WIRELESS SENSOR NETWORK (WSN), ITS TYPES, CLASSIFICATION AND IMBALANCED DATA: A SURVEY

Pragati Dwivedi, Assistant Professor, Department of Computer Science & Engineering, Ambedkar Institute of Technology for Handicapped (A.I.T.H.), Kanpur, India.

Abstract— The field of WSN has been undergoing rapid development over the course of the past several years. In order to facilitate low-cost wireless communication, a new type of network known as a wireless sensor network has been developed. This network is made up of hundreds or thousands of sensor nodes and a base station, also known as a sink. The nodes and the base station are dispersed around the area. The purpose of this work is to provide a brief introduction to the architecture of WSNs, as well as potential topologies and the crossbow tool for measuring physical parameters. After that, the paper describes the various forms of WSN and the applications that use them. The word "imbalance" refers to an uneven distribution of data into classes, which has a significant negative impact on the performance of classical classifiers; more specifically, the classifiers become biassed toward the class that has a larger amount of data. There will be multiple inequalities present in the data that is produced by wireless sensor networks. This review article is a respectable examination of the imbalance issue for wireless sensor networks and other application areas. It will assist the community in better comprehending the imbalance in data as well as the potential solutions to this problem.

Keywords— Wireless sensor networks (WSN), Sensor nodes, Sink node, Imbalanced data, Algorithm modification, etc.

I. INTRODUCTION

They create a WSN when they have a need to monitor a large physical region with a number of sensors. Sensor nodes that are wireless are equipped with processing, communication, and storage capabilities as well. They are able to measure various aspects of physical environments, including temperature, humidity, pressure, and the intensity of the light. As can be seen in figure 1, WSNs are made up of one sink node and a large number of sensor nodes that are dispersed throughout a vast region (the sensing field). Data can be transported from nodes to the base station using either a single hop or several hops of communication, and then from the sink to the user using the internet [1, 2, 3].

In recent years, the development of an effective blueprint for a wireless sensor network has emerged as a primary focus of research. A device that can respond to and detect any form of input from either the physical or environmental circumstances, such as pressure, heat, light, etc., is known as a Sensor. In most cases, the output of the sensor is an electrical signal that is then sent to a controller in order to undergo additional processing. An overview of several kinds of wireless sensor networks, their classification, different kinds of attacks, and different kinds of mobility and routing protocols are covered in this article.

According to the definition given in [28], a wireless sensor network (WSN) is a self-organizing and multihop network of wireless sensor nodes that are utilized to monitor and control physical phenomena. Sensor nodes, gateways (or base stations), and clients are the typical components that make up the WSN.

