ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Anomaly Detection Techniques for Wireless Sensor Networks - A Survey

Satish S. Bhojannawar[1,] Chetan M Bulla[2], Vishal M Danawade[3]

Department of ISE, KLE's KLECET,Chikodi,Karnataka, India[1]

Department of CSE,KLE's KLECET,Chikodi,Karnataka, India[2]

Department of ISE, KLE's KLECET,Chikodi,Karnataka, India[3]

Abstract: Wireless Sensor Networks (WSNs) have emerged as one of the most important research areas, with huge impact on technology enhancement. Large numbers of limited resource sensor nodes operate autonomously to collaborate and manage the wireless networks, through which critical raw data are collected and transmitted to the end users/decision makers. WSNs have been used in critical application scenarios, such as remote patient health monitoring system, home automation, sales tracking, enemy target monitoring and tracking and fire detection system, where the dependability of WSNs becomes very important. Such applications prefer to have complete and accurate data. But WSNs can be susceptible to anomalies due to cheap unreliable hardware and software, and unfavorable operating environment that can affect the network communication. These anomalies must be detected as they can cause failures in the network and hence affect quality of collected data. In this paper, we study the anomalies in WSN, desirable properties of anomaly detection techniques and analyze the various anomaly detection techniques for wireless sensor networks.

Keywords***:*** Wireless sensor network (WSN), Data anomaly detection, Detection effectiveness, Detection efficiency, Energy consumption.

I. Introduction

Wireless sensor networks (WSNs) have become a popular area of research in recent years due to their huge potential to be used in various applications. They have been used with success in critical application scenarios, such as remote patient health monitoring, environmental monitoring, structural monitoring of engineering structures and military surveillance, where the dependability of WSNs becomes an important factor. A number of sensors can be used to monitor and collect information from the environment and send the information to a central location. WSNs can be densely distributed over a geographical area and individual nodes can autonomously communicate and interact with each other over the wireless medium. They have limited computational and energy resource as they are usually small in size [1].The information obtained from the WSNs has to be accurate and complete. Analysis of data collected from sensor at timely manner is of high importance [2]. Raw data collected from the often suffer from inaccuracy and incompleteness. Inaccurate/incomplete data measurements of WSN are often known as WSN anomalies. The complex and dynamic characteristics of WSNs have made them vulnerable to anomalies. Anomalies are defined as observations that do not correspond to a well defined notion of normal behaviors [3]. Anomalies in WSNs can be caused by errors, malfunctioning/failure of nodes and attacks. It is important to effectively detect and respond to anomalies.

The existing anomaly detection solutions for wired networks cannot be ported directly for WSN because of the complex and dynamic characteristics of WSNs. As WSNs are resource constrained networks, any protocols/methods used should make efficient usage of limited resources available in the network. As WSNs are used for many mission critical applications, any anomaly detection method used should be effective in terms of its accuracy, detection rate and false alarms. Anomaly detection methods used in WSNs should be effective and efficient in utilizing the limited network resources. Any anomaly detection techniques should be:

- Running all the time to detect real time anomalies.
- Use distributed approach to make efficient usage of the limited resources
- Adaptive to the various changes in the topology of the WSN.
- Exploit the data correlations (both spatial and temporal) from close neighborhood.
- Converting data of very high dimensionality into data of much lower dimensionality such that each of the lower dimensions conveys much more information.

That means the desirable properties of any anomaly detection techniques should be real-time, distributed, adaptive with provision to reduce data dimension and exploit correlation.

In this paper, we look at i) anomalies in WSN. ii) desirable properties of anomaly detection techniques iii)compare the effectiveness and efficiency of the different techniques.
The rest of paper is organized as follows: Section II describes the anomalies in WSN and requirements of anomaly detection techniques. Section III gives information about different categories of anomaly detection techniques designed for WSN. Section IV compares various detection techniques proposed in the literature. Section V concludes the survey.

