are used in a broad range of military and non-military applications. Examples include tracking objects, keeping an eye on habitats, keeping an eye on patients, and spotting fires on the battlefield. Sensor networks are quickly becoming a popular technology with a bright future. The difficulties of coverage and deployment, scalability, quality-of-service, size, processing power, energy efficiency, and security still need to be resolved. This article provides an overview of the numerous wireless sensor network (WSN) applications as well as other security-related WSN concerns.

A wireless network made up of spatially dispersed autonomous devices that employ sensors to keep track of environmental or physical conditions is known as a wireless sensor network (WSN). A typical WSN system is made up of these autonomous devices, or nodes, together with routers and a gateway. A central gateway, which serves as a bridge to the wired environment and allows you to gather, process, analyse, and show your measurement data, receives wireless communication from the dispersed measurement nodes. You may use routers to provide an extra communication channel between end nodes and the gateway in a wireless sensor network to increase distance and dependability. Wireless sensor network deployment is now starting to pick up speed. It is fair to anticipate that in 10 to 15 years, wireless sensor networks would cover the whole planet, with Internet connection being available for their use. As a result, the Internet may be said to have evolved into a physical network.

This cutting-edge technology has limitless potential for use in a wide range of industries, including the environment, medicine, the military, transportation, entertainment, crisis management, and smart spaces. Military command, control, communication, and intelligence systems are increasingly reliant on WSNs. In a conflict zone, sensors may be set up to keep an eye on the presence of troops and vehicles and to track their movements, allowing for intimate observation of the enemy's forces. Elders and patients may be monitored and tracked via wireless sensor networks, which can help to alleviate the chronic scarcity of healthcare workers and lower the cost of treatment in the present health care systems. For instance, sensors may be installed in a patient's house to track their actions. When a patient falls and needs rapid medical assistance, it may notify physicians.

3. Conclusion

In this field, WSN applications include tracking temperature, humidity, and illumination in office buildings, as well as environmental variables influencing crops or cattle. These monitoring modules may even be paired with actuator modules that may regulate things like the quantity of fertiliser applied to the ground or the amount of cooling or heating applied to a building using dispersed sensor data. Humans can live in more comfortable and intelligent settings thanks to wireless sensor networks. For instance, wireless sensors may be used to wirelessly communicate readings from utility metres in a house, such as those for water, gas, and electricity, to a distant centre. The Wireless Sensor Network (WSN) is a young technology with a lot of potential for both civilian and military uses in the

future. It is profitable and will be widely used in the future thanks to wireless connectivity, computational power, and sensor technologies. Military, health, environmental, water, industries, the home, agriculture, and other fields are just a few of the many uses for WSNs. Security is the primary problem with WSNs, apart from these uses. WSNs are subject to a variety of attacks, including as wormhole, sybil, selective forwarding, and impersonation attacks. We provide an overview of WSN applications, as well as various attacks and their defenses, in this study.

Declarations

Source of Funding

This study did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional, or personal interests.

Consent for publication

The authors declare that they consented to the publication of this study.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam & E. Cayirci (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8): 104–112.

[2] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai & K. Frampton (2004). Sensor network-based countersniper system. In Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD.

[3] J. Yick, B. Mukherjee & D. Ghosal (2005). Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm. In Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston.

[4] M. Castillo-Effen, D.H. Quintela, R. Jordan, W. Westhoff & W. Moreno (2004). Wireless sensor networks for flash-flood alerting. In Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic.

[5] T. Gao, D. Greenspan, M. Welsh, R.R. Juang & A. Alm (2005). Vital signs monitoring and patient tracking over a wireless network. In Proceedings of the 27th IEEE EMBS Annual International Conference.

[6] R.W. Clay, N.R. Wild, D.J. Bird, B.R. Dawson, M. Johnston, R. Patrick & A. Sewell (1998). A cloud monitoring system for remote sites. Publications of the Astronomical Society of Australia, 15(3): 332–335.

[7] A. El-Hoiydi (2002). Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks. In Proceedings of IEEE International Conference on Communications, New York, NY, USA.

[8] D. Estrin, L. Girod, G. Pottie & M. Srivastava (2001). Instrumenting the world with wireless sensor networks. In International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), Salt Lake City, UT.

[9] D. Estrin, R. Govindan, J.S. Heidemann & S. Kumar (1999). Next century challenges: Scalable coordination in sensor networks. Mobile Computing and Networking, Pages 263–270.

[10] Fakhrosadat Fanian & Marjan Kuchaki Rafsanjani (2018). Memetic fuzzy clustering protocol for wireless sensor networks: Shuffled frog leaping algorithm. Applied Soft Computing, 71: 568–590.

[11] Supreet Kaur & Rajiv Mahajan (2018). Hybrid meta-heuristic optimization based energy efficient protocol for Wireless Sensor Networks. Egyptian Informatics Journal, 19(3): 145–150.

[12] R. Logambigai Sannasi & Ganapathy A. Kannana (2018). Energy–efficient grid–based routing algorithm using intelligent fuzzy rules for Wireless Sensor Networks. Computers & Electrical Engineering, 68: 62–75.

[13] Madiha Razzaq, Devarani Devi Ningombam & Seokjoo Shin (2018). Energy Efficient K-means Clustering-Based Routing Protocol for WSN Using Optimal Packet Size. IEEE, 1: 632–635.

[14] Nosratinia, A., Hunter, T.E., & Hedayat, A. (2004). Cooperative communication in wireless networks. IEEE Commun. Mag., 42: 74–80.

[15] Li, Q., Hu, R.Q., Qian, Y., & Wu, G. (2012). Cooperative communications for wireless networks: Techniques and applications in LTE advanced systems. IEEE Wirel. Commun., 19: 22–29.