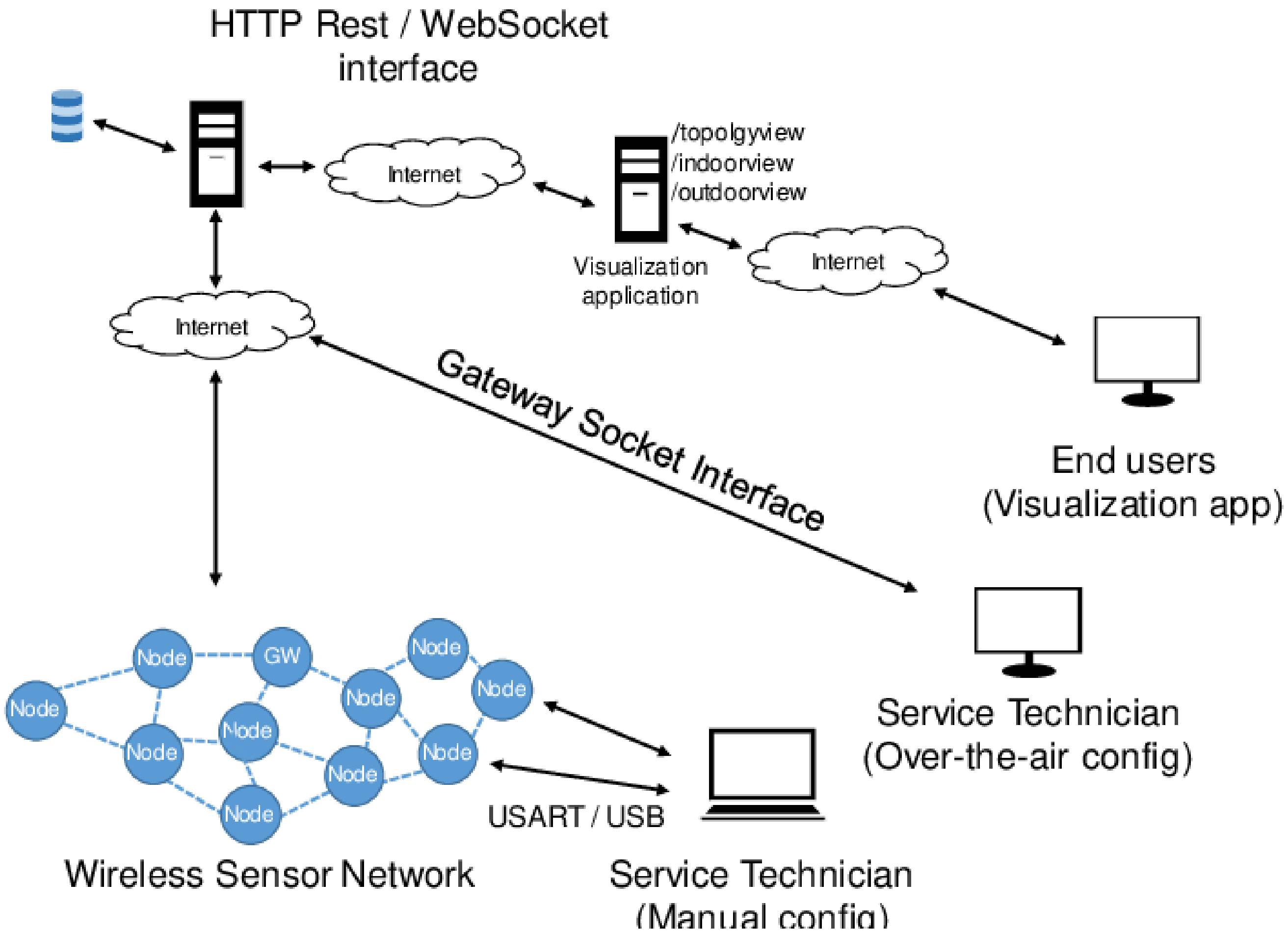

Figure 1: Structure of a wireless sensor network (WSN) system

SENSOR NODE

The wireless sensor node is responsible for converting the analogue data that was gathered from the sensor into digital data and then converting that digital data into a numerical value so that it is machine-readable. Additionally, it is responsible for sending this information to the gateway in order to fulfil its duty.

In this investigation, the chipset for a wireless sensor network that conforms to the IEEE 802.15.4e standard is utilized. The sensor nodes include a wireless transceiver, power supply, power management modules, and a microcontroller that is capable of receiving analogue signals from the sensors. Any sensor node that is positioned close to the interior of the monitoring area is able to participate in the formation of a network through the use of self-organizing functions thanks to the software that is built in the chipset. The data that has been gathered is monitored by the sensor node, and then utilizing hopping technology, it is transmitted to another sensor node. During the process of transmission, the monitoring data is processed by multiple nodes in order to reach the gateway node after being routed by multihopping.

GATEWAY

The gateway combines the functions of the wired and wireless communication modules in order to send data to the server. The gateway is responsible for collecting and processing the measurement data that is collected from the sensor node, and then transmitting the processed data to the final server. Long-term evolution (LTE), Bluetooth, and ZigBee are the three most common forms of wireless communication modules that can be found in sensors. An LTE module is utilized here for the sake of the study [4]. When the IP of the gateway is changed, the data server is notified so that it can maintain compatibility with the internet protocol (IP) modulation required for LTE security. The connection to the gateway is used to control the data collection performed by each individual sensor node.

NETWORK TOPOLOGY

Many sensor nodes in a WSN organize the connected networks according to a specific topology. Figure 2 shows the typical network topology [5-6]. The mesh type, star type, and tree type are mainly adopted in WSNs. For WSNs, the transmission distance among sensor nodes is short since they are battery-powered, so multihop transmission is used to extend the network range. In this study, a mesh topology with excellent flexibility and reliability and a time synchronized mesh protocol (TSMP) from Dust Networks, Inc. are applied to construct a multihop network with a low power consumption.

