[1]Ruchika Rami

[2]Dr. Zakiyabanu Malek

Advance Algorithm for Anomaly Detection for Smart Home: A Comprehensive Approach

JES Journal of Electrical Systems

Abstract: - Wireless Sensor Networks (WSN) are significant and essential platforms for the prospect since they have emerged along the concept of the "Internet of Things." They are utilized to oversee, monitor, and administer a diverse array of Applications in the realms of business, healthcare, the natural world, and the military. Nevertheless, the accuracy of data together through sensor nodes is impacted by anomalies that happen due to many factors, including node failures, reading mistakes, unusual procedures, and malicious attacks. Consequently, anomaly detection is a crucial procedure to verify the precision of sensor data before its use in decision-making. This study examines the challenges associated with anomaly detection in WSN and outlines the necessity for creating a highly efficient and successful anomaly detection model. In this segment, we will explore the latest developments in research on data anomalies detecting in Wireless Sensor Networks (WSN). We will categorize the existing detection strategies into five foremost groups based on the procedures used to build them. The text examines several advanced models for every category, highlighting their limits, along with providing recommendations for further research. In addition, the examined options are associated and evaluated based on their alignment along the specified criteria. Ultimately, the inherent limits of existing methods are recognized, and further avenues for exploration are suggested and taken into account.

Keywords: WSN, Data anomaly detection, Detection effectiveness, Detection-efficiency, Energy-consumption

1 Introduction

Wireless Sensor Network (WSN) consists of compact, inexpensive, energy-efficient sensors that are widely deployed to observe a phenomenon, trace an object, or control a procedure. Wireless Sensor Networks (WSN) are utilized throughout several industries includes individual applications such as industrial applications for planning and control, corporate applications for sales monitoring, military applications for tracking and monitoring enemy objectives, and home automation [1-3]. The Internet of Things (IoT) is an innovative concept that is poised to become the upcoming Wireless Sensor Network(-WSN). It involves connecting everything in human existence along with sensors that interconnect with each other, creating a network that greatly simplifies daily life [4]. The sensor nodes in the Internet of Things (IoT) establish dynamic connections along the Internet and utilize its structure to work together and carry out tasks [5].

WSNs have been addressed in several domains, including networking, embedded systems, procuring of information, distributed systems, and procuring of signals. Consequently, other areas of research have arisen, comprising information procurement, data mining, sensor hardware design, routing protocols, location techniques, security, and privacy.

Analysis of sensor data is of utmost significance to decision-makers. As stated through [9], the determination of utilizing a Wireless Sensor Network (-WSN) is not just to gather data from the placement region, but also to promptly evaluate this data to make important decisions. Data quality is of utmost significance as it directly mirrors the actual state of the WSN Application. Regrettably, the unprocessed data together through sensor nodes, specifically in extensive Wireless Sensor Network(WSN), is often unreliable and deficient [10]. The inaccurate sensor readings may arise due to problems along the device that senses the surrounding sensing conditions. The limitations of sensor device resources, like as storing, energy, computing, and bandwidth, might lead to node failures and thus provide abnormal outcomes. Additional environmental variables, like as the severity and complexity of the deployment area, may also outcome in imprecise outcomes [11–13]. In addition, any physical disturbances, like as damage or displacement caused by humans or animals, might interrupt the procedure of collecting data and lead to abnormal findings [1].

Anomalies refer to data metrics that are incorrect or insufficient as an outcome of the reasons stated above. In reference [21], an anomaly is described as an observation that seems to contradict the rest of a dataset. According to reference [22], the process of identifying data patterns that depart from the behavior that is predicted is referred

[1 1*]Asst. Prof, Faculty of Computer Application and IT Dept., GLS University Gujarat, India, Email: ruchi199.rr@gmail.com. [0000-1111-2222-3333]

2 Professor, Centennial University of Toronto, ON Canada, Email: zakiya.malek@gmail.com. [1111-2222-3333-4444]

to as anomaly detection. Several different points of view, including data mining, pattern recognition, and data security, have been considered about the issue of anomaly detection. The term "anomaly" is also acknowledged in scholarly works as an outlier, flaw, or aberration. WSNs are characterized through their anomaly detection system, which possesses the capability to discover anomalies and effectively use the network's limited resources [9]. Detection efficiency is denoted through energy use and memory utilization. Consequently, any suggested anomaly detection system must include the progress in detection effectiveness while minimizing energy and storing usage throughout the detection procedure.

