ISSN: 0974-5823 Vol. 7 No. 5 May, 2022

International Journal of Mechanical Engineering

Wireless Sensor Network Techniques and its Role in Internet of Things: An Overview

1. Dr K. J. Praveen Kumar

Assistant Professor, Department of Computer Science,

Gobi Arts & Science College (Autonomous)

Gobichettipalayam - 638453

2. Dr. K. Divya

Assistant Professor , Department of information technology,

Bharathidasan college of Arts and Science , Ellispettai, Erode.

3. Dr M. Sathyapriya

Assistant Professor, Department of Computer Science,

Gobi Arts & Science College (Autonomous)

Gobichettipalayam - 638453

4. Dr. T .K. Sumathi

Associate Professor, Department of Computer Science

Gobi Arts & Science College (Autonomous)

Gobichettipalayam - 638453

Abstract

In recent years, it has been observed that wireless systems dependent on the Internet of Things have evolved rapidly in a variety of industries. The Internet of Things, sometimes known as IOT , is a network that allows physical devices, equipment, sensors, and other items to communicate with one another independently of the intervention of humans. The Internet of Things (IOT) has mushroomed into a variety of various real-time applications thanks in large part to a key component known as the Wireless Sensor Network (WSN). The Internet of Things (IOT) and wireless sensor networks (WSNs) today have a variety of applications, both critical and non-critical, that influence practically every facet of our day-to-day lives. WSN nodes are typically very small machines that are powered by batteries. Consequently, the methods of data aggregation that consume less energy while simultaneously extending the lifespan of the network are of the utmost importance. In this presentation, a variety of strategies and methods for data aggregation in IOT -WSN systems that are efficient with energy use were discussed. The purpose of this research is to conduct a literature review, paying particular attention to areas of wireless networking that are concerned with the conservation of energy and the accumulation of data.

Keywords: wireless systems, Internet of Things, Industries, Wireless sensor networks, conservation of energy etc

Introduction

Since the invention of wireless networking technology, a number of significant shifts have taken place across the board in every facet of our regular lives. The Internet of Things (IOT), in particular, is expected to be one of the technologies with the quickest rate of development in the future. With the addition of IOT, several gadgets in the real world can be coupled with one another, which fundamentally alters our lives on a daily

basis. As a result, there is a rapidly growing demand for larger levels of communication all the time and in all places, particularly in spheres of endeavour that are becoming increasingly active.

Traditionally, integration and communication amongst intelligent items have been seen as constituting the IOT (things). The dominance of IOT contributes to the development of new technologies and applications. It is common for these devices to be equipped with a range of transceivers as well as microcontrollers and protocols that allow for the transfer of control and sensor data. This includes devices like as domestic appliances and surveillance cameras. In order to transfer the data they have collected to the central repositories, these real-time modules, such as sensors, are linked together. These repositories are where the data is accumulated and can be accessed by people who have been granted permission to do so. Because of the large number of communication devices, the characteristics of IOT systems that make use of wireless technologies are relatively distinct when compared to the characteristics of ordinary wired or wireless networking systems. IOT traffic isn't often deemed significant because each IOT device senses and transmits some data to a specific Internet of Things (IOT) Server. Thus, data generated by several items may have an impact on the overall performance of the network. IOT networks will be able to operate without human intervention for a long period of time since they are secure and sustainable. The heterogeneous wireless sensor networks (WSN) that link a wide variety of intelligent sensors have formed the foundation for the Internet of Things (IOT)-based technologies that are all around us and will soon introduce major improvements. The rapid growth of these technologies has led in issues with energy usage, which have become more appealing. On the one hand, the dramatic increase in the speed of communication and the dissemination of information has contributed to unsustainable increases in the amount of energy utilised and carbon emissions. On the other hand, in the vast majority of applications, it is necessary for the sensor nodes to function effectively for extensive amounts of time, often even years, and to fulfil a wide range of application requirements (such as for environmental control and protection, agriculture, border surveillance and protection, etc.). The quantity of energy that is used up by the sensors is the primary factor that determines how long the application will continue to function, and the existence of dead nodes can have an impact on the interoperability of devices in addition to the dependability and accuracy of data. In spite of this, the following four primary units are commonly included in the construction of a sensor node:

- the processing unit,
- the sensing/identification unit,
- the communication unit and
- the power supply unit,

It is shown in Fig. 1.