II. ANOMALY DETECTION IN WSN

The complex and dynamic characteristics of WSNs have made them vulnerable to anomalies. Anomalies are observations that do not correspond to a well defined notion of normal behaviors. [3].In WSNs, anomalies can occur in the nodes, networks, transmission channels and application data and can be caused by systematic errors, random errors and malicious attacks. For instance, WSNs may be deployed in a hostile and inaccessible location, maintenance on the network components is impossible. These nodes usually operate unattended over a long period of time until the battery depleted. Node failure can cause the networks to be unavailable. The networks are also susceptible to systematic hardware failure, random hardware and communication errors, and malicious attacks. The different types of the anomalies in WSNs are as following.

A. Types of anomalies

Anomalies in WSNs can be [4] classified 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. The node fault occur due to deployment of nodes in harsh environment

Unlike node anomalies, the network Anomalies can occur at group of nodes. These are mainly communication related problem. The sensor nodes communicate with each other and if that communication is interrupted due to some reasons then network anomaly occurs. Malicious attacks such DOS, sinkhole, balckhole, selective forwarding & wormhole attacks contributes to the occurrence of network anomalies.

Data Anomaly occurs when there are some irregularities are present in the sensed data. Some security breaches can also lead to anomalous data. Data anomalies are of three types

- Temporal
- Spatial
- Spatial temporal

Temporal anomaly at a single node location due to changes in data values over time. Spatial anomaly at a single node location due to comparison with neighboring nodes. Spatiotemporal anomaly detected through a number of node location due to changes in data value over time and space.

B. Challenges of Anomaly Detection Techniques in WSNs

Challenges faced by any anomaly detection techniques are :

- Resource constraints of WSN
- High communication cost
- Distributed streaming of data
- Dynamic network topology, mobility, heterogeneity of nodes and frequent communication failures
- Large-scale deployment

C. Desirable Properties of Anomaly Detection in WSNs

Following are the desirable properties of anomaly detection techniques.

*a. Data Dimension Reduction***:** Due to resource restriction, it is necessary to adapt some strategies to reduce the amount of data that are transmitted in the WSN. Minimizing complexity in terms of communication and computation is critical. In WSNs, data streams can be univariate or multivariate. Univariate streams are represented by a set of values read by a unique type of sensor, e.g., a sensor node that monitors only environmental temperature. On the other hand, multivariate streams are represented by a set of values coming from different sensors of the same sensor node, e.g., a node that monitors temperature, pressure and humidity simultaneously, or by a set of measurements coming from the same sensor type located in different sensor nodes, e.g., a node that processes data from different nodes monitoring only temperature. The transmission of multivariate data causes excessive network delay, node energy consumption and reduces the network lifetime resulting in node and network anomalies. Thus it important to have the multivariate data dimensionality reduction to diminish network delay, reduce energy consumption and prolong the network lifetime.

b. Real-Time Detection: It is desirable for a detection algorithm to be able to detect anomalies in real-time or near real-time. This is particularly important for sensor systems corresponding to temporary deployments (as it might not be as useful to detect anomalies once the deployment is over) and those monitoring hazardous natural phenomena (e.g., spread of contaminants in aquatic ecosystems), where prompt detection (and reaction) can be essential for reducing loss of life and money. To minimize the delay time and to ensure data integrity online anomaly detection is preferred. Online anomaly detection techniques should be light weight to cope with the resource limitations of WSN. The detection cost in terms of computation and communication should be minimal.

c. Architectural structure: Existing anomaly detection techniques mainly use either centralized or distributed or local approach for detecting the anomalies.