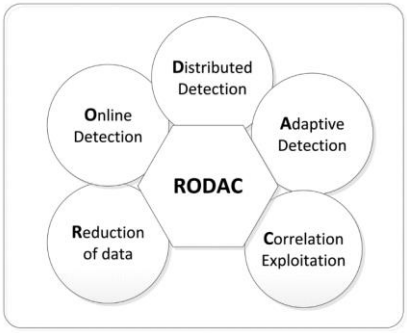

Fig 1: RODAC

This review examines the challenge associated along building and improving anomaly detection algorithms in WSN that are both efficient and effective. The aforementioned challenges arise because to inherent limitations of sensor nodes, like as resource limits that hinder the straightforward application of existing anomaly detection methods on alternative platforms. Gaining insight into the challenges facilitates the exploration of prerequisites for devising proficient and impactful anomaly detection algorithms that surmount these hindrances.

The objective of this review is to enhance readers' comprehension of RODAC standards and pinpoint possible enhancements to current anomaly detection algorithms that are based on these standards. Moreover, it is objective to establish guidelines for creating novel anomaly detection systems which are considered the RODAC criteria, guaranteeing both detection efficiency and effectiveness. An evaluation is conducted to compare the present methods of detection from every class, assessing their adherence to the RODAC necessities. Additionally, the limits of every model are examined. In addition, the study examines the existing limitations of current methodologies to propose potential topics for upcoming research. As survey has examined the matter of anomaly detection in -WSN utilizing the identical set of RODAC criteria.

1.1 Literature Review

The significance of anomaly detection in ensuring sensor data quality and identifying malicious attempts which is disrupt network operation and data integrity has prompted prior research to explore WSN security and anomaly detection technologies. This section describes the present studies of anomaly detection in WSN and the modifications that set this study apart from others.

Rajasegarar and his colleagues devised a methodological classification system for anomaly detection models in Wireless Sensor Networks (WSN) [27, 28]. Both researches classified anomaly detection models as either statistical or non-parametric, depending on the techniques employed in constructing the detection model. The non-parametric model was classified as rule-based, CUSUM-based, data-clustering-based, density-based, and support vector machine (SVM)based model. The statistical model relies on established or inferred density distributions to categorize data as either usual or unusual. In contrast, the non-parametric model does not rely on any assumptions about the characteristics of the data and employs many measures to capture the typical patterns in the data, which are then compared to the patterns observed in upcoming measurements.

A different approach to categorizing outlier detection model based on their techniques was suggested in [9]. Along in this categorization, the non-parametric model was incorporated as a statistical model, and two more classifications were introduced: the nearest neighbor-based model and the spectrum decomposition-based model. The

SVM-based model was categorized as a classification model along the Bayesian network model. Bayesian network model was categorized into three subtypes: naïve Bayesian, belief Bayesian, and dynamic Bayesian model.

The article [29] presented a detailed classification of the anomaly detection model in Wireless Sensor Network (WSN), focusing on three key factors: speed of detection, generality of detection, and achieving a balance among the two. The taxonomy categorizes intrusion detection methods into two types depending on network structure: flat-based or hierarchical. This taxonomy examines numerous intrusion detection algorithms and focuses on the security elements of the anomaly. According to the taxonomy, rule-based models are highly fast and ideal for flat-structured WSNs, but the statistical model is fast for the hierarchical system. In terms of generality, data mining or computational intelligence models were proposed as the best options for both WSN structure types. Additionally, it was proposed that statistical approaches can achieve a good balance of rapidity and generality in both flat and hierarchical WSN systems.

2. Anomaly Detection in Wireless Sensor Networks

Ensuring sensor data quality is critical for creating the appropriate decisions. Cryptographic and key management systems are insufficient to assure data integrity since they do not protect sensor nodes against insider assaults, Like as data fabrication. As an outcome, the anomaly detection model is intended to identify any aberrant behavior in sensor data streams. The subsequent discusses the principles, problems, and needs for anomaly detection in WSN.

