Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study of Various Anomalies and Anomaly Detection Methodologies in Wireless Sensor Network

Gourav Sahni*
Research Scholar
CSE Dept., Kurukshetra University
India.

Sonia Sharma
Assistant Professor
CSE Dept., Kurukshetra University
India.

Abstract— In Wireless Sensor Networks (WSNs), the sensor reading which deviates from the normal pattern of the sensed data are usually considered as anomaly or outlier. Detection of these anomalies is a challenging area of research due to unreliable hardware and software. Finding or detecting such anomalies is laborious and difficult process. This survey provides an overview of wireless sensor network and outlines the various anomalies types occurring in WSNs and their detection methods.

Keywords— Wireless Sensor Network; Anomaly Detection; Outlier; Sensor Node; Anomaly types; Sensors.

I. INTRODUCTION

Wireless sensor networks (WSNs) have become a popular area of research in recent years due to their number of strengths and applications in various domains. Sensor networks can be deployed over a large geographical area (a few meters to kilometres or larger than that) through deploying small devices known as sensors. In accordance with deployment of nodes the WSNs could be of two types: *Unstructured and structured WSN*. The difference between them is that in unstructured WSN nodes are densely and randomly deployed over a field which makes network management tasks difficult such as detecting failures and connectivity management since there are large number of nodes where as in structured WSN some or all nodes are densely deployed in pre- planned manner (nodes have fixed locations) [1]. There are a number of applications such as military applications, environmental monitoring, commercial or human centric applications and applications to robotics that utilize wireless sensor networks. In military applications WSNs generally used for enemy tracking and battlefield surveillance. In environmental monitoring the sensor can be used for sense temperature, barometric pressure, and humidity etc. Human centric applications includes include tracking and monitoring doctors and patients, or tracking drug usage inside hospitals In many of these applications mining of sensor reading is essential to make appropriate decision [4].

In WSNs sensors are small in size, low cost devices with limited processing and computing resources. These sensors are capable of performing task like sensing, data processing and communicating with other sensor nodes. A sensor node equipped with components such as *sensor* (one or more) which is used for sensing and the position of sensor nodes need not be engineered or pre-determined [2]. A *power source* such as battery allocates the needed energy for consumption and can be charged by solar energy depending on the appropriateness of the environment where the sensor will be deployed. An *Analog-to-Digital Converter* (ADC) converts the received analog signal into digital signals. A *processor* (node acts as a central processor) and memory for processing and storing information needed for processing. A *Transceiver* used for communication with other nodes in network [3].The sensor nodes are distributed or deployed in the sensor field. Each node can collect the data and route it to another node and then back to the sink which can communicate with end user by taking the help of the internet. The wireless sensor network is shown in Fig 1. [2].

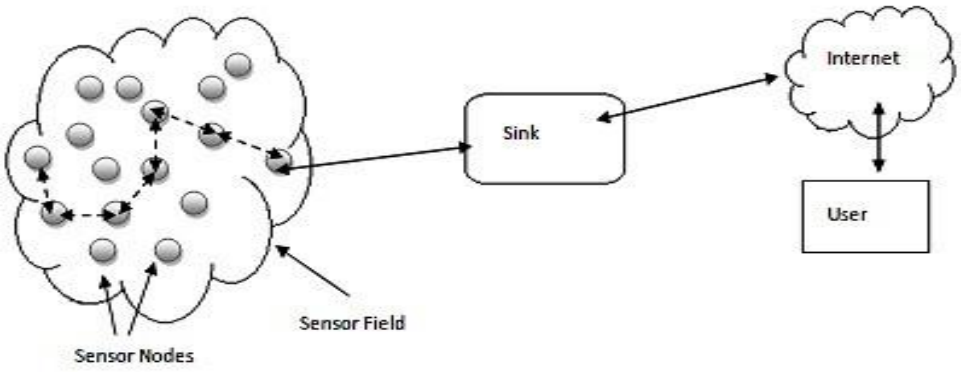


Fig 1: Wireless Sensor Network

A. ***Challenges In Wireless Sensor Networks:***

There are various challenges faced by WSNs. Some of them are stated below:

- **Power/ Energy Management:** This the main challenge in sensor network. A large amount of energy is consumed during communication among the nodes. For monitoring the critical areas, sensor should not deplete with battery. So instead of using single sensor multiple sensors should be deployed in such areas.
- **Real-Time:** Sometime it is necessary to deliver the data within given time or deadline. Not all the protocol developed for WSNs provide real time requirements. So for WSNs, developing real time protocol is a challenge.
- **Security:** One of great challenge threatening the WSNs. If sensor nodes are deployed in those areas which are easily accessible, then there is a great risk of physical attacks. To achieve security in sensor network, security must be integrated in every single component of the system. One of the main challenges is how to secure a wireless network from eavesdropping because current security methods are inadequate for WSNs [5].
- **Anomaly:** Sensor node gathers data and there is high possibility of corruption of that data. The main focus of this survey is on this challenge.

