electronics

Article

Detecting Sensor Faults, Anomalies and Outliers in the Internet of Things: A Survey on the Challenges and Solutions

Anuroop Gaddam *, Tim Wilkin, Maia Angelova and Jyotheesh Gaddam

School of Information Technology, Deakin University, Geelong 3216, Australia;
Tim.Wilkin@deakin.edu.au (T.W.); maia.a@deakin.edu.au (M.A.); jgaddam@deakin.edu.au (J.G.)
* Correspondence: Anuroop.Gaddam@deakin.edu.au; Tel.: +61-3-924-45775

Received: 28 January 2020; Accepted: 14 March 2020; Published: 20 March 2020

Abstract: The Internet of Things (IoT) has gained significant recognition to become a novel sensing paradigm to interact with the physical world in this Industry 4.0 era. The IoTs are being used in many diverse applications that are part of our life and is growing to become the global digital nervous systems. It is quite evident that in the near future, hundreds of millions of individuals and businesses with billions will have smart-sensors and advanced communication technology, and these things will expand the boundaries of current systems. This will result in a potential change in the way we work, learn, innovate, live and entertain. The heterogeneous smart sensors within the Internet of Things are indispensable parts, which capture the raw data from the physical world by being the first port of contact. Often the sensors within the IoT are deployed or installed in harsh environments. This inevitably means that the sensors are prone to failure, malfunction, rapid attrition, malicious attacks, theft and tampering. All of these conditions cause the sensors within the IoT to produce unusual and erroneous readings, often known as outliers. Much of the current research has been done in developing the sensor outlier and fault detection models exclusively for the Wireless Sensor Networks (WSN), and adequate research has not been done so far in the context of the IoT. Wireless sensor network's operational framework differ greatly when compared to IoT's operational framework, using some of the existing models developed for WSN cannot be used on IoT's for detecting outliers and faults. Sensor faults and outlier detection is very crucial in the IoT to detect the high probability of erroneous reading or data corruption, thereby ensuring the quality of the data collected by sensors. The data collected by sensors are initially pre-processed to be transformed into information and when Artificially Intelligent (AI), Machine Learning (ML) models are further used by the IoT, the information is further processed into applications and processes. Any faulty, erroneous, corrupted sensor readings corrupt the trained models, which thereby produces abnormal processes or outliers that are significantly distinct from the normal behavioural processes of a system. In this paper, we present a comprehensive review of the detecting sensor faults, anomalies, outliers in the Internet of Things and the challenges. A comprehensive guideline to select an adequate outlier detection model for the sensors in the IoT context for various applications is discussed.

Keywords: sensor reliability; outlier detection; time series; Internet of Things; anomaly detection; multi-agent deep reinforcement learning

1. Introduction

The Internet of Things is one of the key disruptive technologies in the Industry 4.0 era [1]. There is a growing trend to use the Internet of Things (IoT) in scientific and industrial communities [2,3]. There are many definitions proposed for the IoT, in general, the IoT can be described as a confluence of various technologies that provide Internet-based services and applications with the help of electronics devices connected to physical things for the purpose of collecting data through heterogeneous sensors, for controlling processes [4]. IoTs are being used in many applications in various fields, from environmental monitoring, health care, agriculture and manufacturing sectors [5–7]. IoTs have evolved from being a just a connection and communication point for acquiring the data of physical objects to comprehensive smart systems that are capable collecting enormous amounts of data and monitoring various processes for maximising the profits for organisations and individuals. An abstraction of the Internet of Thing's (IoT) architecture is shown in Figure 1.