2.1 Definitions and Basic Concepts

Accordingly, anomalies are "patterns in data that do not conform to a well-defined notion of normal behaviors" [22]. Another definition in [21] is "an observation that appears to be inconsistent along the reminder of a dataset." Anomalies may emerge in data for a variety of reasons, including hostile conduct, like as cyber-attacks, card fraud, system failure, or terrorist activities, However, the common thread that runs across all of these explanations is that they are interesting to investigate [22].

In WSN, anomalies are characterized as large departures from the typical sensing data profile [22]. These anomalies arise for a variety of reasons, including inaccuracies in measurements generated through malfunctioning sensor nodes, noise introduced through external sources, genuine events induced through changes in the perceived environment, and malicious assaults conducted through hacked sensor nodes. As stated in [22], anomaly detection is the challenge of identifying patterns in data that do not fit well-established and anticipated behavior.

3. Characteristics of Sensor Data

Sensing data is acquired in the form of data streams, which might represent massive quantities of genuine observations from the environment [43]. Some WSNs are simply intended to capture one sort of data, Like as temperature, light, and humidity. This type of data is referred to as univariate. Modern -WSN have the Idea of simultaneously collecting many types of data from the area, which is referred to as multivariate data. These networks' nodes are typically outfitted along several sensors that collect various sorts of data at a similar time. Every piece of data in multivariate analysis is referred to as an attribute or feature. An anomalous sensing data measurement is defined as one or more abnormal properties [44]. Along univariate data, anomaly identification is simple: observe that a single data attribute is aberrant in comparison to the characteristics of other data instances. However, detecting anomalies in multivariate -WSN is difficult since individual characteristics may not exhibit aberrant behavior, but when combined, they may do [45]. Sensor readings have spatial and temporal connections. Temporal correlation implies that data taken during the one-time period is connected to readings consolidated during the preceding period. According to [9], the geographical and temporal correlation of sensing data properties aids in identifying the cause of the abnormality.

3.1 Anomaly Detection in WSN:

WSN are susceptible to anomalies because of their complex and dynamic nature. Anomalies are observations that do not conform to a well-defined set of typical behaviors. Anomalies in -WSN can arise in

nodes, networks, transmission channels, and application data as an outcome of systematic, random,

making network component maintenance unfeasible. These nodes normally work unsupervised for an extended period until the battery is drained.

The dissimilar types of anomalies in -WSN are as subsequent [41]:

- Node Anomaly
- Network Anomaly
- Data Anomaly

Node anomalies occur when there is a failure in a single node. The main factor contributing to this abnormality is a battery malfunction, Like a failure or depletion. The occurrence of node failure is a direct outcome of deploying nodes in an inhospitable environment. Contrary to irregularities in nodes.

Network anomalies may occur inside a cluster of nodes. These difficulties mostly pertain to communication. When the link among sensor nodes is interrupted, a network abnormality occurs. Network anomalies are caused by many malicious attacks, including DoS, sinkholes, black-hole, selected forwarding, and wormhole assaults.

A point anomaly refers to an individual occurrence within a dataset that stands out as being aberrant compared to the other examples. Point anomalies typically denote extreme values, irregularities, or deviations that occur randomly and without specific significance. I like to designate it as an outlier. The time series graph below displays isolated point anomalies as red points.

Contextual anomaly refers to a specific incident that may be regarded as abnormal within a certain context. Consequently, the act of examining a particular topic from various perspectives does not consistently provide us with evidence of abnormal conduct. The determination of the contextual abnormality is achieved by incorporating both contextual and behavioral information. Contextual features commonly rely on the dimensions of time and location, but behavioral features vary depending on the specific area under analysis, such as the amount of money spent, average temperature, or other quantitative measures employed as features.

Dataset

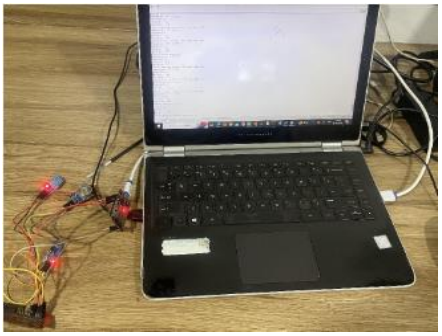

Fig 2: Hardware setup

This IOT-based anomaly detection system could be installed in industrial and commercial buildings where temperature and humidity, Gas, and sunlight values are Generated form sensors for analysis. This system also gives an alarming beep it user when the temperature or humidity level increases by the set values.