Secondary components, such as filters, amplifiers, transducers, comparators, and so on, are included in each of the previously stated components. The sensing device collects and senses data from the workplace. Among the many functions of the processing unit is data collecting and other forms of data manipulation. Contrary to this, data transmission at the base stations (BS) is the responsibility of the communication unit, while all other devices receive power from the power unit (which is often restricted by battery life).

A sensor node will need a certain amount of energy when it is active, sleeping, or idle. This amount of energy consumption will vary depending on the operational environment. When the node is operating in its active state, it has the greatest appetite for energy. In order for the sensor to have the greatest potential for energy output, it consumes the absolute minimum amount of power necessary for the transmission and receiving of information. Even while it uses a lot less electricity than the radio subsystem, the processor unit nevertheless uses a lot more electricity than the sensor subsystem. There are other factors that come into play, including the communication distance, the monitoring case, the operational criteria, and the activities that take place in each unit. During the idle mode, a node waits for data packets from another node to arrive. Due to the increased energy consumption (by CPU and radio, for example) it is feasible that between fifty and one hundred percent of the total energy wasted through data reception can be accounted for. In sleep mode, the node does not process any data and the communication unit is turned off. As a result, the node loses a much lower amount of energy while it is sleeping. As a matter of fact, there are a number of other kinds of energy loss, including frame overheating, channel failure, lost packets, and so on and so forth. This has driven the IOT group to develop IOT solutions that are both renewable and energy efficient.

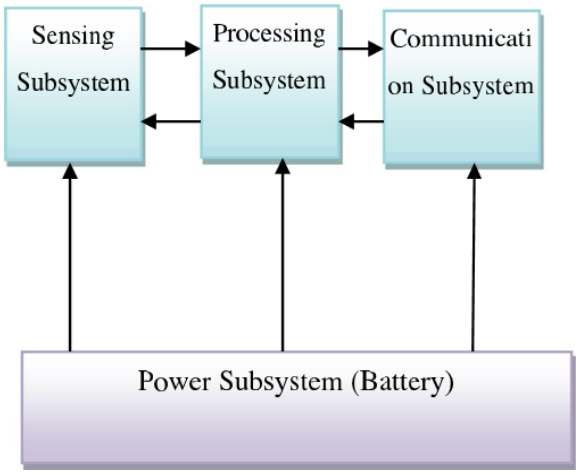

Fig.1. A typical IOT-based sensor node architecture.

The administration of these IOT networks is naturally concerned about energy efficiency, because battery energy sources are often used to operate devices. The cost of battery power is a consideration. For a long time, battery-powered sensor nodes' energy efficiency and life extension have been issues for researchers in a specific WSN domain. Sensor node functioning is prioritised by MAC protocols, while routing layer protocols are designed to aggregate and transport data from multiple-to-one. Here, a review of wireless networking's energy conservation and data collection components is offered in light of this, with a specific focus on these aspects of wireless networking.

2. Role of IOT in WSN

Several research papers and studies have provided support for significant classification opinions and surveys of WSN and IOT based energy-saving devices. Throughout the course of this section, we will examine a selection of these significant literary works, which will provide an overview of their primary concerns and the various categories described by them:

According to the findings of the research, the Chaotic Whale Optimization Process could be an effective method for increasing the efficiency with which WSN-IOT environmental operations utilise energy. We were able to acquire the findings of energy efficiency in comparison to other more conventional methods. In the WSN-IOT integrated system, the results indicated that the proposed approach provides superior energy efficiency than other approaches.

Latencies, energy consumption, jitters, throughput, and packet-delivery ratios (PDR) were the focus of the research that was carried out with regard to WSN. In addition, the effectiveness of routing protocols was evaluated by utilising delay, bandwidth, jitter, and delay as test parameters. It was agreed that an algorithm should be developed.