i) Centralized approach: In centralized detection, the anomaly detection is performed at the base station. WSNs collect information from the sensor nodes and send it to the base station to be processed and analyzed. The anomaly detection techniques can utilize this information to detect any missing data or data anomalies collected. A base station usually has more resource available to use more complex traditional detection algorithms to improve the accuracy. It also has more storage to log historical data which can assist in detecting anomalies. However, additional information, such as number of hops traversed, may be required to pinpoint the cause of data anomalies or detect any malicious attacks such as sinkhole attack in WSNs. This additional information can create a high volume of data transmission in the network and can congest the network. In WSNs, communication consumes more energy than local processing. Clustering technique has been proposed to reduce the communication overhead by sending only aggregated data. Clustering the data can reduce the size and number of the packet in the network, but it also removes information necessary for detecting the cause of the anomalies. This centralized approach may also affect time to resolve the anomalies as the base station can be very far away from the anomalous nodes.

ii) Distributed approach: In distributed approach, the detection agent is installed in every node. It monitors the behavior of neighboring node within its transmission range locally to detect any abnormal behavior. To perform a real time anomaly detection, some rule based detection techniques are used in a node. Node listens promiscuously to neighboring nodes within its transmission range to collect data necessary for anomaly detection. The collected data will be analyzed to detect any deviation from normal behavior using neighboring historical data stored in the memory. Once anomalies have been detected, an alarm is sends to alert the base station or neighboring nodes.

iii) Local approach: In some methods, node at their own level within their scope detect the anomalies.

It is clear that centralized techniques incur high communication overhead in transmitting the whole data for detection in the centralized location. As mentioned before, most of sensor energy is consumed in transmission rather than processing. Therefore, distributed detection is preferable in order to minimize the energy consumption. But distributed approach needs consider two factors i) the amount information needs to be stored in the memory to perform the anomaly detection ii) energy required to listen to the network promiscuously to perform the detection periodically or continuously.

d. Adaptability with Dynamic Data Changes: As the data is being continually generated and transmitted in WNS, large volumes of data can quickly accumulate and lead to a bottle-neck in the analysis necessary to gain knowledge. Such data analysis is used to build normal data behavior models, so as use same models to detect the anomalies. It is therefore desirable to automate the processing of such continually streaming data, in order to detect those points that are of genuine interest to build and continuously update the data behavior model. However, due to the severe resource constraints in WSNs hardware and long unsupervised operations, the key challenges remain to be the development of lightweight methods that able to efficiently detect changes in context under constrained computational resources.

e. Spatial/Temporal Correlation Exploitation: Sensor data measurements are characterized by high attribute, spatial and temporal data correlations. The spatial and temporal correlation among sensor observations is significant and unique characteristics of WSN which can be exploited to drastically enhance the overall network performance.

III. ANOMALY DETECTION TECHNIQUES DESIGNED FOR WSN

Anomaly detection techniques for WSNs can be categorized into statistical-based, nearest neighbor-based, clustering-based, classification-based approaches.

A. Statistical - Based Anomaly Detection Techniques

These techniques build data reference model and evaluate each data pattern with respect to that reference model. Any deviation from the reference model is considered as anomaly. There are two types statistical based techniques i) parametric ii) non parametric techniques. In parametric techniques, known data distribution builds reference model against which parameters are evaluated. In non-parametric, as data distribution in not known a priori, some distribution estimation methods are used to build the reference model against which parameters are evaluated.

Limitations

- Dynamic nature of WSN makes it difficult to select appropriate threshold value for evaluation.
- Non-parametric statistical models are not that suitable for real time applications.
- Computational cost of handling multivariate data is more.

B. Nearest-Neighborhood Based Anomaly Detection Techniques

Methods based on data mining and machine learning are used for anomaly detection. These techniques use some data measurement methods to differentiate normal or anomalous data patterns.

Limitations

- Computational cost of handling multivariate data is more.
- Not scalable.

C. Clustering Based Anomaly Detection Techniques

A cluster is said to be anomalous if it is distant from other clusters in data set[5].Each node builds a local reference model (LRM) and sends it to its cluster head(CH). Upon receiving such LRMs from its nodes, CH constructs a global reference model (GRM) from LRMs. After that CH sends GRM to all its cluster members and summary of GRM to base station. Upon receiving GRM each cluster member uses same for detecting anomalies locally. Base station use GRM summary to differentiate normal or anomalous clusters.