This system is less costly, more efficient, and more precise as compared to other systems.

Load Data in Thing speak and also analysis the pattern and behaviour of data.

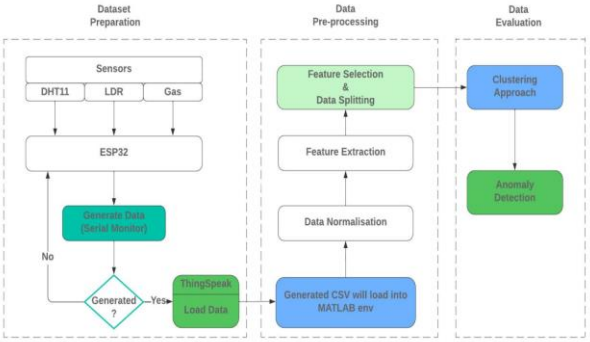

Fig 3: System Architecture

Steps:

1. We initiate procedure
2. Create a dataset along ESP32 hardware. It contains chip microcontrollers that include Wi-Fi and dual-mode Bluetooth.
3. Load Data Temperature Humidity, Air Quality and LDR: Temperature Humidity takes into consideration the combined impacts of ambient temperature and relative humidity, and it is a valuable and simple technique to measure the danger of heat stress. Consider the AQI to be a yardstick along a range of 0-500. A higher Air Quality Index (AQI) figure indicates that the air is more polluted and poses a greater danger to human health. LDR is an abbreviation for Light Dependent Resistor. LDRs are small
4. light-sensing devices, commonly known as photo resistors. An LDR is a resistor whose resistance varies in proportion to the quantity of light passing through it. The LDR's resistance reduces as the light intensity grows, and vice versa.
5. Pre-processing cleans and transforms data to make it ready for analysis. The Idea of data preparation is to ensure that the data is correct, consistent, and ready for analysis.
6. The procedure separates the data frame based on the number of pieces specified.
7. Fuzzy c-means clustering is a soft clustering approach in machine learning that assigns probability scores to every data point inside a cluster.
8. Detecting anomalies entails recognizing atypical events, objects, or observations that significantly diverge from anticipated behaviors or patterns. Data anomalies can be described along the use of terms like standard deviations, outliers, noises, novelties, and exceptions.
9. End

3.2 Pseudocode of fuzzy

Begin

Fix c, $2 < c < n$;

Fix $\in$, ($\in$=0.001);

Fix max Iterations, (maxIterations=100):

Choose whatever inner product norm metric you choose, Like as the Euclidean distance.

Fix m, $1 < m, \infty$, (m = 2);

Randomly set V_0= v_ (1,) v_ (2,), v_(c,) cluster centers;

For t=1 to maxIterations do

Update the membership matrix U

Calculate the membership matrix V^t

Calculate the new objective function J_m^t

If (abs (J_m^t- J_m^(t-1)) < c) then

Breakdown;

Else

J_m^(t-1) =J_m^t;

End if

End for

end

3.3 k- Means Clustering

KM iteratively computes cluster centroids for each distance measure in order to minimize the sum with respect to the specified measure. KM algorithm aims at minimizing an objective function known as squared error function given in Equation (1) as follows:

$$J_{KM}(\boldsymbol{X};\ \boldsymbol{V}) = \sum_{i=1}^{c}\sum_{j=1}^{n} D_{ij}^{2} \quad (1)$$

the chosen distance measure which is generally in Euclidean norm:

$\|xij - vi\|^2$, $1 \le i \le c$, $1 \le j \le n_i$.

Where n_i represents the number of data points in i_{th} cluster. For c clusters, KM is based on an iterative algorithm minimizing the sum of distances from each object to its cluster centroid. The objects are moved between clusters until the sum cannot be decreased any more. KM algorithm involves the following steps:

1) Centroids of c clusters are chosen from $\boldsymbol{X}$ randomly.

2) Distances between data points and cluster centroids are calculated.