Data gathered by the sensor nodes is unreliable due to limited resources. Especially, when battery power is exhausted, the probability of poor quality of data is increased [6]. To ensure the better quality of data collected by WSNs identification of faulty or anomalous data is essential. This survey paper is organized as follows: In section II we study the concept of anomaly and briefly explain various anomalies types that can occur in WSNs. In section III we surveyed the architecture and application of anomaly detection. Section IV gives an overview of the anomaly detection techniques. Section V we presented the related work. Paper is concluded in Section VI.

II. OVERVIEW OF WSNS ANOMALIES

WSNs are more vulnerable to anomalies due to their complex and dynamic characteristics. In general, an *anomaly* in a set of data can be defined as an observation that appears to be inconsistent with the remainder of the data set [7].

In WSNs anomalies also known as *Outliers*, are those patterns of data that do not conform to the normal pattern of sensed data means data reading deviate from their original values [8]. Raja Jurdak et. al.[9] classify the anomalies mainly into three broad categories.

- Node anomaly
- Network anomaly
- Data anomaly

Node Anomalies occur due to fault at single node. Main reason behind this anomaly is battery issue, i.e. battery failure or depletion [9]. In the nodes fault occur due to deployment of nodes in harsh environment. Chen et. al.[10] provide a localized fault detection algorithm to detect faulty sensor. In this algorithm sensor identifies them as good or faulty.

Unlike node anomalies, the *Network Anomalies* can occur at group of nodes. These are mainly communication related problem. As already stated in this paper that sensor nodes communicate with each other and if that communication is interrupted due to some reasons then network anomaly occurs [9]. Nithya Ramanathan et. al.[11] provide a tool named Sympathy to detect and debug network failure. *Data Anomaly* occurs when there are some irregularities are present in the sensed data. Some security breaches can also lead to anomalous data. According to Raja Jurdak et. al. data anomalies are of three types [9].

- Temporal
- Spatial
- Spatial temporal

There is another classification of anomaly given in [8].In accordance to nature of the anomalies, they can be classified as follows:

- Point anomalies.
- Contextual anomalies
- Collective anomalies

In *Point Anomalies* only a single data instance is anomalous with respect to rest of the normal data. In *contextual Anomalies* can be defined by the contextual and behavioural attribute of the data. For example in spatial data, longitude of a location is contextual and average rainfall at a location is behavioural attribute. If we found a collection of data does not conform to entire set of data then it is known as *collective anomalies* [8].

III. ANOMALY DETECTION:- ARCHITECTURES AND APPLICATIONS

The problem of detecting changes from the normal observed behavior in sensor measurements is known as *anomaly detection* [11].

A. ***Architectures:*** R. Jurdak et al. [9] presents three types of architecture for anomaly detection presented below:

1) ***Centralized:*** In this data is collected from all the nodes at a centralized location for the detection of anomalies as shown in fig 2[9]. Here each node is measuring the temperature and the reading sensed by them is written in circle. And all the reading is getting stored in central database. The node in bold is showing anomalous data that is having large difference from another nodes and localization of anomaly is then performed by sender ID [9]. Nithya Ramanathan et. al.[11] proposed this approach for detecting anomalies in which all data is gathered at a

centralized location called sink for the analysis. This approach considers being energy in-efficient as all nodes communicate to each other to send data to the sink and hence reduce the lifetime of the network.