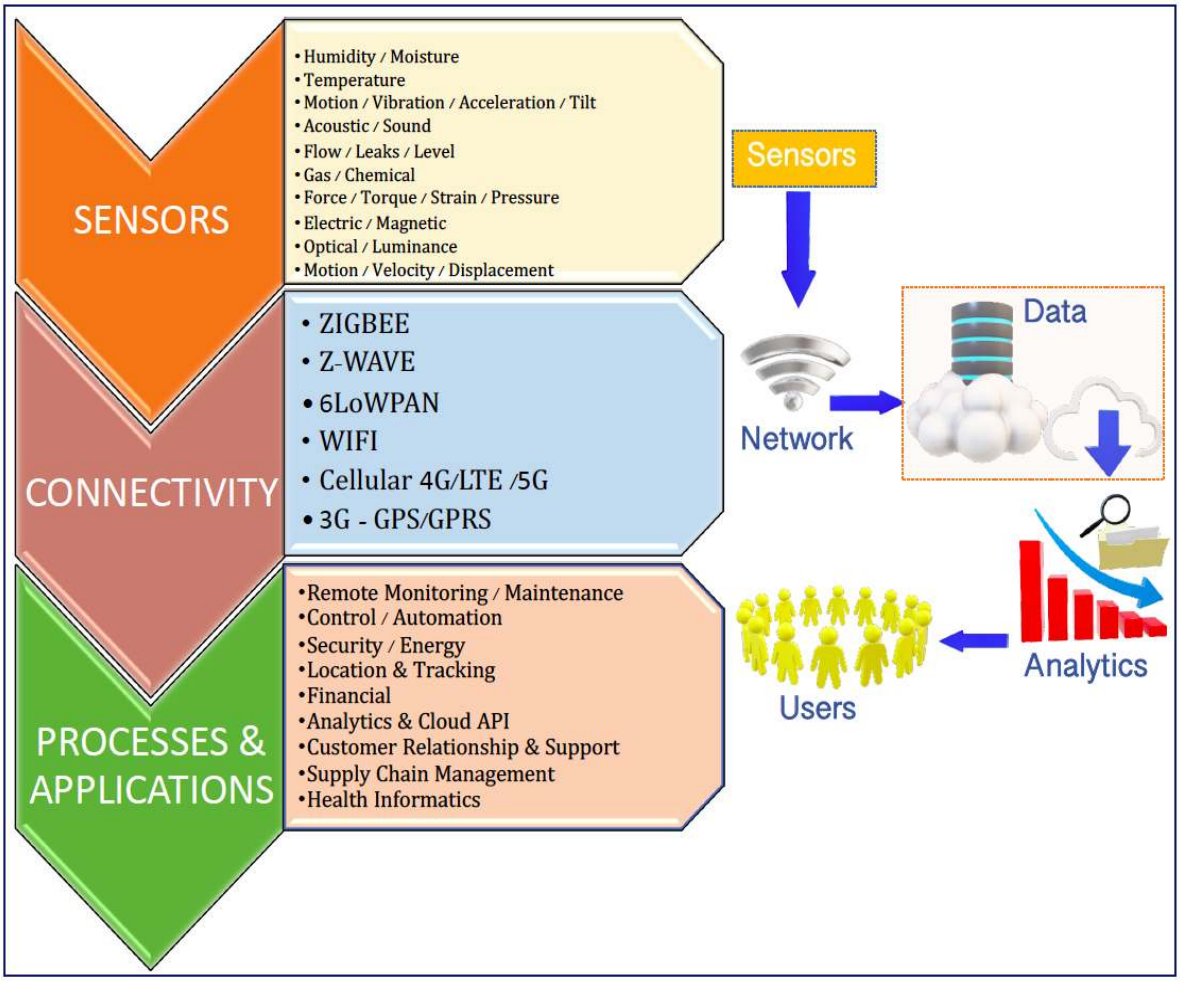

Figure 1. Abstraction of the Internet of Things (IoT) architecture.

IoT has proved to be a productive technology in many sectors like industry, community and academia. IoTs have lately become the main topic of research in the wider research community. Currently, the global Internet of Things market has reached a value of US $9.1 billion and according to [8,9] the Compound Annual Growth Rate (CAGR) is growing at 40% leading to year 2024. It is estimated that by the year 2020, on average, every person will own seven IoT-based communications devices [10]. In the automobiles industry by the year 2020, over 23.6 million cars will have internet access. According to the Verizon report [11], the global Internet of Things market is expected to grow at a projected pace of 17% to reach US $1.3 trillion. In the area of agriculture, the IoT-based digital precision agriculture services are expected to reach US $4.5 billion worldwide by the year 2020 [12]. The ability of IoT to monitor in real-time and the relative ease of use has opened up, to researchers, a whole new range of using IoT in many applications. The compendium of in-situ sensors that are embedded within the IoT devices are the fundamental components that collect valuable raw data. The correct operation of the sensors within the IoT device plays a vital role in the overall performance of the system and the dependent processes, applications[13]. The IoT sensors are often deployed in harsh environments; guaranteeing the sensor's correct operation and predicting malfunctions, however, is quite difficult. Additionally, sensors within the IoT typically are the most inexpensive electronic components typically prone to malfunctions.