Several research papers and studies have provided support for significant classification opinions and surveys of WSN and IOT based energy-saving devices. Throughout the course of this section, we will examine a selection of these significant literary works, which will provide an overview of their primary concerns and the various categories described by them:

An IOT-based solar-powered precision agricultural (PA) network with the WSN was designed and implemented as part of this paper's mandate to identify highly effective means of implementing a smart agriculture management system. In the paper, the design and the accomplishment were described. Farmers were shown a system that supplied useful data in an easy-to-use manner, including real-time data transmission via IOT concerning saltwater intrusions, soil moisture levels, water levels, wet conditions, temperature, and an overall assessment of the land's condition.

The authors of presented a study that focused on the gathering of IOT data as well as the various decision-making principles. The writers of also presented their findings. The results of an operational and maintenance

assessment of photovoltaic (PV) systems and wireless sensor networks (WSNs) based on Internet of Things technology for the monitoring of PV panels were provided in that paper.

According to the findings of the research, the Chaotic Whale Optimization Process could be an effective method for increasing the efficiency with which WSN-IOT environmental operations consume energy. We were able to acquire the findings of energy efficiency in comparison to other more conventional methods. The findings showed that the proposed method produces higher levels of energy efficiency inside the WSN-IOT integrated system.

The study was conducted on the latencies, energy, jitters, throughput, and packet-delivery ratios (PDR) from the perspective of WSN. Additionally, the performance of routing protocols was tested utilising delay, bandwidth, jitter, and delay. In order to make AODV routing in IOT more efficient, an algorithm was developed. In order to optimise the protocol, two separate tables—the table of routing, and the table of internet access—were combined into a single table. This study's primary objective was to conduct an analysis of simulation studies pertaining to the IOT AODV routing protocol and to make use of the NS2 simulator in order to enhance the performance of both AODV and IOT AODV. The most recent version can be downloaded here.

Also, because WSN-assisted IOT has so many drawbacks, it is not viable to employ conventional routing protocols in a direct manner. The consumption of energy by IoT devices that are supported by WSN is a serious limitation. It takes more power to communicate between sensor nodes than it does to actually do the sensing and computing. As a result, methods of efficient energy management are very necessary in order to lengthen the life of the network. An energy-conscious multi-user and Multi-Hop Hierarchical Routing Protocol (EAMMH-RP) was proposed by the author in the paper. This protocol covers Communication with Multi-Hop and makes sure that sensor nodes in a cluster formation all get the same amount of energy. The author also suggested a new set of algorithms for adapting and rotating clusters, as well as a new way to reduce the amount of energy needed for long-distance communications.

The sensors can be utilised to monitor the environment and continue to return information for a longer period of time. It was proposed that IOT sensing networks use a protocol that incorporates a resilient routing mechanism. In the beginning, a rendezvous area was constructed right in the middle of the network field. We made use of the clustering and multipath tactics because doing so reduces the amount of energy that is consumed and increases the level of dependability. The introduced protocol was simulated in the Castalia simulator in order to achieve efficiency under various scenarios, such as packet transmission, average energy usage, end-to-end latency, and network lifetime. This was done in order to achieve efficiency.

A number of performance metrics, including latency, energy usage, and data delivery ratio, were taken into consideration when developing the routing algorithms and models used in this research. IOT and WSN algorithms based on IOT were classified into two groups for the sake of ease of use for researchers. These classes included energy awareness, latency, data transfer, and packet loss awareness.

The study improved upon the standard routing protocol and presented a novel protocol with novel characteristics such as a new data transmission system and a better technique of selecting CHs. Additionally, the conventional routing protocol was optimised. Therefore, there was a connection between the WSNs' shortcomings in the real world and the actual diverse situation. The outcome of the simulation, which was determined with the assistance of performance measurements, highlighted the disparity between the currently implemented HY-IOT and the predicted protocol.

3. Challenges of WSN in IOT

The complexity of the Internet of Things is achieved through the presentation and communication of a variety of heterogeneous artefacts in a variety of circumstances, which further complicates the deployment of security systems. The majority of the solutions that are offered in existing WSN security research are aimed at resolving subjective problems, and they do not take into account the influence of the IOT concepts and features that are discussed in this document.