Limitation

- Dynamic data streaming often outdate the LRM and it turn GRM, so there is need for both have to be updated continuously. Updating reference model involves lot of communication overhead and is also computationally expensive

- Because of high computational complexity involved in measuring distance specially among multivariate data patterns, anomaly detection is expensive.

D. Classification-Based Approaches

Classification approaches are important systematic approaches in the data mining and machine learning community. They learn a classification model using the set of data instances (training) and classify an unseen instance into one of the learned (normal/anomalous) class (testing). The unsupervised classification-based techniques require no knowledge of available labeled training data and learn the classification model which fits the majority of the data instance during training.

The one-class unsupervised techniques learn the boundary around the normal instances while some anomalous instance may exist and declare any new instance falling outside this boundary as an outlier. The classifier may need to update itself to accommodate the new instance that belongs to the normal class. In existing anomaly detection techniques for WSNs, classification-based approaches are categorized into support vector machines (SVM)-based and Bayesian network-based approaches based on type of classification model they use.

i) Support Vector Machine-Based(SVM) Approaches: SVM techniques separate the data belonging to different classes by fitting a hyperplane between them, which maximizes the separation. The data is mapped into a higher dimensional feature space where it can be easily separated by a hyperplane. Furthermore, a kernel function is used to approximate the dot products between the mapped vectors in the feature space to find the hyperplane.

ii) Bayesian Network-Based Approaches: Bayesian network-based approaches use a probabilistic graphical model to represent a set of variables and their probabilistic independencies. They aggregate information from different variables and provide an estimate on the expectancy of an event to belong to the learned class. They are categorized as naive Bayesian network, Bayesian belief network, and dynamic Bayesian network approaches based on degree of probabilistic independencies among variables. Naïve Bayesian networks techniques capture spatio-temporal correlations among sensor nodes. Bayesian belief network techniques consider the correlations among the attributes of the sensor data. Dynamic Bayesian networks techniques consider the dynamic network topology that evolves over time, adding new state variables to represent the system state at the current time instance.

Approach	Class	Data Dimension	Detection Mode	Architectural Structure	Adaptability with change	Correlation exploitation
[6]	Statistical Based	Univariate	Distributed	Offline	Non-Adaptive	-
[7]		Univariate	Distributed	Offline	Non-Adaptive	-
[8]		Multivariate	Distributed	Offline	Non-Adaptive	Spatial & Temporal
[9]		Univariate	Centralized	Offline	Non-Adaptive	-
[10]		Univariate & Multivariate	Centralized	Offline	Non-Adaptive	-
[11]		Univariate	Distributed	Online	Non-Adaptive	-
[12]		Univariate	Distributed	Online	Adaptive	-
[13]	NN Based	Multivariate	Distributed	Offline	Non-Adaptive	-
[14]		Multivariate	Distributed	Offline	Non-Adaptive	-
[15]		Multivariate	Distributed	Online	Non-Adaptive	-
[16]	Clustering Based	Multivariate	Distributed	Offline	Non-Adaptive	-
[17]		Multivariate	Local	Offline	Non-Adaptive	-
[18]		Multivariate	Distributed	Offline	Non-Adaptive	-
[19]		Multivariate	Distributed	Offline	Non-Adaptive	-
[20]		Multivariate	Local	Offline	Adaptive	-
[21]	Classification Based	Multivariate	Distributed	Offline	Non-Adaptive	Spatial & Temporal
[22]		Univariate	Centralized	Offline	Non-Adaptive	
[23]		Univariate	Distributed	Offline	Adaptive	Spatial & Temporal
[24]		Multivariate	Distributed	Offline	Non-Adaptive	-
[25]		Multivariate	Distributed	Offline	Non-Adaptive	-
[26]		Multivariate	Local	Online	Non-Adaptive	-
[27]		Multivariate	Distributed	Online	Adaptive	Spatial & Temporal
[28]		Multivariate	Distributed	Online	Adaptive	Spatial & Temporal
[29]		Multivariate	Distributed	Online	Adaptive	Spatial & Temporal
[30]		Univariate Multivariate	Centralized	Offline	Non-Adaptive	-
[31]		Univariate	Centralized	Online	Adaptive	Spatial & Temporal
[32]		Multivariate	Distributed	Offline	Non-Adaptive	-
[33]		Multivariate	Distributed	Online	Adaptive	Spatial & Temporal
[34]		Multivariate	Distributed	Online	Adaptive	Spatial & Temporal
[35]		Univariate	Centralized	Online	Non-Adaptive	-