3) Each data point is assigned to the cluster whose centroid is closest to it.

4) Cluster centroids are updated by using the formula in Equation (2):

5) $$\boldsymbol{v}_i = \sum_{i=1}^{n_i} x_{ij} / n_i \ ; 1 \le i \le c \quad (2)$$

6) Distances from the updated cluster centroids are recalculated.

7) If no data point is assigned to a new cluster the run of algorithm is stopped, otherwise the steps from 3 to 5 are repeated for probable movements of data points between the clusters.

3.4 K-Medoids Clustering

K-Medoids clustering, a variation of K-Means, partitions data into K clusters by selecting actual data points (medoids) as cluster representatives. This approach offers robustness to outliers and enhances interpretability.

Let X be the dataset with n data points (x_i) in a p-dimensional space. The goal is to find K clusters (1, 2, C_1, C_2… , C_K) and K medoids (m_1, m_2,...,m_K) to minimize total dissimilarity within clusters.

The dissimilarity between data point x_i and medoid m_j is measured using distance metric d (x_i, mj). The dissimilarity within cluster C_k and medoid m_k is $\sum_{xi \in Ck} d$ (xi, mk).

Algorithm:

1. Initialize K medoids.
2. Assign data points to nearest medoids.
3. Update medoids by selecting data points with minimum dissimilarity.
4. Repeat steps 2-3 until convergence.

Objective Function:

Minimize total dissimilarity within clusters:

$\sum_{k=1}^{K}\sum_{xi\in Ck}d\ (x_i, m_k)$

K-Medoids clustering provides a robust and interpretable approach for partitioning data, suitable for various data analysis tasks.