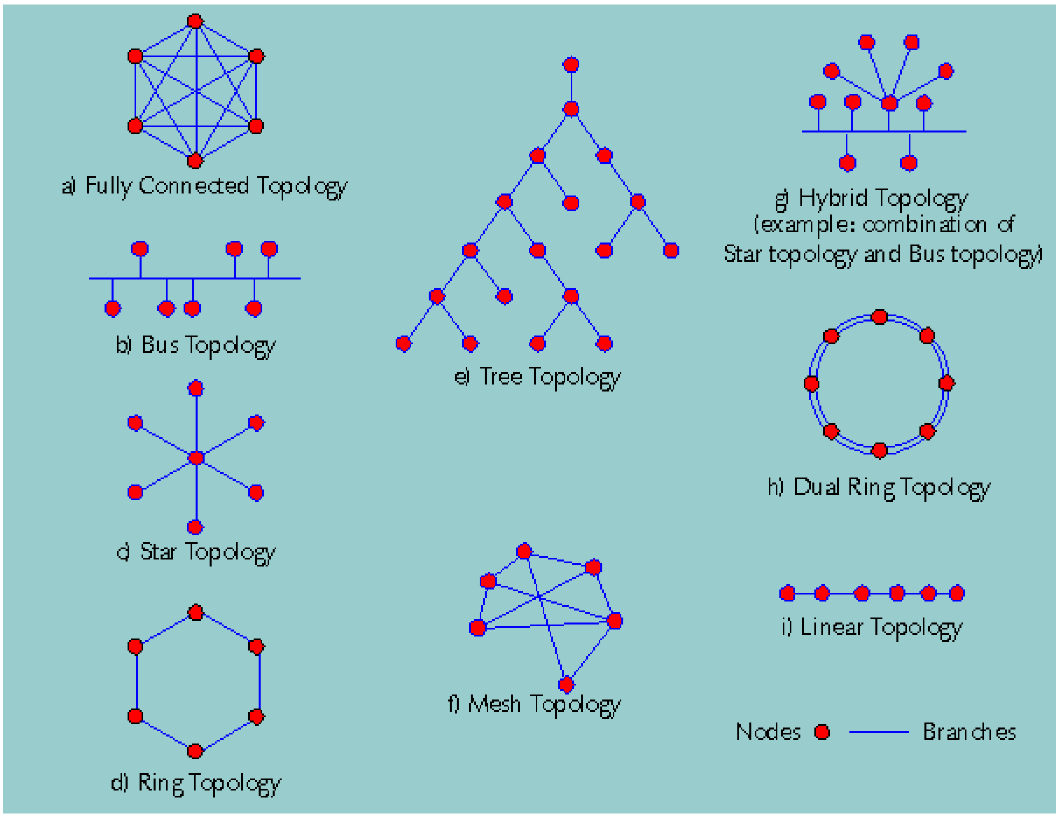

Figure 2: Typical network topology: (a) ring, (b) mesh, (c) star, (d) fully connected, (e) line, (f) tree, and (g) bus.

Star Topologies

A communication topology known as the star topology is characterized by each node's direct connection to a gateway. A message can be sent or received by multiple remote nodes through the use of a single gateway. It is forbidden for the nodes in an instar topology to communicate with one another via exchanging messages. This makes it possible for the remote node and the gateway to have communications with a low latency (base station).

Because it relies on a single node to run the network, the gateway needs to be located within radio transmission range of each individual node. This is necessary because the gateway is dependent on that node. The ability to maintain the power consumption of the remote nodes to a minimal and simple under control is one of the advantages of this system. The number of connections that are established to the hub determines the overall scale of the network.

Tree Topologies

Cascaded star topology is another name for tree topology, which is another name for tree topology. Each node in a tree topology connects to another node that is positioned higher up in the tree, and then those nodes connect to the gateway. The primary benefit of using a tree topology is that it makes error detection and network growth much simpler. Another advantage is that the tree topology makes it easier to expand a network. This network has the problem of being overly dependent on the bus cable; if that cable were to break, the entire network would be rendered inoperable.

Mesh Topologies

Within the radio transmission range of a node, the Mesh topologies enable the transfer of data from that node to any other node within the network. If one node wants to send a message to another node that is beyond the range of radio transmission, the sending node needs an intermediary node so that the message can be sent to the intended node. The capability of quickly isolating and locating problems in the network is one of the benefits offered by this mesh design. The fact that the network is so extensive and calls for such a significant financial investment is a significant drawback.

Bus Topologies

A topology for a computer network in which all of the nodes, also known as stations, are linked together by a single bus.

Fully Connected Topologies

A topology for a network in which every pair of nodes can be connected by an unbroken chain of branches. Take note that there are n(n-1)/2 direct paths, also known as branches, in a network that has n nodes and is fully connected. Similar to a completely interconnected mesh network.

Hybrid Topologies

A network topology that is the result of combining any two or more other topologies. Note 1: There are some circumstances in which two fundamental network topologies, when coupled together, can still maintain the fundamental network nature and, as a result, are not considered to be a hybrid network. A tree network that is connected to another tree network is still considered to be a tree network, for instance. Therefore, a hybrid network is only created when two basic networks are connected, and the resulting network topology does not satisfy the description of either of the fundamental topologies. As an illustration, hybrid network topologies can be seen in the form of two star networks that are connected to one another. Note 2: A hybrid topology will invariably result whenever two distinct fundamental network topologies are joined to one another.

Ring Topologies

A topology for a computer network in which every node is connected to exactly two other nodes.

Types of Wireless Sensor Networks

The kinds of networks that are used are determined by the environment, which allows for their use in a variety of settings, such as on land, underground, in water, and so on. There are several varieties of wireless sensor networks [7-8]:

- Terrestrial WSNs
- Underground WSNs
- Underwater WSNs
- Multimedia WSNs
- Mobile WSNs

Terrestrial WSNs

Terrestrial wireless sensor networks are effective at interacting with base stations and are made up of hundreds to thousands of wireless sensor nodes that can be set up in either an unstructured (ad hoc) or structured (Pre-planned) manner. When the mode is set to unstructured, the sensor nodes are dispersed at random within the target region, which is dropped from a stationary plane. When using the preplanned or structured mode, optimal placement, grid placement, and both 2D and 3D placement models are taken into consideration.

In this WSN, the power provided by the battery is restricted; nevertheless, the battery has solar cells that can be used as an alternative source of power. These WSNs are able to conserve energy by employing low duty cycle activities, reducing delays as much as possible, and utilizing efficient routing, amongst other strategies.