A malfunctioning sensor produces corrupted data or erroneous readings or conflicting information to the IoT device [14]. When the IoT processes this corrupted sensor data, the overall performance of the IoT system is compromised, making it inaccurate and unreliable. The recently growing trend of automating many processes, like autonomous driving vehicles to reduce the number of crashes, emphasises the importance of the correct operation of sensors that are operating within the system. As the IoT systems work continuously, generating large volumes of multi-modal data, ensuring the accurate operation of the sensors within the IoT is critical and there should be a precise monitoring process in place to verify the behaviour and performance of the sensors within IoT. Additionally, this sensor monitoring process has to be automated, scalable and needs to be agile enough to be used for the streaming of raw data produced by the numerous sensors embedded within the IoT device. This monitoring process, commonly referred to as the sensor outlier detection, is known to detect any anomaly or deviation in the sensor's readings and is usually one of the key processes that influence the quality of the data collected by the sensor. Of late, within the research communities, the detection of outliers is of great interest [15–18].

However, much of the current research on outlier detection is in the area of Wireless Sensor Networks (WSN) and is also used widely for fraud detection, network security breaches, target tracking, environmental and health monitoring. However, adequate research has not been done in identifying the sensor outliers in the context of IoTs. The unique characteristics of IoTs, when compared with WSN, shows that the traditional outlier detection techniques are not directly applicable to IoTs. Usually, an IoT is a compendium of multiple-similar sensors embedded as a unit capable of producing huge amounts of spatial–temporal data at low latency, unlike the WSN [19]. When there is erroneous data produced by one kind of sensing unit within the IoT caused by the failure or malfunctioning of one sensor out of a pair, identifying the faulty sensor to make the data provided by that sensor redundant in real-time, whilst allowing the data produced by the secondary similar intact sensor plays an essential role in the correct functioning of the IoT device. The contribution of the survey in this paper is presented as follows,

- Section 2 presents the research methodology adopted for determining the sensor faults, errors, outliers relevant to the Internet of Things and Wireless Sensors Networks,
- Fundamental differences between the IoTs and WSN are presented in Section 3,
- Introducing the fundamentals of sensor outlier detection in IoT and the related existing research in this are is presented in Section 4,
- Relevant outlier detection techniques that can be used for IoTs and their pros and cons are discussed in Section 5,
- A comparative analysis on the sensor failure detection and identification strategies is presented in Section 6, to help select an adequate sensor fault and outlier detection strategy for the IoT-based applications.
- A Multi-Agent Distributed Deep reinforcement learning based sensor sensor outlier detection for IoT is presented in the Section 7.
- The future research direction and some open research questions are discussed in Section 8

2. Research Methodology

The research methodology was categorised into three main stages. During the primary stage, information regarding the need for detecting sensor failures, errors were analysed using systematic literature review and by consulting the industry and companies with IoT-based products in the market.

In the second stage, critical analysis to understand the etymological differences between the IoT and the WSN relevant to sensor failures and errors was conducted. After determining the sensors functional and operational differences between the IoT and the WSN, in the final stage, relevant literature was thoroughly reviewed to obtain the sensor outlier and fault detection techniques that are appropriate for IoTs.

3. Differences between the IoTs and Wireless Sensor Networks

This section identifies and reviews several significant differences between IoTs and Wireless Sensor Networks (WSN). Much of the research has been done in developing the sensor outlier and fault detection models exclusively for the WSN, however, adequate research has not been done so far in the IoT context. As the wireless sensor networks and their operational framework differ greatly when compared to IoTs operational framework (shown in Figure 2, some of the existing models developed for WSN cannot be used on IoTs for detecting outliers and faults [20–22].