Limitation

- Techniques are computationally expensive. Not suitable for online anomaly detection.
- Some techniques are not adaptive.
- Non scalable to handle multivariate data.

IV. ANALYSIS OF CURRENT ANOMALY DETECTION TECHNIQUES

In section we are going to analyze the existing anomaly detection techniques based on the desirable properties specified in the section II . The evaluation is given in Table 1.

Table 1: Evaluation of Current Anomaly Detection Techniques

[8,27, 28,29,33,34] do fulfill all the desirable properties, but till do not represent optimal anomaly detection solutions for WSNs for some reasons. As [8] is parametric-based, finding the correct threshold is difficult due to dynamic nature of WSN.[27,28,29,33,34] SVM based classification techniques. In these, computation cost is high, so they are not suitable for real- time applications of WSN.

The major observations from Table 1 are as following:

- Most of the WSN applications deal with multivariate data. Processing and transmission of multivariate data are costly operations. So there is need definite need for data dimension reduction. But only few techniques apply data reduction techniques prior to detection process.
- Most of the anomaly detection techniques are distributed in nature. But there are some concerns like i)the amount information needs to be stored in the memory to perform the anomaly detection ii) energy required to listen to the network promiscuously to perform the detection periodically or continuously.
- Most of the anomaly detection techniques are offline and few them are online. Offline techniques are not useful for real-time applications. Online techniques should be light-weight to cope with resource constraints of WSNs.
- Very few anomaly detection techniques adapt to the dynamic data streaming feature of WSNs.
- Few anomaly detection techniques exploit the temporal and spatial correlation among the data to reduce the data dimension and hence improve the detection accuracy.

V. CONCLUSION

In this paper, we address the problem of anomaly detection in WSNs. We also provide information about anomalies in WSNs, desirable properties of any anomaly detection techniques designed for WSNs. Furthermore, we present a comparative table to compare these techniques in terms of their capability to fulfill desirable properties of anomaly detection techniques. The shortcomings of existing techniques for WSNs clearly calls for developing anomaly detection technique, which takes into account multivariate data and the dependencies of attributes of the sensor node, provides reliable, real-time adaptive detection while considering unique characteristics of WSNs.

REFERENCES

[1] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* 2002, *38*, 393–422.

[2] Zhang, Y.; Meratnia, N.; Havinga, P. Outlier detection techniques for wireless sensor networks: A survey. *IEEE Commun. Surv. Tutor*. 2010, *12*, 159–170.

[3] Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv.* 2009, *41*, 15

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

[5] Burbeck, K.; Nadjm-Tehrani, S. Adaptive real-time anomaly detection with incremental clustering. *Inf. Secur. Tech. Rep.* 2007, *12*, 56–67.

[6] Palpanas, T.; Papadopoulos, D.; Kalogeraki, V.; Gunopulos, D. Distributed deviation detection in sensor networks. *SIGMOD Record* 2003, *32*, 77–82

[7] Sharma, A.B.; Golubchik, L.; Govindan, R. Sensor faults: Detection methods and prevalence in real-world datasets. *ACM Trans. Sen. Netw.* 2010, *6*, 1–39.