Underground WSNs

When deployment, maintenance, and equipment costs are taken into consideration, as well as the need for careful planning, the costs associated with underground wireless sensor networks are higher than those associated with terrestrial WSNs. The WSNs networks are made up of a number of sensor nodes that are buried beneath the surface in order to keep an eye on the environment below.

Additional sink nodes are placed in elevated positions above the ground in order to facilitate the transmission of data from the sensor nodes to the base station.

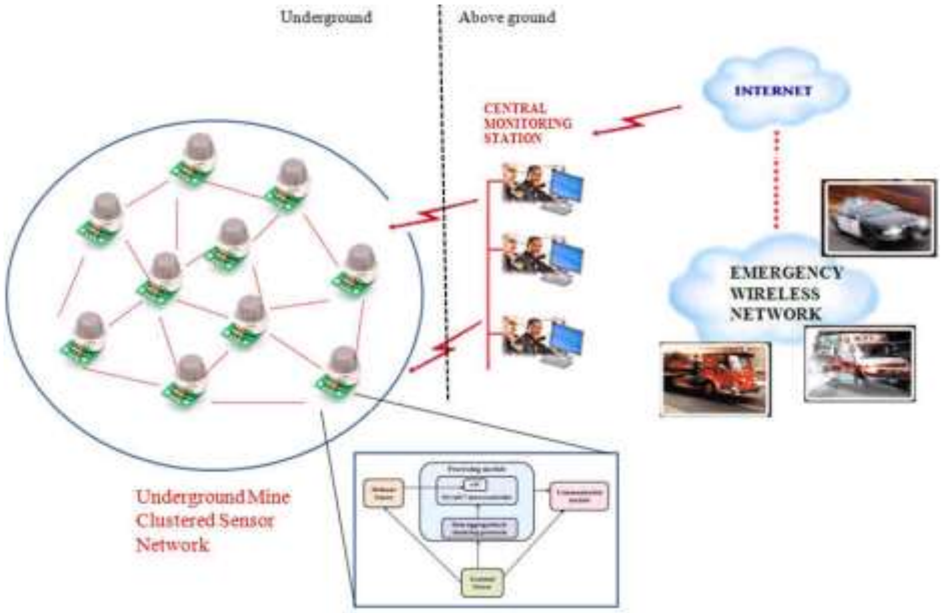

Figure 3: Underground WSNs

It is challenging to provide power to the underground wireless sensor networks that have been installed into the ground. It is difficult to replenish the sensor battery nodes because they only have a limited amount of battery power. In contrast to this, the underground environment poses a difficulty for wireless communication because of the significant amount of attenuation and signal loss that occurs there.

Under Water WSNs

More over 70 percent of the earth's surface is covered by water. These networks are made up of a number of sensor nodes and vehicles that are placed below the surface. For the purpose of data collection from these sensor nodes, autonomous underwater vehicles are utilized. A lengthy propagation delay, as well as bandwidth and sensor failures, are challenges that are unique to underwater communication.

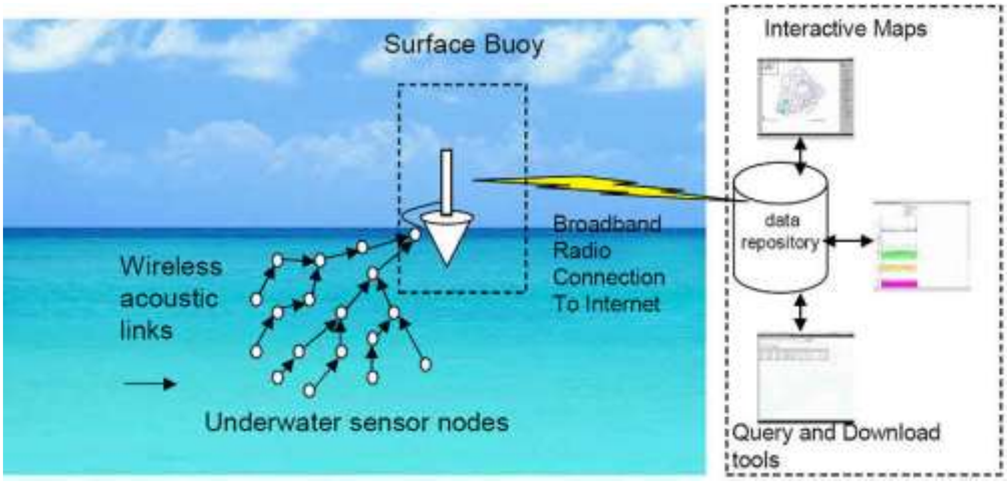

Figure 4: Under Water WSNs

Multimedia WSNs

It has been suggested that multimedia wireless sensor networks might be used to enable the tracking and monitoring of occurrences using various forms of multimedia data, including imaging, video, and audio. These networks are made up of low-cost sensor nodes that have both microphones and cameras attached to them. In order to facilitate data compression, data retrieval, and correlation, these nodes are wirelessly connected to one another and interconnected with one another.