3.1. Real time management

It is a challenging topic for sensor networks that govern their available resources. In this scenario, the Internet of Things (IoT) system requires an effective design for its service gateway in order to reduce the amount of data that must be transmitted by continuously analysing user data. Additionally, an intelligent data-driven middleware design is required in order to communicate real-time information only when the threshold is exceeded.

3.2. Security and privacy

In applications that are used in the real world, safety, trust, and privacy are other challenges that are vital to consider. The path to achieving varying levels of safety can be challenging as well as straightforward. These security solutions are appropriate for M2M deployments in which the device and the server already have an established trust relationship with one another. [30]

With this "IP to the field" approach, sensor nodes have extra obligations in addition to the standard sensor functions they provide. As a result of this added obligation, the sensor nodes will be faced with new responsibilities or difficulties. The topics of network setup, service quality (QOS), and security will be discussed as potential future responsibilities. The following issues are taken into consideration.

3.3. Security

Depending on the level of complexity of the application, WSNs may be able to provide data with confidentiality, verification, fairness, and usability even in the absence of Internet connectivity. For the attacker to be successful in adding malicious nodes to the current network or in blocking or catching them, they need to engage in physical activities in close proximity to the WSN. The connection of WSNs to the internet, on the other hand, makes it possible for malicious actors located anywhere in the globe to carry out their schemes. Because of this, the WSNs need to find a permanent solution to the problems that are caused by their connection to the internet, such as malware and other problems. To ensure that present WSNs maintain an adequate level of security, both the key and a specialised effective gateway are made available. A similar security system can't be duplicated due to the limited processing power, energy, and memory resources available today. Other Internet networks have implemented cryptography with longer key lengths such as RSA-1024, but sensor nodes supposed to give greater privacy have not. Furthermore, in order to guard against the plethora of dangers that the Internet may bring, it is critical that any new security measures take account of the multiple resource restrictions already in place.

3.4. Quality of service

In terms of the intelligence that is provided to the sensor nodes, each disparate device that is connected to the internet of things is required to make a contribution to the overall quality of service. These heterogeneous devices enable a workload to be distributed among multiple nodes, each of which has access to a certain set of resources. Due to the ever-changing configurations of networks and the varied capabilities of links, the currently available QOS approaches on the internet still need to be improved.

3.5. Configuration

In addition to managing QOS and ensuring network security, sensor nodes must also manage a variety of other tasks. These tasks include networking for a new node that is joining the network, ensuring self-healing by locating and removing faulty nodes, and addressing management for the construction of scalable networks, among other things. However, self-configuring the most recent node on the Internet does not do this action as a normal function. Therefore, the user is responsible for installing the necessary software and taking the necessary precautions to prevent device failures if they want this network configuration to perform well.

3.6. Availability

The presence of hacked nodes makes it possible to take advantage of WSNs. Additional funds should be budgeted in order to implement an encryption technique for wireless sensor network security. In spite of this, researchers have created major approaches, some of which include modifying the code in order to reuse it, while others involve using supplemental communications in order to achieve the aims. In addition to this, several methods have been developed in order to access the data. Therefore, the necessity for availability is absolutely necessary in order to maintain the operating services of WSN's. Additionally, it contributes to the maintenance of the entire network up until the point where it is shut down.

3.7. Data integrity

The integrity of a WSN may be jeopardised if a hostile node joins the network and injects erroneous data or if a fluctuating wireless channel corrupts the data that was first transmitted. For instance, the integrity of the data could be compromised if a mobile node were to add forged information to the packets that the base station (BS) was processing. Nevertheless, a malfunctioning network may be to blame for the loss of data or the change of data. As a result, it is imperative that the integrity of the data be preserved all the way through the transmission of the data packets.