[8] Bettencourt, S.M.A.; Hagberg, A.A.; Larkey, L.B. Separating the Wheat from the Chaff:Practical Anomaly Detection Schemes in Ecological Applications of Distributed Sensor Networks. In Proceedings of the 3rd IEEE International Conference on Distributed Computing in Sensor Systems, Santa Fe, NM, USA, 18–20 June 2007; pp. 223–239.

[9] Sheng, B.; Li, Q.; Mao, W.; Jin, W. Outlier Detection in Sensor Networks. In Proceedings of the 8th ACM International Symposium on MOBILE Ad Hoc Networking and Computing, Montreal, Canada , 9–14 September 2007; pp 219–228.

[10] Li, Y. *Anomaly Detection in Unknown Environments Using Wireless Sensor Networks*; The University of Tennessee: Knoxville, TN, USA, 2010.

[11] Yao, Y.; Sharma, A.; Golubchik, L.; Govindan, R. Online anomaly detection for sensor systems: A simple and efficient approach. *Perform. Eval.* 2010, *67*, 1059–1075.

[12] Miao, X.; Jiankun, H.; Biming, T. Histogram-Based Online Anomaly Detection in Hierarchical Wireless Sensor Networks. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25–27 June 2012; pp. 751–759.

[13] Branch, J.; Szymanski, B.; Giannella, C.; Ran, W.; Kargupta, H. In-Network Outlier Detection in Wireless Sensor Networks. In Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS), Lisbon, Portugal, 4–7 July 2006; p. 51.

[14] Xie, M.; Han, S.; Tian, B. Highly Efficient Distance-Based Anomaly Detection Through Univariate with PCA in Wireless Sensor Networks. In Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011), Changsha, China, 16–18 November 2011.

[15] Miao, X.; Jiankun, H.; Song, H.; Hsiao-Hwa, C. Scalable hyper-grid k-NN-based online anomaly detection in wireless sensor networks. *IEEE Trans. Parallel Distribut. Syst.* 2013, *24*, 1661–1670.

[16] Rajasegarar, S.; Leckie, C.; Bezdek, J.C.; Palaniswami, M. Distributed Anomaly Detection in Wireless Sensor Networks. In Proceedings of the 10th IEEE Singapore International Conference on Communication Systems (ICCS 2006), Singapore, 30 October–1 November 2006; pp. 1–5.

[17] Bezdek, J.C.; Rajasegarar, S.; Moshtaghi, M.; Leckie, C.; Palaniswami, M.; Havens, T.C. Anomaly detection in environmental monitoring networks [application notes]. *IEEE Comput. Intell. Mag.* 2011, *6*, 52–58.

[18] Moshtaghi, M.; Rajasegarar, S.; Leckie, C.; Karunasekera, S. Anomaly Detection by Clustering Ellipsoids in Wireless Sensor Networks. In Proceedings of the 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Melbourne, Australia, 7–10 December 2009; pp. 331–336.

[19] Moshtaghi, M.; Leckie, C.; Karunasekera, S.; Bezdek, J.C.; Rajasegarar, S.; Palaniswami, M. Incremental Elliptical Boundary Estimation for Anomaly Detection in Wireless Sensor Networks. In Proceedings of the 11th IEEE International Conference on Data Mining (ICDM), Vancouver, BC, Canada, 11–14 December 2011; pp. 467–476.

[20] Moshtaghi, M.; Bezdek, J.C.; Havens, T.C.; Leckie, C.; Karunasekera, S.; Rajasegarar, S.; Palaniswami, M. Streaming analysis in wireless sensor networks. *Wirel. Commun. Mobile Comput.* 2012, doi:10.1002/wcm.2248.

[21] Janakiram, D.; Adi Mallikarjuna Reddy, V.; Phani Kumar, A.V.U. Outlier Detection in Wireless Sensor Networks Using Bayesian Belief Networks, In Proceedings of the First International Conference on Communication System Software and Middleware (COMSWARE 2006), Delhi, India, 8–12 January 2006; pp. 1–6.