4. Implementation

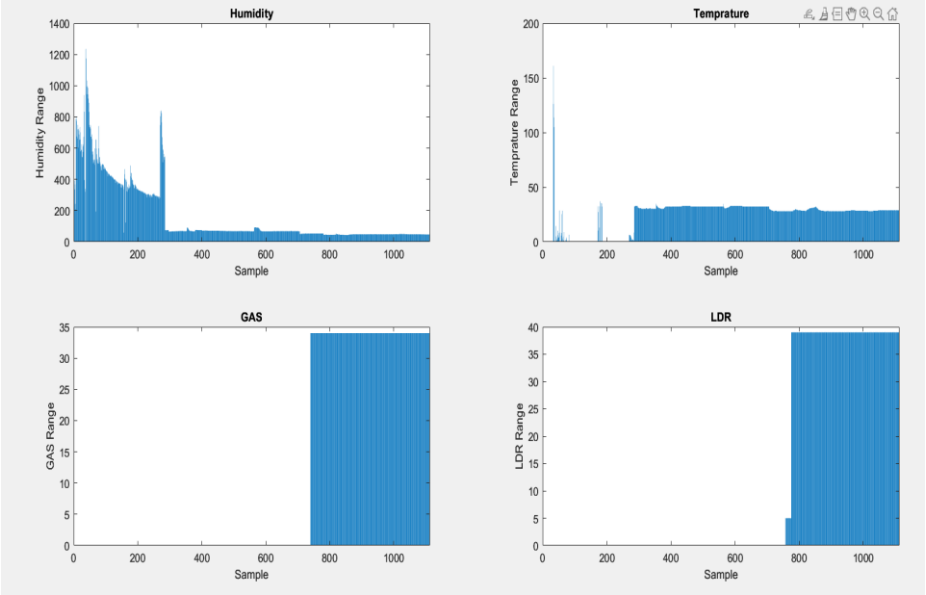

Fig 4: Humidity, Temp, Air-quality, LDR value

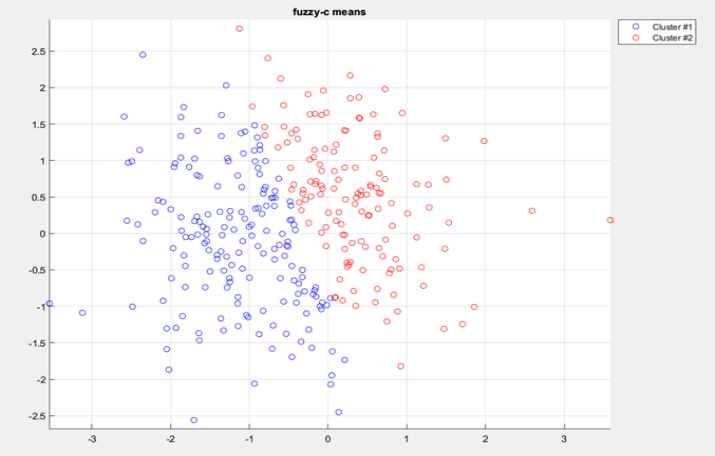

Fig 5: Hybrid Cluster

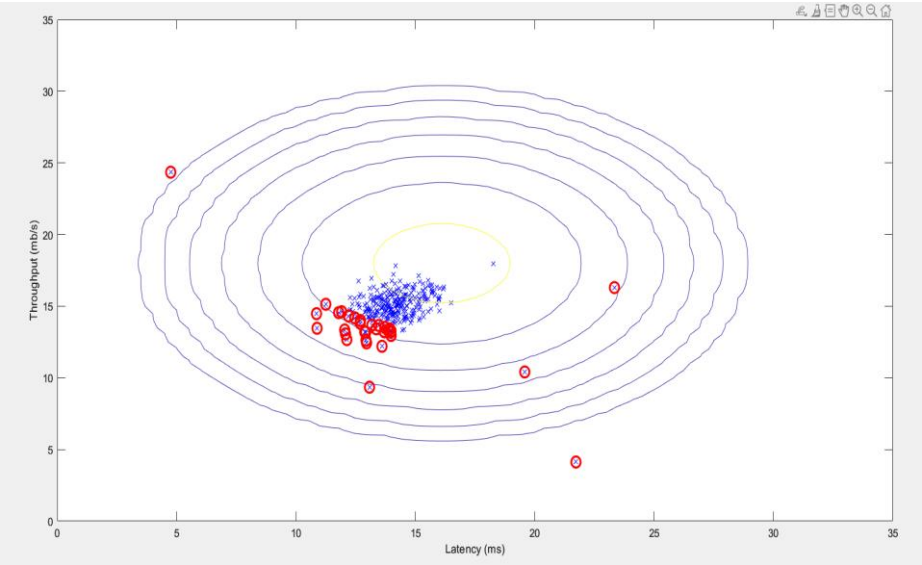

Fig 6: Anomaly Detection

Conclusion

Efficient and effective anomaly detection in sensor readings is crucial for assuring the quality of obtained sensor data and generating good conclusions. Unfortunately, most of the anomaly detection models that have been published in the literature either have poor detection effectiveness or use too much energy. The present research examined the challenges and necessary necessities (RODAC components) for developing an effective and efficient anomaly detection model for -WSN. A complete assessment of cutting-edge detection models was proposed, categorizing them based on detection approaches Like as statistical, clustering, classification, and nearest-neighbor based. A brief explanation of every model was provided in every category, as well as an examination of the category's general constraints. All model from the four categories were compared and analyzed to determine their satisfaction along the necessities given in the RODAC components. The research finds that none of the present model satisfy the entire set of RODAC components. As an outcome, new model or enhancements to existing model are necessary to incorporate all of these criteria. The study continues through discussing the basic limits of existing anomaly detection methods and recommending some upcoming research options.

Reference

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

[2] Arampatzis, T.; Lygeros, J.; Manesis, S. A Survey of Application of Wireless Sensors and Wireless Sensor Networks. Proceedings of the 2005 IEEE International Symposium on Intelligent Control, 2005 and 13th Mediterrean Conference on Control and Automation, Limassol, Cyprus, 27–29 June 2005; pp. 719–724.

[3] Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. Comput. Netw. 2008, 52, 2292–2330. [Google Scholar]

[4] Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. Comput. Netw. 2010, 54, 2787–2805. [Google Scholar]

[5] Christin, D.; Reinhardt, A.; Mogre, P.S.; Steinmetz, R. Wireless Sensor Networkand the Internet of Things: Selected Challenges. Proceedings of the 8th Gesellschaft für Informatik e.V./ Informationstechnische Gesellschaft Kommunikation und Verteilte Systeme Fachgespräch Drahtlose Sensornetze, Hamburg, Germany, 13–14 August 2009; pp. 31–34.