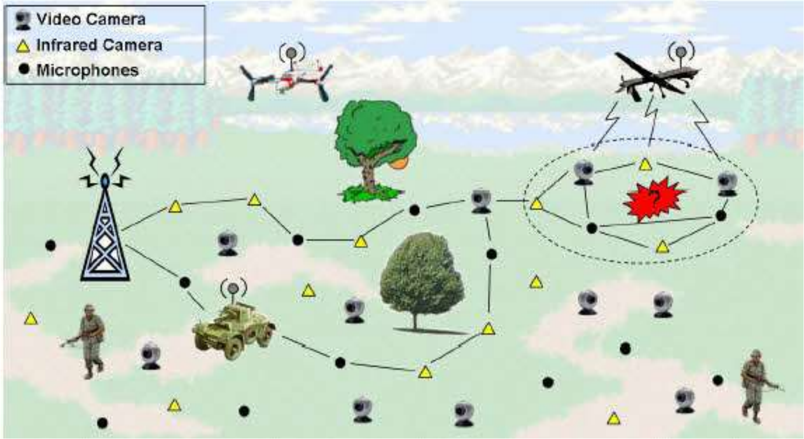

Figure 5: Multimedia WSNs

The multimedia WSN presents a number of issues, including a high energy consumption, high bandwidth needs, the need for data processing, and strategies for compressing data. In addition to this, the delivery of multimedia contents requires a high bandwidth in order to ensure that the content is received in an accurate and uncomplicated manner.

Mobile WSNs

These networks are made up of a collection of sensor nodes that are capable of moving around on their own and interacting with the environment around them physically. The mobile nodes are able to both compute and communicate with one another.

Mobile wireless sensor networks have a far greater degree of adaptability than static sensor networks. The advantages of mobile wireless sensor networks over static wireless sensor networks include greater and enhanced coverage, higher energy efficiency, superior channel capacity, and so on.

II. Related Work

In the past ten years, wireless sensor networks, also known as WSNs, have found widespread use in monitoring systems that are designed to regulate and monitor a variety of indoor premises, agricultural lands, and forest monitoring applications [9]. The proliferation of wireless sensor networks (WSNs) has given rise to concerns over the integrity of computer networks as a result of potential security breaches. Traditional security algorithms in WSNs have been successful in accomplishing a variety of security goals, including protection of base stations [9], cryptography [8], detection of attack attempts [9], and security location and routing [10-12]. A large number of researchers have created substantial solutions to solve the concerns raised by WSNs regarding their security. These sensors produce an enormous amount of data that needs to be processed and transmitted to the base station. Because of limits in power consumption, poor memory (storage capacity), communication capabilities, and resource constraints in sensors [13, 14], standard security algorithms are not appropriate for wireless sensor networks (WSNs).

Because of the high level of energy consumption in the network, one of the most significant challenges is the communication and exchange of information between sensors. This information needs to be shielded from the many dangers that could potentially affect it [15, 16]. Support for several security qualities, including confidentiality, authenticity, availability, and integrity, ought to be implemented in the networks in order to ensure their safety. The vast majority of these sensors do not have any form of physical security, which results in compromised nodes. If an attacker is able to compromise one or more nodes in a network, they will have the ability to conduct a variety of assaults that will disrupt the communication between networks [17]. There are many different types of assaults, including adversary, hacked node(s), eavesdropper, and so on [18]. These kinds of assaults can cause packets to be lost or modified, which has the effect of degrading the performance of wireless sensor networks (WSNs). Source location privacy, often known as SLPs, refers to systems that generate phoney nodes in order to shield sensor data from being attacked. The false node and packets, also known as the dummy message, are responsible for the creation of phoney identities and packets, both of which omit any mention of the source or destination identities. This approach has the disadvantage of requiring a greater expenditure of both energy and overhead [17, 18].

Middleware has been recently incorporated into WSNs in order to overcome some of the difficulties that were previously mentioned. In reference number 4, the authors examined and talked about a variety of middleware strategies, including SOMM, USEME, ESOA, and MiSense. The vast majority of middleware approaches do not have a security mechanism, which makes it impossible to protect the network and critical data from harmful attacks. In addition, middleware applications have been developed in order to implement machine learning (ML) methods. The study that was described in [19] utilized a method of unsupervised learning that is known as self-organizing map, and it was applied to WSN. The authors of [20] introduced SOM as a solution to the issue of detecting network attacks on ad hoc networks, which was one of their primary concerns. The SOM has the disadvantage that it is not suited for detecting assaults in complicated and huge datasets, which are frequently utilized in WSNs. This is a limitation of the SOM. The challenge of ontology heterogeneity was addressed by the machine learning middleware known as MaML. However, the overhead is something that could be considered a potential issue with MaML. Because of the requirements placed on the system's architecture, the dynamic behavior of a WSN has been continuously optimized. Machine learning (ML) strategies are implemented in wireless sensor networks (WSNs) so that there is no longer a requirement for an unnecessary redesign of the network. Machine learning is referred to by the creators of sensor networks as both an algorithm and a collection tool that is utilized in the process of developing prediction models. In order to extend the lifespan of the network, ML enhances the distribution, usage, and delegation of available resources. Machine learning employs mathematical models that are founded on statistical methods as a means of data sampling for artificial intelligence. It is able to acquire new knowledge and adjust its behavior in response to the ever-changing environment [21]. Applications that use WSN make significant use of the interface mechanisms that are available in ML. The processing of data, the aggregation of data, and the interfacing of ML are the three processes that are required to complete the process [3]. Monitoring and modelling the dynamic environments that are related with WSNs are accomplished with the help of these stages.