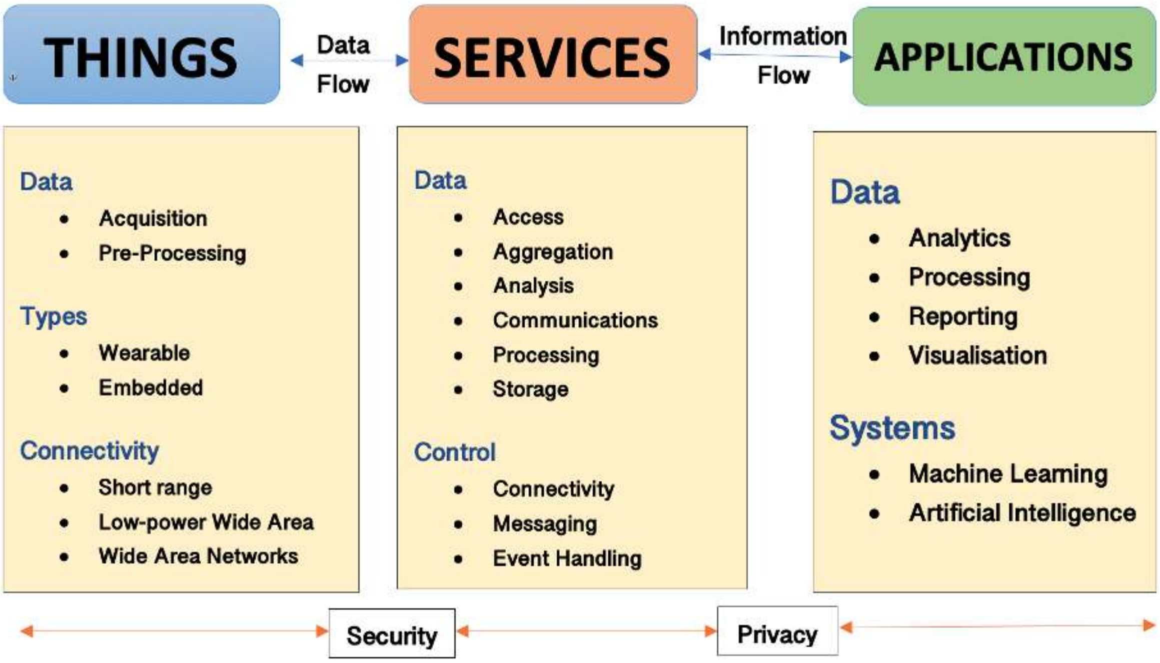

Figure 2. IoT's operational framework.

Figure 3 depicts a concept map based on the field of operations. The IoTs exists and operate at a higher level than the WSN's. Figure 3 depicts the WSN as a subset of IoT, since the WSN is a technological framework often used within an IoT system to capture physical phenomena data in a real-world setting. Unlike WSN, the IoTs have less amount of issues that are related to network failures, power shortages or node failures etc. However, the IoTs will be having their own set of unique issues (as discussed in the above sections), where only few types of existing outlier and fault detection techniques can be used.