[6] Internet of Things in 2020: Roadmap for the Future. Available online: http://www.smart-system-integration.org/public/internet-of-things (on accessed 27 June 2013).

[7] Alcaraz, C.; Najera, P.; Lopez, J.; Roman, R. Wireless Sensor Networkand the Internet of Things: Do We Need a Complete Integration. Proceedings of the 1st International Workshop On The Security of The Internet of Things (SecIoT), Tokyo, Japan, 29 November 2010.

[8] Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. Internet proposed standard RFC 4944: Transmission of IPv6 packets over IEEE 802.15. 4 networks. 2007. Available online: http://www.hjp.at/doc/rfc/rfc4944.html (on accessed 25 June 2013). [Google Scholar]

[9] Zhang, Y.; Meratnia, N.; Havinga, P. Outlier detection techniques for wireless sensor networks: A survey. IEEE Commun. Surv. Tutor. 2010, 12, 159–170. [Google Scholar]
[10] Han, J.; Kamber, M. Data Mining: Concepts and Techniques, 2nd ed.; Morgan Kaufmann: San Fransisco, CA, USA, 2006. [Google Scholar]
[11] Marzullo, K. Tolerating failures of continuous-valued sensors. ACM Trans. Comput. Syst. 1990, 8, 284–304. [Google Scholar]
[12] Bettencourt, S.M.A.; Hagberg, A.A.; Larkey, L.B. Separating the Wheat from the Chaff: Practical Anomaly Detection Schemes in Ecological Application of Distributed Sensor Networks. Proceedings of the 3rd IEEE International Conference on Distributed Computing in Sensor System, Santa Fe, NM, USA, 18–20 June 2007; pp. 223–239.
[13] Elnahrawy, E. Research directions in sensor data streams: Solutions and challenges; DCIS Technical Report DCIS-TR-527; Rutgers University: New Brunswick, NJ, USA, 2003. [Google Scholar]
[14] Krontiris, I.; Benenson, Z.; Giannetsos, T.; Freiling, F.; Dimitriou, T. Cooperative Intrusion Detection in Wireless Sensor Networks; Springer: Berlin/Heidelberg, Germany, 2009; pp. 263–278. [Google Scholar]
[15] Krontiris, I.; Dimitriou, T.; Freiling, F.C. Towards Intrusion Detection in Wireless Sensor Networks. Proceedings of the 13th European Wireless Conference, Paris, France, 1–4 April 2007.
[16] Krontiris, I.; Dimitriou, T.; Giannetsos, T.; Mpasoukos, M. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 150–161. [Google Scholar]
[17] Ngai, E.C.H.; Liu, J.; Lyu, M.R. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Comput. Commun. 2007, 30, 2353–2364. [Google Scholar]
[18] Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutor. 2006, 8, 2–23. [Google Scholar]
[19] Chen, X.; Makki, K.; Yen, K.; Pissinou, N. Sensor network security: A survey. IEEE Commun. Surv. Tutor. 2009, 11, 52–73. [Google Scholar]
[20] Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad. Hoc. Netw. 2003, 1, 293–315. [Google Scholar]
[21] Hodge, V.; Austin, J. A survey of outlier detection methodologies. Artif. Intell. Rev. 2004, 22, 85–126. [Google Scholar]
[22] Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. ACM Comput. Surv. 2009, 41, 15. [Google Scholar]
[23] Zhenwei, Y.; Tsai, J.J.P. A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks. IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC'08), Taichung, Taiwan, 11–13 June 2008; pp. 272–279.
[24] Farooqi, A.H.; Khan, F.A. Intrusion Detection System for Wireless Sensor Networks: A Survey. In Communication and Networking; Ślęzak, D., Kim, T.-H., Chang, A.C.-C., Vasilakos, T., Li, M., Sakurai, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 56, pp. 234–241. [Google Scholar]
[25] Wang, L.; Deshpande, A. Predictive Modelingbased Data Collection in Wireless Sensor Networks. In Wireless Sensor Networks; Springer: Berlin/Heidelberg, Germany, 2008; pp. 34–51. [Google Scholar]
[26] Deshpande, A.; Guestrin, C.; Madden, S.R.; Hellerstein, J.M.; Hong, W. Model-Driven Data Acquisition in Sensor Networks. Proceedings of the 30th International Conference on Very Large Data Bases, Toronto, Canada, 31 August–3 September 2004; Volume 30, pp. 588–599.
[27] Rajasegarar, S.; Leckie, C.; Palaniswami, M. Anomaly detection in wireless sensor networks. IEEE Wirel. Commun. 2008, 15, 34–40. [Google Scholar]
[28] Rajasegarar, S.; Leckie, C.; Palaniswami, M. Detecting data anomalies in wireless sensor networks. Secur. Ad Hoc. Sens. Netw. 2009, 3, 231–259. [Google Scholar]
[29] Xie, M.; Han, S.; Tian, B.; Parvin, S. Anomaly detection in wireless sensor networks: A survey. J. Netw. Comput. Applic. 2011, 34, 1302–1325. [Google Scholar]
[30] Jurdak, R.; Wang, X.R.; Obst, O.; Valencia, P. Wireless sensor Network Anomalies: Diagnosis and Detection Strategies. In Intelligencebased System Engineering; Springer: Berlin/Heidelberg, Germany, 2011; pp. 309–325. [Google Scholar]
[31] Ni, K.; Ramanathan, N.; Chehade, M.N.H.; Balzano, L.; Nair, S.; Zahedi, S.; Kohler, E.; Pottie, G.; Hansen, M.; Srivastava, M. Sensor network data fault types. ACM Trans. Sen. Netw. 2009, 5, 1–29. [Google Scholar]
[32] Hill, J.; Szewczyk, R.; Woo, A.; Hollar, S.; Culler, D.; Pister, K. System architecture directions for networked sensors. Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating System, Cambridge, MA, USA, 12–15 November 2000; pp. 93–104.
[33] Estrin, D.; Govindan, R.; Heidemann, J.; Kumar, S. Next Century Challenges: Scalable Coordination in Sensor Networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99), Seattle, WA, USA, 15–19 August 1999; ACM: Seattle, WA, USA, 1999; pp. 263–270. [Google Scholar]
[34] Romer, K.; Mattern, F. The design space of wireless sensor networks. Wirel. Commun. IEEE. 2004, 11, 54–61. [Google Scholar]