To generate prediction models, machine learning is utilized, and the resulting algorithms can be broken down into three categories: supervised learning, unsupervised learning, and reinforcement learning. The data sample, also known as the training set, must first be labelled in order for supervised learning to take place. Several difficulties that are unique to WSNs, including data aggregation, localization, grouping, energy awareness, detection, and real-time routing, have been successfully tackled by machine learning methods such support vector machine (SVM), decision tree (DT), and K-nearest neighbor (K-NN). Several different machine learning techniques that solve the security issues that plague WSNs are presented in the aforementioned research. Bayesian belief networks were used by Janakiram et al. [19] to demonstrate the ability to identify outliers (BBNs). The authors performed a correlation analysis on the temporal and spatial data points in order to locate readings that were comparable in surrounding nodes. These measurements are approximations that are then compared to one another in order to identify any potential anomalies in the data that was collected from sensor nodes. When developing conditional relationships, one must not only search for data points that deviate from the norm but also attempt to complete any gaps in information. A method for detecting outliers within a network that makes use of k-nearest neighbor was developed by Branch et al. [20]. This method is quite similar to the analysis of k-nearest neighbor that was provided in [21]. However, utilizing the k-nearest method comes with a number of significant drawbacks, the most significant of which is the requirement of a sizable memory space to store the data.

III. Perspectives and Study Objectives

The need of ensuring that data transmissions are kept private and safe has ballooned in recent years as a direct result of the rapid proliferation of wireless sensor networks in commercial, medical, and military settings. Recent research has pointed to the importance of middleware in wireless sensor networks (WSNs). Regrettably, many of these systems do not solve the security problem, which results in communication and data transmission that are not secure. Generally speaking, such data is sensitive, and as such, it needs to be protected against assaults as well as the dangers of exposure. This study was inspired by the constraints of the currently available middleware for wireless sensor networks (WSNs), and it is based on the following reasons to increase the performance of WSNs middleware:

- The methodologies that are proposed offer a one-of-a-kind WSN middleware that has the ability to control and monitor sensor data by employing intelligent, unsupervised machine learning to secure the data. It is possible to enhance the power consumption as well as the overhead by filtering out unneeded information from the sensors and performing regular updates. The unsupervised learning approach that has been proposed for middleware is one way to solve this challenge.
- They offer an unsupervised learning algorithm that delivers an all-encompassing security method that is able to manage large-scale WSNs. The GANs method is highly effective and features sophisticated generator and detector networks that operate according to the rules of game theory. The usefulness of the robust generator model, denoted by the letter G, is demonstrated by this body of work.
- The generator network takes the samples that are provided and makes synthetic data that is extremely similar to the genuine data. This bogus data is blended with the genuine data (from the sensors) so that the attackers cannot distinguish between the two sets of information. As a result, there is no requirement to generate bogus packets or data in order to throw off the attackers, which results in a huge reduction in the amount of power consumed.

IV. Imbalanced data in WSNs

Handling imbalanced data in classification is a significant obstacle that must be overcome in the process of data mining. It is common knowledge that one of the most essential methods of data mining is known as classification. In this method, samples of an unknown class are "classified" by applying prior information gained from training examples. An imbalance occurs when the data are distributed into classes in an unequal manner; certain classes may contain a huge quantity of data and be referred to as the majority class, while other classes may have just a few instances of data and be referred to as the minority class [22-23]. Because traditional classifiers take into account the error rate and not the distribution of the data, and because minority classes have a small quantity of data instances, they are ignored in the overall classification result. The biassed effectiveness of traditional classifiers is caused by this uneven distribution of the data. This problem manifests itself in a wide variety of real-world applications, including the healthcare industry, the detection of oil spills, the investigation of fraudulent use of credit cards, the modelling of cultures, the investigation of intrusions into computer networks, the classification of texts, and many more. The imbalanced statistics are depicted in figure 6, which is a representational picture.

Over the course of the past few years, a wide variety of different approaches have been presented as potential answers to this problem. Review papers of a high quality have been published in the past decade on imbalanced data and their related aspects. These papers contain information beginning with the definition of imbalance in data space, including the characteristics, types, and effect on classification performance, and ending with all of the possible ways to deal with the issue. In this regard, the papers have been published in the last decade. These study and review articles are extremely useful sources of information that can help one grasp the issue of imbalance in a more comprehensive manner. A comprehensive review of the relevant literature is revealing a vast amount of study and research on data inequalities. The examples that follow are some examples of popular research topics that deal with this natural instance of data distribution.