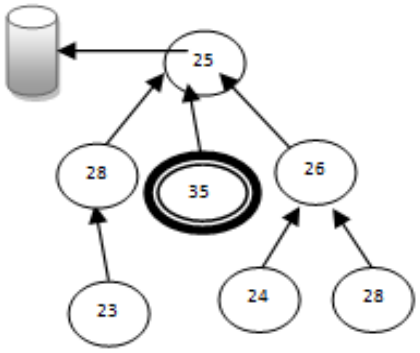


Fig 2. Centralized Approach for Anomaly Detection

2) ***Distributed:*** In Distributed approach, each node is itself responsible for detection of the anomalies. It is the responsibility of sensor nodes to monitor their conditions and detect anomalous behavior by themselves or their neighbors. Jinran Chen et. al. [10] presents a distributed node anomaly detection algorithm. As sensor nodes are powered with a limited resource battery so using centralized approach for faulty sensor detection is not a better choice.
3) ***Hybrid:*** In Hybrid approach, the detection used both distributed and centralized approach [9]. Sutharshan Rajasegarar et. al.[12] uses hybrid approach to detect anomalies in WSN. They proposed a novel approach by which communication overhead is reduced. Instead of gathering reading from individual nodes, the data clustering concept is used.

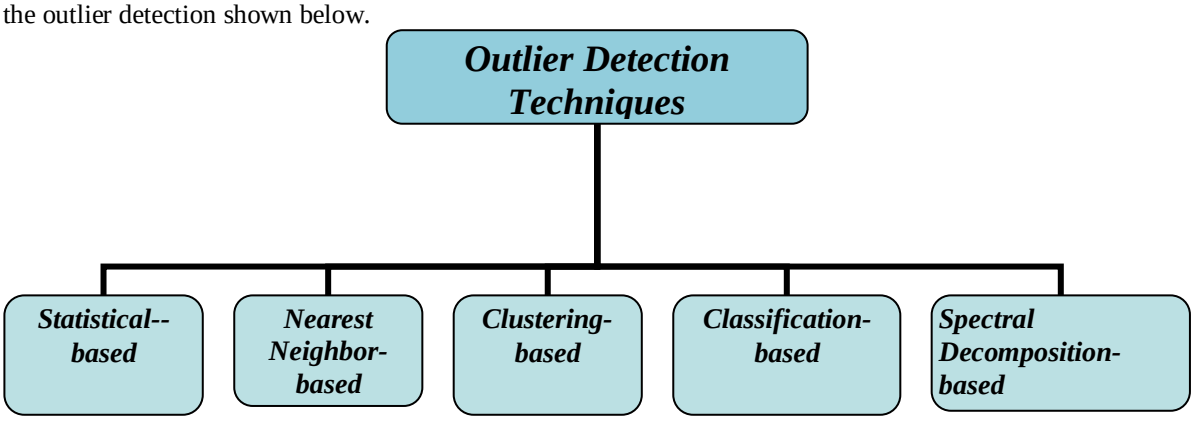
B. ***Applications:***

There are various *applications* of anomaly detection in WSNs. Sutharshan rajasegarar et. al. [14] presents in his papers some of these application stated below:

- When we don't have any prior knowledge how irregularities look like, anomaly detection is used. It is way of generating alert when there is an unusual change in the system.
- Intrusion detection: anomaly detection is useful in detecting new types of intrusions that emerge in WSN. But there is a high possibility of the false alarm.
- Another main application is to detect and remove those measurements which are having errors.

IV. ANOMALY DETECTION METHODOLOGIES

In this we survey the recent techniques for the anomalies detection. Classification of these techniques can be done on the basis of the knowledge of the data available. The *unsupervised approach* finds out the anomalies without any prior knowledge of data. There is no labeled data. This assumes that the anomalies are separated from the data instances that are normal. In *both supervised and semi-supervised*, we classify the data as normal and abnormal. The sensed data is then compared with the defined labeled data and anomalies are detected [7]. Further, the classification of anomaly detection can be done on the basis of the *model* they learn. Yang Zhang et. al. [6] proposed a taxonomy framework for the outlier detection shown below.



Statistical-based approach uses the unsupervised technique and it can be further classified into *parametric based approach* in which we have knowledge of the data available and *Non- parametric based approach* in which availability

of data distribution is not known. In Nearest *Neighbor-based approach* the data instance is analyzed with nearest neighbor. The Euclidean distance is popular approach used in it. *Clustering-Based Approaches*, by clustering we mean to group similar type of data. Sutharshan Rajasegarar et. al. [12] present this distributed anomaly detection which was based on Clustering-Based Approaches. Topology used was hierarchical in nature. Classification-Based Approaches mainly used in data mining. They can classify as support vector machines based and Bayesian network-based approaches.