[35] Al-Karaki, J.N.; Kamal, A.E. Routing techniques in wireless sensor networks: A survey. IEEE Wirel. Commun. 2004, 11, 6–28. [Google Scholar]
[36] Thuc, K.-X.; Insoo, K. A collaborative event detection scheme using fuzzy logic in clustered wireless sensor networks. AEU-Int. J. Electron. Commun. 2011, 65, 485–488. [Google Scholar]
[37] Bahrepour, M.; Meratnia, N.; Poel, M.; Taghikhaki, Z.; Havinga, P.J.M. Distributed Event Detection in Wireless Sensor Networkfor Disaster Management. Proceedings of the 2nd International Conference on Intelligent Networking and Collaborative System (INCoS), Thessaloniki, Greece, 24–26 November 2010; IEEE Computer Society: Thessaloniki, Greece, 2010; pp. 507–512. [Google Scholar]
[38] Baig, Z.A. Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks. Comput. Commun. 2011, 34, 468–484. [Google Scholar]
[39] Baig, Z.A.; Khan, S.A. Fuzzy Logicbased Decision Making for Detecting Distributed Node Exhaustion Attacks in Wireless Sensor Networks. Proceedings of the 2nd IEEE Computer Society Second International Conference on Future Networks, Sanya, Hainan, China, 22–24 January 2010; pp. 185–189.
[40] Kaplantzis, S.; Shilton, A.; Mani, N.; Sekercioglu, Y.A. Detecting Selective Forwarding Attacks in Wireless Sensor Networkusing Support Vector Machines. Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP), Melbourne, 5–8 December 2007; pp. 335–340
[41] Satish S. Bhojannawar1, Chetan M Bulla2, Vishal M Danawade, “Anomaly Detection Techniques for Wireless Sensor Network- A Survey”, IJARCCE, Vol. 2, Issue 10, October 2013.
[42] https://www.researchgate.net/figure/Pseudo-code-of-the-FCM-algorithm_fig1_221470917