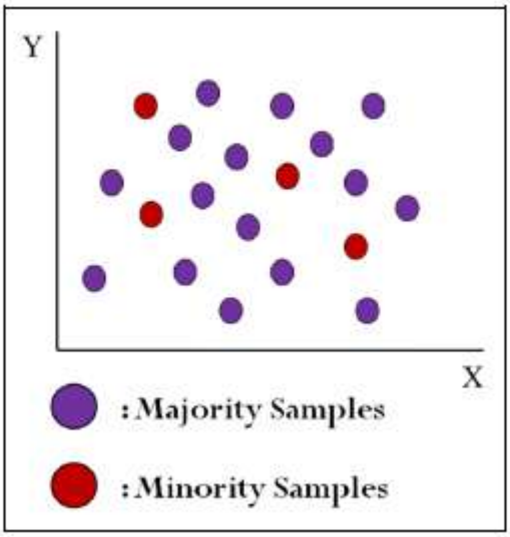

Figure 6: Imbalance in a binary dataset

WSN offers a variety of applications in fields such as medicine, agriculture, meteorology, the Internet of Things, and the detection of forest fires, among other fields. Even when studying the routing protocols for WSN, there is still a high probability that imbalanced data will be produced. Take, for example, the use of WSN in agricultural applications. Sensors for detecting soil moisture, location sensors, humidity detection sensors, temperature sensors, optical sensors, electrochemical sensors, airflow sensors, and other types of sensors are utilized in this application. If the temperature readings are being taken by sensors in a tropical nation, such as those found in Africa, then the majority of the time, the temperature will be on the upper side. As a consequence of this, while assessing the temperature data produced by these sensors, the weight will be skewed toward higher temperatures. Because there are fewer instances of low temperatures, conducting analysis connected to them in this scenario is challenging due to the fact that there are so few of them. In this section, we talk about the work that numerous academics have done to handle uneven data in wireless sensor networks (WSNs).

Techniques for dealing with unbalanced data in WSN

In this section, we will explore the lessons learnt concerning the handling of imbalanced data in WSN and the implications these lessons have. Handling of unbalanced data in WSNs has only been the focus of a very limited number of works. When data are continuously created by a broad variety of sensors, there is a possibility that the data generated from some of these sensors may be discrete; hence, the data generated from those sensors may be sparse. The dataset that is produced by these sensors as a result is unbalanced because of this. The extraction of patterns from datasets that are uneven can then become subject to bias. The following strategies, which have been utilized by a number of researchers for the purpose of controlling data imbalance in traditional datasets, can be applied to wireless sensor networks (WSNs) in order to deal with the kinds of scenarios that are described above [24-25].

- K-fold cross-validation is a method that is implemented throughout the training process for machine learning algorithms. During the phase of machine learning referred to as training, this method involves re-sampling the dataset. This method divides the datasets into k distinct categories to analyses them. The remaining groups are considered to be training data, whereas one of these groups will serve as the testing data. This strategy provides unequal or scarce data with the same level of attention as other data.
- Ensemble re-sampled datasets: This method involves re-sampling the dataset in such a way that the data that are scarce or unusual are oversampled. In this manner, the whole data may be brought into equilibrium, and the findings obtained through the application of machine learning algorithms will be accurate and objective.
- Decrease the weight of the traits that have a strong presence and raise the weight of the attributes that have a low presence: In this strategy, the importance of each attribute is taken into account. In order to achieve fair and balanced conclusions from the data, qualities that have a greater presence will be assigned higher weights, whereas attributes that have a lesser prevalence will be assigned a lower Patel et al. weight. In this manner, imbalances in datasets can be dealt with in an effective manner.
- Cost-sensitive learning: This strategy takes into account the costs of misclassification in data mining in order to reduce the overall cost as much as possible. This method does not involve the pre-selection of any hyper-parameters, instead modifying them in a dynamic fashion.
- Combined class methods: This strategy makes use of a combination of multiple different ways in order to properly manage imbalanced data. This method has the potential to get rid of the noise in unbalanced datasets. Taking this technique will prevent any potentially valuable information from being lost.

V. Conclusion

Wireless sensor networks, often known as WSNs, are an important data transmission medium that can be used in a wide variety of applications. The gap that exists between applications and WSNs can be bridged thanks to middleware, which helps handle issues related to power consumption, communication, and security. Rapid progress is being made in the transition of wired communication networks to wireless ones. On the other hand, wireless sensor networks (WSNs) are becoming increasingly popular in wireless networks and are an active topic of research. We have seen in this post that there are a number of different applications for WSN. In the beginning of the study, there was a brief overview of WSN architecture, as well as applications and problems. Following that, the paper discusses the numerous varieties of wireless sensor networks as well as their topologies. This article improves the foundation for this emerging field and subsequent ones; after that, we will select a specific problem in WSN and focus on developing an effective method.

References

[1] K. Bispo, N. Rosa, and P. Cunha, "SITRUS: Semantic Infrastructure for Wireless Sensor Networks," Sensors, vol. 15, no. 11, p. 27436, 2015.

[2] G. Xu, W. Shen, and X. Wang, "Applications of Wireless Sensor Networks in Marine Environment Monitoring: A Survey," Sensors, vol. 14, no. 9, p. 16932, 2014.