V. RELATED WORK

Detection of anomaly in WSN has been the topic of research and many surveys and review papers. Victoria J. Hodge et. al. [7] proposed a survey on Outlier Detection Methodologies in machine learning and statistical domains.. In this paper, they have also presented a number of applications where the anomaly detection can be useful such as in Fraud detection, Detecting mislabeled data in given training set etc. Sutharshan rajasegarar et. al. [14] has surveyed state of the art in anomaly detection techniques and discusses some issues for research. Yang Zhang et. al. [15] has proposed online outlier detection technique they used the one-class quarter-sphere SVM (support vector machine) for this purpose. Varun chandola et. al. [8] also proposed a comprehensive overview of anomaly detection techniques. Jinran Chen et. al. [10] proposes and evaluates a fault detection algorithm. This algorithm is used to localize the faulty sensor. Nithya Ramanathan et. al.[11] proposed a tool for detecting failure In pre deployment or post deployment of the sensor network. This tool is based on the centralized architecture approach. Sutharshan Rajasegarar et. al. [13] have proposed another approach for distributed anomaly detection which uses the one-class quarter sphere SVM and provide accuracy comparable to centralized approach. The hierarchical topology is used for detection of anomalies

VI. CONCLUSIONS

In this paper, we have given an overview of the wireless sensor networks and their challenges. One of challenge that is anomaly detection being a recent area of research as used for mining the sensor data is surveyed. Various types of the anomalies that can present in wireless sensor network are briefly explained to provide an overview. We also introduce the architecture used for anomaly detection and brief introduction to techniques.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal. "*Wireless Sensor Network Survey*". Computer Networks 52 (2008), Elsevier, 2292–2330.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "*Wireless sensor networks: A survey*". Computer Networks, 38(4):393-422, 2002

[3] Jalil Jabari Lotf, Seyed Hossein Hosseini Nazhad, Rasim M. Alguliev "*A Survey Of Wireless Sensor Networks*", Department of Computer Engineering, Australian Journal of Basic and Applied Sciences, 5(8): 1496-1503, 2011.

[4] Th. Arampatzis, J. Lygeros, Senior Member, IEEE, and S. Manesis, Member, IEEE "*A Survey of Applications of Wireless Sensors and Wireless Sensor Networks*" Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June2005

[5] John A. Stankovic,Department of Computer Science, University of Virginia "*Research Challenges for Wireless Sensor Networks*".

[6] Yang Zhang, Nirvana Meratnia, And Paul Having "*Outlier Detection Techniques For Wireless Sensor Networks: A Survey*" IEEE Communications Surveys & Tutorials, Vol. 12, No. 2, Second Quarter 2010

[7] V. Hodge and J. Austin, "*A Survey of Outlier Detection Methodologies*" Artificial Intelligence Rev., 2004, pp. 85–126.

[8] Varun Chandola, Arindam Banerjee Vipin Kumar "*Anomaly detection: A survey*" ACM (2009)

[9] Raja Jurdak, X. Rosalind Wang, Oliver Obst, and Philip Valencia "*Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies*"

[10] Jinran Chen, Shubha Kher, and Arun Somani,Dependable Computing and Networking Lab, Iowa State University, "*Distributed Fault Detection of Wireless Sensor Networks*"

[11] Nithya Ramanathan, Kevin Chang, Rahul Kapur, Lewis Girod, Eddie Kohler, and Deborah Estrin "*Sympathy for the Sensor Network Debugger*".

[12] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "*Distributed Anomaly Detection In Wireless Sensor Network*," in *IEEE* International Conference on Communications Systems. (Singapore), October 2006

[13] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "*Quarter Sphere Based Distributed Anomaly Detection In Wireless Sensor Networks*" in IEEE International Conference on Communications, 2007.

[14] Sutharshan Rajasegarar, Christopher Leckie, And Marimuthu Palaniswami,University Of Melbourne, Australia, "*Anomaly Detection In Wireless Sensor Networks*" IEEE Wireless Communications , August 2008

[15] Yang Zhang, Nirvana Meratnia and Paul J.M. Havinga "*Ensuring High Sensor Data Quality Through Use Of Online Outlier Detection Techniques*", Int. J. Sensor Networks, Vol. 7, No. 3, 2010.