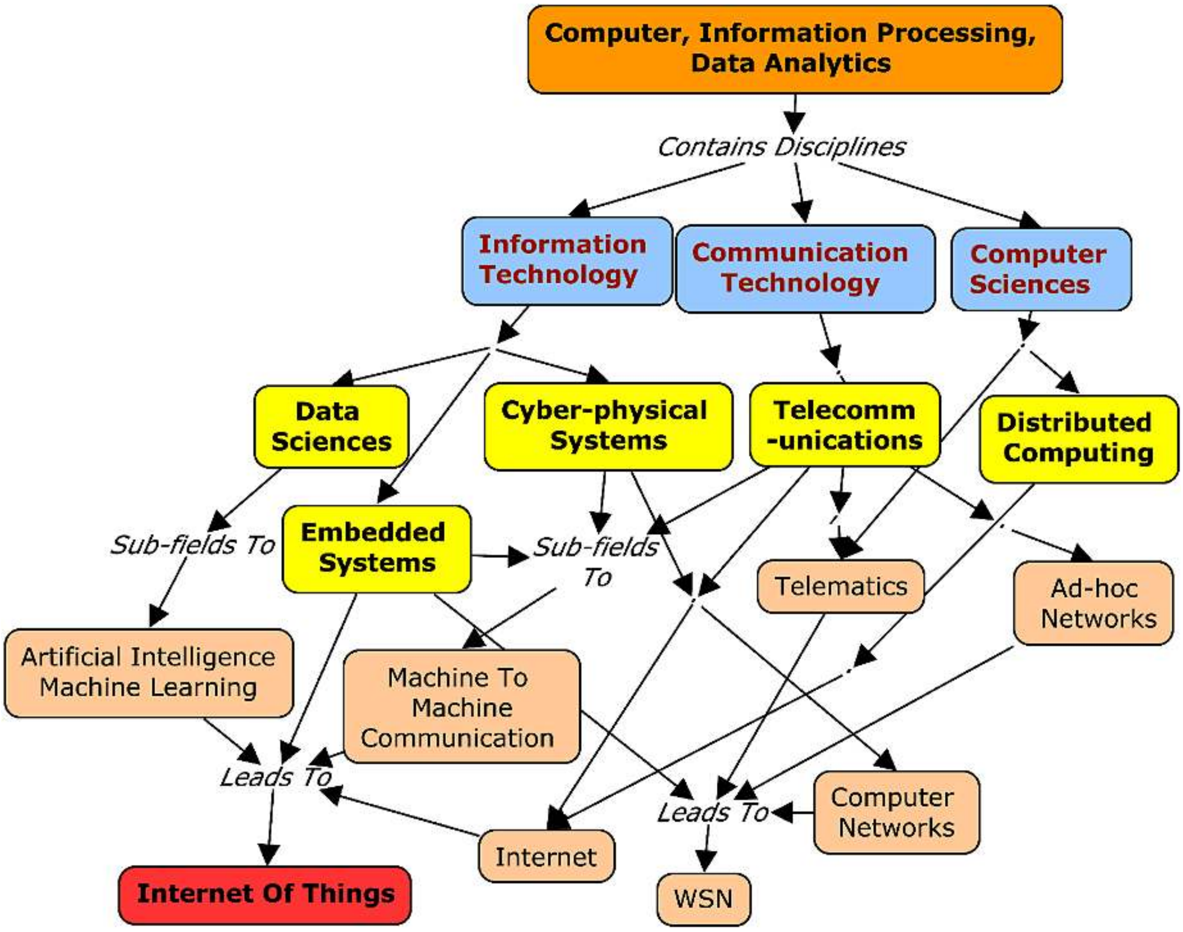

Figure 3. Etymological relationship/differences between IoT and WSN.

4. Outliers in IoT Context

In the context of IoTs, the sensor's outlier is commonly known to be an irregularity or a divergence in sensor behaviour during the process of cataloguing particular parameters or events when compared to its previous behaviour or readings. There is no standard confined definition for sensor outliers. Table 1 presents a set of comprehensive definitions stated in the literature for the sensor outliers in the IoT context.

Table 1. Definitions of sensor outliers in the IoT context.

Reference	Definitions
[23]	*"An outlier is an observation which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism"*
[24]	*"An outlier is a data point which is significantly different from other data points, or does not conform to the expected normal behaviour, or conforms well to a defined abnormal behaviour."*
[25]	*"A spatial-temporal point whose non-spatial attribute values are significantly different from those of other spatially and temporally referenced points in its spatial or/and temporal neighbourhoods is considered as a spatial-temporal outlier."*
[26]	*"An outlier is an observation or subset of observations that appears to be inconsistent with the rest of the set of data"*

4.1. Main Sources for Sensor Outliers that are Relevant to the IoT Context

There are three main causes of sensor outliers that are relevant to the IoT as shown in Figure 4.

- Intrinsic Sensor Errors: This kind of error is associated with impaired readings or measurements coming from a faulty sensor which is embedded within an IoT device. As the sensors are electronic components, they often fail suddenly and stop working without any indication of degrading performance [26–28]. This kind of sensor failure feeds in either no readings or null readings to the data processing algorithm within the IoT system [23]. Some literature identified this kind of sensor failure as "Binary failure".

- Sensor Events: As the sensor is deployed to collect the data in real-world scenarios or events, there is a probability of unprecedented change in the event caused by unlikely situations that severely affects the sensor thereby causing outliers. For example, an IoT system with multiple sensors monitoring temperature and humidity levels in a farm, if a worm crawls on one of the sensors, the farmer will be getting readings on how moist and warm the worm is, these readings will be ineffectual for the system and hinders the performance of the whole monitoring IoT system.
- Intermittent Sensor Errors: The last category of sensor failure is the intermittent errors that mare majorly caused due to sporadic events like theft, malicious attack and tampering with the sensor [29–31]. A situation where a loose connector in the sensor or elsewhere within the sensing hardware could also cause the sensor to produce intermittent sparse data to the data processing algorithms [32].