[22] Hill, D.; Minsker, B.; Amir, E. Real-time Bayesian Anomaly Detection for Environmental Sensor Data. In Proceedings of the Congress-International Association for Hydraulic Research (IAHR), Venice, Italy, 1–6 July 2007.

[23] Suthaharan, S.; Leckie, C.; Moshtaghi, M.; Karunasekera, S.; Rajasegarar, S. Sensor Data Boundary Estimation for Anomaly Detection in Wireless Sensor Networks. In Proceedings of the 7th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), San Francisco, CA, USA, 8–12 November 2010; pp. 546–551.

[24] Rajasegarar, S.; Leckie, C.; Palaniswami, M.; Bezdek, J.C. Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Communications (ICC '07), Glasgow, UK, 24–28 June 2007; pp. 3864–3869.

[25] Rajasegarar, S.; Leckie, C.; Bezdek, J.C.; Palaniswami, M. Centered hyper spherical and hyper ellipsoidal one-class support vector machines for anomaly detection in sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2**010, *5*, 518–533.

[26] Zhang, Y.; Meratnia, N.; Havinga, P. An Online Outlier Detection Technique for Wireless Sensor Networks Using Unsupervised Quarter-Sphere Support Vector Machine. In Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Sydney, Australia, 15–18 December 2008; pp. 151–156.

[27] Zhang, Y.; Meratnia, N.; Havinga, P. Adaptive and Online One-Class Support Vector Machine-Based Outlier Detection Techniques for Wireless Sensor Networks. In Proceedings of the International Conference on Advanced Information Networking and Applications Workshops, Bradford, UK, 26–29 May 2009; pp. 990–995.

[28] Zhang, Y.; Meratnia, N.; Havinga, P.J. Ensuring high sensor data quality through use of online outlier detection techniques. *Int. J. Sens. Netw***.** 2010, *7*, 141–151.

[29] Siripanadorn, S.; Hattagam, W.; Teaumroog, N. Anomaly detection in wireless sensor networks using self-organizing map and wavelets. *Int. J. Commun.* 2010, *4*, 74–83.

[30] Takianngam, S.; Usaha, W. Discrete Wavelet Transform and One-Class Support Vector Machines for Anomaly Detection in Wireless Sensor Networks. In Proceedings of the International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS), Chiang Mai, Thailand, 7–9 December 2011; pp. 1–6.

[31] Dereszynski, E.W.; Dietterich, T.G. Spatiotemporal models for data-anomaly detection in dynamic environmental monitoring campaigns. *ACM Trans. Sen. Netw.* 2011, *8*, 1–36.

[32] Bahrepour, M.; Meratnia, N.; Poel, M.; Taghikhaki, Z.; Havinga, P.J.M. Distributed Event Detection in Wireless Sensor Networks for Disaster Management. In Proceedings of the 2nd International Conference on Intelligent Networking and Collaborative Systems (INCoS) Thessaloniki, Greece, 24–26 November 2010; IEEE Computer Society: Thessaloniki, Greece, 2010; pp. 507–512.

[33] Shahid, N.; Naqvi, I.; Qaisar, S. Real Time Energy Efficient Approach to Outlier & Event Detection in Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Communication Systems (ICCS), Singapore, 21–23 November 2012; pp. 162–166.

[34] Shahid, N.; Naqvi, I.H.; Qaisar, S.B. Quarter-Sphere SVM: Attribute and Spatio-Temporal correlations Based Outlier & Event Detection in Wireless Sensor Networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Paris, France, 1–4 April 2012; pp. 2048–2053.

[35] Curiac, D.-I.; Volosencu, C. Ensemble based sensing anomaly detection in wireless sensor networks. *Expert Syst. Appl.* 2012, *39*, 9087–9096.