3.8. Confidentiality

When it comes to Internet of Things security, there are several obstacles to overcome, the most important of which is maintaining secrecy. Encryption functions, such as common and shared secret key encryption techniques, such as the Blowfish, AES block cypher, and Triple DES, are utilised in order to maintain the data's secrecy and prevent unauthorised access. However, the encryption process is not adequate on its own as a security technique to ensure the confidentiality of the data and information being transmitted. The attacker is able to perform a traffic analysis for the cypher data in order to effectively disseminate sensitive material by exploiting a vulnerability in the cypher. In addition to this, the rogue node has the potential to effectively compromise the.

4. Data aggregation

WSNs are fundamental building elements for the Internet of Things, and their use in a wide variety of real-time applications has led to their proliferation. WSN nodes are typically very small devices that operate off of batteries. As a result, one of the most important factors to think about while aggregating data from WSNs is the stability of the network. During the process of collecting data, a number of issues, including higher energy consumption, sometimes known as energy inefficiency, and an increased lifespan, were discovered.

In order to maintain an appropriate level of servicing efficiency in the distribution of sensed data, data aggregation algorithms are utilised extensively. The goal of the software that collects data is to properly incarcerate and distribute data packets in order to reduce the amount of energy used, the amount of traffic congestion on the network, the amount of time the network is expected to live, and other factors. As a result, several other approaches were suggested for use in this industry, some of which are outlined below:

5. Conclusion

Increasing computer technology has helped WSNs, which are always aware of the necessary requirements, rise in popularity. The WSN systems based on the Internet of Things (IOT) have received a lot of interest recently. However, when transmitting point-to-point, these systems are limited in bandwidth, power, and resources. An excellent way to deal with this issue is to collect data on the subject. Sensor networks have the challenge of processing critical data in a way that is both efficient and cost-effective. There are a variety of power-saving data aggregation methods discussed in this study. Previous studies that have attempted to define the function of IOT in WSN are summarised in this paper, followed by an examination of the various data aggregation methodologies offered in those studies. For energy conservation, better QoS, and a higher level of network security, data aggregation techniques are used.

References

A. Alkhamisi, M.S.H. Nazmudeen, S.M. Buhari, ‘‘A cross-layer framework for sensor data aggregation for IOT applications in smart cities”,, IEEE International Smart Cities Conference (ISC2), Trento 2016 (2016) 1–6, https://doi.org/ 10.1109/ISC2.2016.7580853.

A. K. Idrees, W. L. Al-Yaseen, M. A. Taam and O. Zahwe, ‘‘Distributed Data Aggregation based Modified K-means technique for energy conservation in periodic wireless sensor networks,” 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, 2018, pp. 1-6, doi: 10.1109/MENACOMM.2018.8371007.

1. A.S. Abdul-Qawy, P.P.J.E. Magesh, T. Srinivasulu, The Internet of Things (IOT): An Overview, Int. J. Eng. Res. Appl. (IJERA) 5 (12) (2015) 71–82.

B. Luo, F. Wu, J. Sun, and C. W. Chen, ‘‘Compressive data gathering for largescale wireless sensor networks,” in Proc. 15th ACM MobiCom, pp. 145-156, 2009