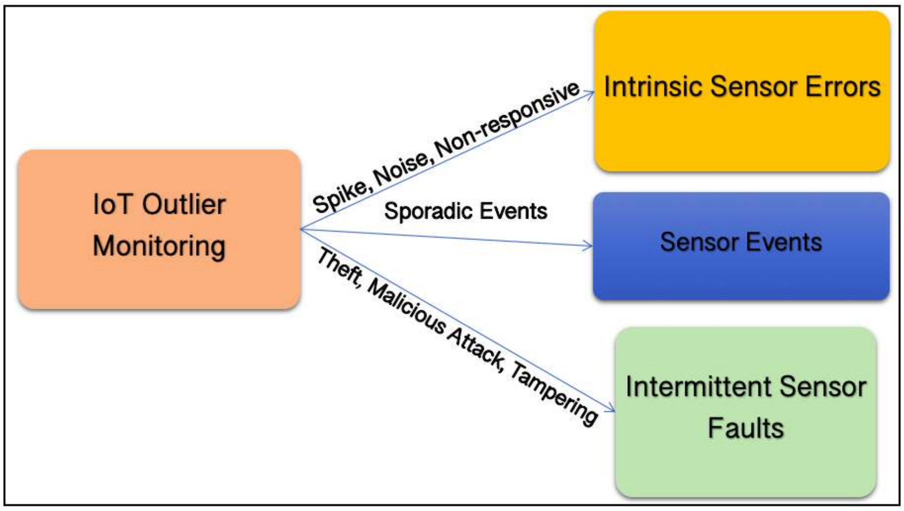
IoT Outlier Monitoring
Spike, Noise, Non-responsive
Intrinsic Sensor Errors
Sporadic Events
Sensor Events
Theft, Malicious Attack, Tampering
Intermittent Sensor Faults

Figure 4. Sensor outlier sources in IoT.

5. Sensor Faults and Outlier Detection Models for IoTs

Sensor failure detection and outlier identification in an IoT context started to gain considerable attention in the research community. In general, there are five macro-classes of automatic sensor outlier and failure detection techniques that can be used in an IoT context as shown in Figure 5. In this section, the sensor fault and outlier detection techniques for IoTs are discussed, based on the disciplines like statistical-based techniques, nearest-neighbour-based techniques, machine learning and artificial intelligence-based techniques, clustering-based techniques and classification-based techniques.

5.1. Statistical Techniques

Statistical-based techniques were the first algorithms used for sensor faults detection and outlier detection by many researchers. In this technique, the data from the sensors are modelled by employing a stochastic distribution. The data points from sensors can be identified as outliers or faults when the likelihood of the data instance that is generated by this model is very low. This technique uses previous sensor measurements to approximate and build a model of the accurate behaviour of a sensor. However, whenever the new measurement from the same sensor is registered, this data point is then compared to the model to check if the new data point statistically incompatible with the model. If the model is incompatible with new sensor reading, it is then marked as outlier or a faulty measurement.

A statistical window based approach typically assists in decreasing the number of false positives of the faults and outliers. The low–high pass filter is an example of the basic statistical technique that classifies the sensor readings as faults or anomalies based on working out the average of past measurements and measuring how different the new readings are.