[3] S. Hadim and N. Mohamed, "Middleware for Wireless Sensor Networks: A Survey," in 1st International Conference on Communication Systems Software & Middleware, New Delhi, India, 8-12 Jan. 2006 pp. 1-7.

[4] R. Alshinina and K. Elleithy, "Performance and Challenges of Service-Oriented Architecture for Wireless Sensor Networks," Sensors, vol. 17, no. 3, p. 536, 2017.

[5] J. Al-Jaroodi and A. Al-Dhaheri, "Security issues of service-oriented middleware," International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. PP.153-160, 2011.

[6] A. Shchzad, N. Hung Quoc, S. Y. Lee, and L. Young-Koo, "A comprehensive middleware architecture for context-aware ubiquitous computing systems," in Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05), Jeju Island, South Korea, 14-16 July 2005, pp. 251-256.

[7] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks” 0163-6804/02/$17.00 © 2002 IEEE

[8] Mohd Fauzi Othman, Khairunnisa Shazali, “Wireless Sensor Network Applications: A Study in Environment Monitoring System” International S ymposium on Robotics and Intelligent Sensors 2012.

[9] Halil Yetgin, Kent Tsz Kan Cheung, Mohammed El-Hajjar “A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks” IEEE communication & tutorials ,vol. 19 ,no 2 second quarter 2017

[10] Krati Varshney, Manish Kumar Singh, Vibhav Kumar Sachan, Syed Akhtar Imam, “Energy Efficient Data Transmission Scheme for Wireless Sensor Network using DSC-MIMO” International Journal of Computer Applications (0975 – 8887) Volume 167 – No.6, June 2017

[11] Syed Akhtar Imam, Manish Kumar Singh and Vibhav kumar Sachan , “Energy efficient wireless sensor network using DSC-MIMO” Journal of Engineering Technology (ISSN: 0747-9964) Volume 6, Issue 2, July, 2017, PP.268-277

[12] Syed Akhtar Imam, Amit Choudhary, Aijaz Mehdi Zaidi, Manish Kumar Singh, Vibhav Kumar Sachan, “Cooperative Effort Based Wireless Sensor Network Clustering Algorithm for Smart Home Application” Integrated Circuits and Microsystems 2nd IEEE International Conference on, Nanjing, China , 2017

[13] Luís M. Borges, Fernando J. Velez and António S. Lebres, “Survey on the Characterization and Classification of Wireless Sensor Network Applications” IEEE Communication surveys & tutorial,Vol.16, No. 4,Fourth Quarter 2014.

[14] Mr. Puneet Garg, Mr. Kuntal Saroha, Mrs. Ruchika Lochab, “Review of Wireless Sensor Networks- Architecture and Applications” International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011”

[15] Muhammad Umar Aftab, Omair Ashraf, Muhammad Irfan, Muhammad Majid, Amna Nisar, Muhammad Asif Habib, “A Review Study of Wireless Sensor Networks and Its Security” Communications and Network, 2015, 7, 172-179

[16] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996-2018, 2014.

[17] M. Ribeiro, K. Grolinger, and M. A. M. Capretz, "MLaaS: Machine Learning as a Service," in IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 2015, pp. 896-902.

[18] R. Husain and D. R. Vohra, "A Survey On Machine Learning In Wireless Sensor Networks," International Education And Research Journal, Wireless Sensor Networks(WSNs), Machine Learning Techniques,WSN applications. vol. 3, no. 1, 2017-01-16 2017.

[19] D. Janakiram, V. A. Reddy, and A. V. U. P. Kumar, "Outlier Detection in Wireless Sensor Networks using Bayesian Belief Networks," in 1st International Conference on Communication Systems Software & Middleware, New Delhi, India, 2006, pp. 1-6: IEEE.

[20] J. Branch, B. Szymanski, C. Giannella, W. Ran, and H. Kargupta, "In-Network Outlier Detection in Wireless Sensor Networks," in 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), Lisboa, Portugal, Portugal, 2006, pp. 51-51.

[21] K. Beyer, J. Goldstein, R. Ramakrishnan, and U. Shaft, "When Is "Nearest Neighbor" Meaningful?," in Database Theory — ICDT'99: 7th International Conference Jerusalem, Israel, January 10–12, 1999 Proceedings, C. Beeri and P. Buneman, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 217-235.

[22] Cai Z-W and Huang L-H. Finite-time synchronization by switching state-feedback control for discontinuous Cohen–Grossberg neural networks with mixed delays. Int J Mach Learn Cybern 2018; 9: 1683–1695.

[23] Yin X, Zhang K, Li B, et al. A task allocation strategy for complex applications in heterogeneous cluster–based wireless sensor networks. Int J Distrib Sens Netw 2018; 14: 1–15.

[24] Wang J, Gao Y, Yin X, et al. An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. Wirel Commun Mob Comput 2018; 2018: 9472075.

[25] Hosen AS, Singh S, Mariappan V, et al. A secure and privacy preserving partial deterministic RWP model to reduce overlapping in IoT sensing environment. IEEE Access 2019; 7: 39702–39716.