2. Emma Fitzgerald, Michal Pioro, Artur Tomaszwski, Energy-Optimal Data Aggregation and Dissemination for the Internet of Things, IEEE Int. Things J. 5 (2) (2018) 955–969, https://doi.org/10.1109/JIOT.648890710.1109/ JIOT.2018.2803792.
3. F. Arat, S. Demirci, ‘‘Energy and QoS Aware Analysis and Classification of Routing Protocols for IOT and WSN,” 2020 7th International Conference on Electrical and Electronics Engineering (ICEEE), Antalya, Turkey, 2020, pp. 221225, doi: 10.1109/ICEEE49618.2020.9102614
4. G. Thangarasu, P. D. D. Dominic, M. bin Othman, R. Sokkalingam and K. Subramanian, ‘‘An Efficient Energy Consumption Technique in Integrated WSN-IOT Environment Operations,” 2019 IEEE Student Conference on Research and Development (SCOReD), Bandar Seri Iskandar, Malaysia, 2019, pp. 45-48, doi: 10.1109/SCORED.2019.8896238
5. H. Rahman, N. Ahmed, M.I. Hussain, A hybrid data aggregation scheme for provisioning Quality of Service (QoS) in Internet of Things (IOT),‘‘ Cloudification of the Internet of Things (CIOT), Paris 2016 (2016) 1–5, https://doi.org/10.1109/CIOT.2016.7872917.
6. H.M., FahmyWireless Sensor Networks: Concepts. Applications, Experimentation and Analysis, Signal and Communication Technology, Springer, 2016.
7. H.W. Kim, D. Kyue, Technology and Security of IOT, J. Korea Instit. Informat. Secur. Cryptol. 22 (1) (2012) 7–13.
8. K. Begum, S. Dixit, ‘‘Industrial WSN using IOT: A survey,” 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 499-504, doi: 10.1109/ICEEOT.2016.7755660.
9. K.I. Kim, ‘‘Clustering Scheme for (m, k)-Firm Streams in Wireless Sensor Networks,” the Journal of information and communication convergence engineering, vol.14, no. 2, pp. 84-88, 2016
10. M. Healy, T. Newe, E. Lewis, Wireless Sensor Node hardware: A review, in: 2008 IEEE Sensors, 621-624, 2008.
11. M. Priyanga, S. Leones Sherwin Vimalraj, J. Lydia, ‘‘Energy Aware Multiuser & Multi-hop Hierarchical –Based Routing Protocol for Energy Management in WSN-Assisted IOT,” 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 701-705, doi: 10.1109/CESYS.2018.8724073
12. M. S. Islam, G. K. Dey, ‘‘Precision Agriculture: Renewable Energy Based Smart Crop Field Monitoring and Management System Using WSN via IOT,” 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/STI47673.2019.9068017
13. N. Kaur, S.K. Sood, An Energy-Efficient Architecture for the Internet of Things (IOT), IEEE Syst. J. 11 (2) (2017) 796–805.
14. N. Mahakalkar, R. Pethe, ‘‘Review of Routing Protocol in a Wireless Sensor Network for an IOT Application,” 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 21-25, doi: 10.1109/CESYS.2018.8723935
15. R. Prakash, P. Kansal, V. K. Kakar, ‘‘Optimized Hybrid Clustered Protocol for IOT Heterogeneous Wireless Sensor Networks,” 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.9066258

16. Rakesh Kumar Lenka, Amiya Kumar Rath, Suraj Sharma, Building Reliable Routing Infrastructure for Green IOT Network, IEEE Access 7 (2019) 129892– 129909, https://doi.org/10.1109/Access.628763910.1109/ACCESS.2019.2939883.
17. S. Sarkar, K. U. Rao, J. Bhargav, S. Sheshaprasad and A. Sharma C.A., ‘‘IOT Based Wireless Sensor Network (WSN) for Condition Monitoring of Low Power Rooftop PV Panels,” 2019 IEEE 4th International Conference on Condition Assessment Techniques in Electrical Systems (CATCON), Chennai, India, 2019, pp. 1-5, doi: 10.1109/CATCON47128.2019.CN004 View publication stats
18. S. Swathi, H. K. Yogish, ‘‘Efficient-CSDA (Consensus based) Approach to Achieve Secure Data Aggregation,” 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Msyuru, India, 2018, pp. 355-361, doi: 10.1109/ ICEECCOT43722.2018.9001390
19. S.A.H. Antar, N.M. Abdul-Qaw, S. Almurisi, S. Tadisetty, Classification of Energy Saving Techniques for IOT-based Heterogeneous Wireless Nodes, Procedia Comput. Sci. 171 (2020) 2590–2599.
20. X. Zhou, Green Communication Protocols for Mobile Wireless Networks Ph.D. thesis, University of Ottawa, 2017.
21. Y. Cho, M. Kim, S. Woo, Energy Efficient IOT based on Wireless Sensor Networks for Healthcare, Int. Conf. Adv. Commun. Technol. (ICACT) (2018).
22. Young-bok Cho, Sang-ho Lee, Sung-Hee Woo, ‘‘An Adaptive Clustering Algorithm of Wireless Sensor Networks for Energy Efficiency”, Journal of The Institute of Internet, Broadcast. Commun. (IIBC) 17 (1) (2017) 99–106.