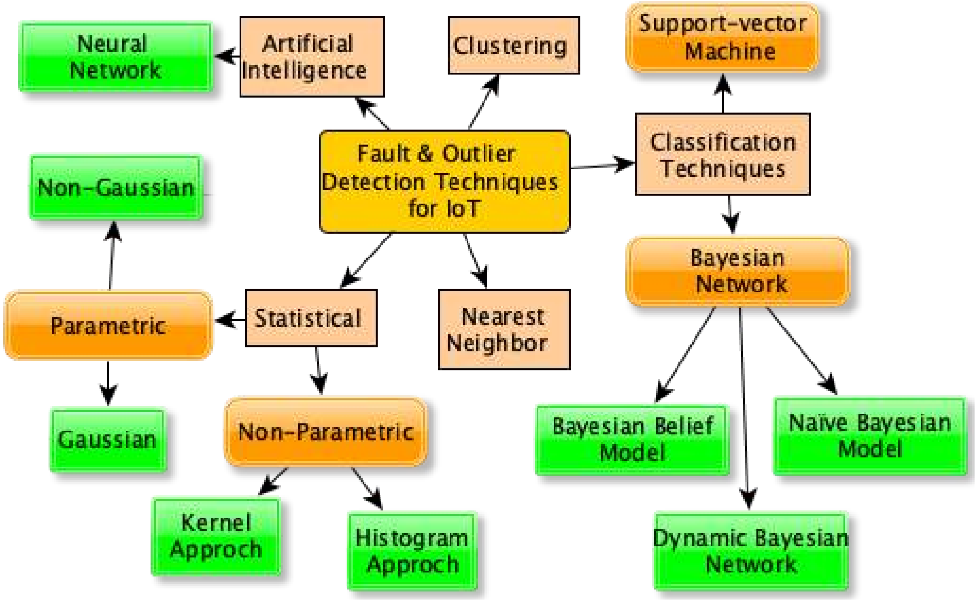

Figure 5. Taxonomy of fault and outlier detection models for IoT.

A statistical technique based on the spatio-temporal data interdependence's of sensor data is proposed by Hida et al. [30]. This technique mostly utilises two statistical tests, to locally detect outliers to make simple aggregation processes more reliable. Statistical models are relevant to quantitative data sets of real-value or at the very least is a quantitative data distribution that needs to be converted to a suitable numerical value for the numerical treatment. As the complexity and the amount of the sensor data increases (as it is common in the case of IoT), this model will take a longer time processing to convert the complex data.

5.2. Nearest-Neighbour Techniques

Nearest-neighbour-based technique is the widely used technique to analyse the sensors' data point concerning its nearest neighbours. Basically, the nearest-neighbour technique for sensor fault and outlier detection explicitly relies on the notion of proximity. The nearest-neighbour technique works by relying on the distances between sensor data measurements to differentiate between the abnormal and correct readings. The Local Outlier Factor (LOF) is a prominent nearest-neighbour algorithm [33], which attributes a fault or the outlier score to each sensor reading based on the number of measurements around its k-nearest-neighbours and the number of measurements around the sensor reading. The sensor readings with the higher scores are labelled as anomalies.

5.3. Artificial Neural Network Techniques

Neural networks and fuzzy logic are the recent approaches for detecting the sensor faults and the outliers in the IoT context. The neural network technique is a logical model that renders a comprehensive idea that aids the decision making the process by analysing the whole sensor data set [34,35]. Whereas the fuzzy logic technique allows transition values (like right/wrong, yes/no, high/low) to demarcate between the standard/correct sensor readings. In IoTs, the fuzzy logic approach can be used to improve decision making, enhance the clustering head selection, improve network security and data aggregation, efficiently deal the routing, MAC protocols, quality of service and ultimately efficient detection of sensor faults and the outliers.

5.4. Cluster-Based Techniques

Cluster-based analysis [36] is a popular approach within the area of the data mining community that groups related data instances into clusters of similar behaviour. By partitioning the data into clusters of similar data points from sensors in which each data cluster contains data points that are similar to one another and are different from the data points in other groups of clusters. This approach is a subset of the proximity techniques. The initial readings from sensor/s are first used to create the clusters and then the new sensor measurements that are allocated to small and remote data clusters or sensor measurements that are very far from the primary cluster's centroid are marked as abnormal readings.

5.5. Classification-Based Techniques

Classification-based techniques are important precise methods in data mining and machine learning. Classification techniques aim to identify a classification model (named as a classifier) using a collection of designated sensor data points (training points) and then classify obscure data instances into one of the learned (normal/outlier) group. This type of technique requires constant updating to accommodate the new sensor data that belongs to a normal class. In the case of IoTs, this classification technique is adequately suited for the faults and outlier detection as this technique tends to operate under the common assumption that a classifier could be learned from a provided space feature to identify normal and outlier classes [37]. In order to make this technique, it needs to be devised into two stages which are training and experimenting [38]. In the training phase, the technique aims at learning a classifier using the available labelled training data followed by an experimenting phase that classifies a test instance as regular or an outlier or a sensor fault [39,40].

5.6. Comparison of Fault and Outlier Detection Techniques for IoTs

Even though the above-discussed techniques for sensor fault and outliers detection for IoTs have been recently tried by some researchers to achieve high accuracy, however, each one of the techniques has pros and cons as discussed below.

5.6.1. Statistical Techniques

Pros:

- Can efficiently identify any sensor faults and outliers in an IoT once a proper probability distribution model is obtained.
- The sensor faults and outliers can be detected by using temporal correlation. Any unforeseen change in the data distribution immediately decreases the temporal correlations thereby detecting outliers.

Cons:

- As the IoTs are often used in real-life settings, where there is often no previous sensor data distribution knowledge, the parametric statistical approach is not beneficial.
- The non-parametric statistical models are not suitable for data-intense IoTs working in a real-time setting.
- Often there is a high computational cost of managing multivariate data produced.

5.6.2. Nearest-Neighbour Techniques

Pros:

- Very simple to apply to various types of data produced by diverse sensors in an IoT system.

- Can be left unattended and are primarily required to define a proper distance measure for the given data.

Cons:

- When used on a complex multivariate data produced by IoT, the computation cost increases dramatically.
- Scalability of these types of models is a matter of concern, especially in the IoT context.
- Often produces a high false-negative rate for sensor faults and outlier detection.

5.6.3. Machine Learning Techniques

Pros:

- Can be used when the sensors produce poor, noisy and fragmentary data, as the inherent behaviour of this model generalises the produced data points.
- There is a limited need, sometimes no need, to re-train the model when there is new sensor data added.

Cons:

- The model requires fine-tuning and simulations before being made operational in a real-life setting.
- As this model is often rules-based, if the number of sensor data variables increases, this will also exponentially increase the number of rules.

5.6.4. Cluster Techniques

Pros:

- Once the clusters and new data points inserted into the system and tested for sensor faults and outliers, the model can easily be made to be adaptable to an incremental form.
- No supervision is needed.
- Very much suited for detecting sensor anomaly from the IoTs temporal data.

Cons:

- Is very computationally costly when working on multivariate sensor data for fault detection.
- Due to the models' high computational cost, it is unsuitable for inadequately resourced sensors.
- Cannot cope with any changes in the IoT data.

5.6.5. Classification Techniques

Pros:

- This model is not dependant on either a statistical model or on the estimated data parameters.
- Provides optimal and sometimes maximum identification of sensor faults and outliers.
- Can be used on multidimensional data to detect sensor outliers and faults.

Cons:

- This model is computationally complex when compared to clustering and statistical techniques.
- The model needs to train itself for new data points.

6. Strategies for Sensor Failure Detection and Identification

Automatic sensor failure detection and automatic identification can be done using three strategies: network-level strategy, homogeneous strategy and heterogeneous strategy.

6.1. Network-Level Strategy

By using network-level management and monitoring the network packets, this approach detects any sensor failures [41,42]. The sensors within the IoT systems effectively monitor each other in order to detect any problematic sensor/s. This approach primarily uses Markov models to characterise the normal and abnormal behaviour of sensors [43,44].

6.2. Homogeneous Strategy

The homogeneous strategy uses multiple sensors of the same type to identify and detect any sensor within the IoT systems, that tends to show abnormal behaviour [45]. By placing the same type of sensors that are generating similar values, spatially close to each other, this approach detects any uncorrelated behaviour thereby able to detect any faulty sensor. This type of sensors mainly uses Auto-Regressive Integrated Moving Average (ARIMA) time-series model to compare the predicted measure of the sensors with the reported sensor measurement [45,46].

6.3. Heterogeneous Strategy

The heterogeneous strategy tends to combine different types of data points from the sensor to detect sensor failure [47,48]. The strategy became popular lately with the development of IoT systems with various types of sensors embedded within. This strategy detects sensor failure by classifying the sensor outputs and then training the classifier to identify the same set of data points based on different subsets of sensors within the same IoT system [49].

7. Proposed IoT Sensor's Outlier Detection Model

The sensor malfunction diagnosis for IoTs has unique challenges, multi-agent distributed deep reinforcement learning-based sensor outlier detection is a machine learning technique that can be utilised for IoTs sensor malfunction diagnosis. Within the IoT module, the heterogeneous sensors will be connected to the Outlier Detection Module (ODM) and the microcontroller. The data produced by the sensors are sent to both ODM and microcontroller. The ODM is equipped with a PICAXE-08M2 microcontroller and the sensor outputs are connected to its IO ports.

The microcontroller will be monitoring the data from the sensors while executing the multi-agent deep reinforcement learning-based algorithm. The schematic of ODM module and IoTs modules main processing unit is shown below in Figure 6. The ODM ensemble, the heterogeneous sensors connected within the individual IoT module and the dynamics of each pair of heterogeneous sensors was modelled.

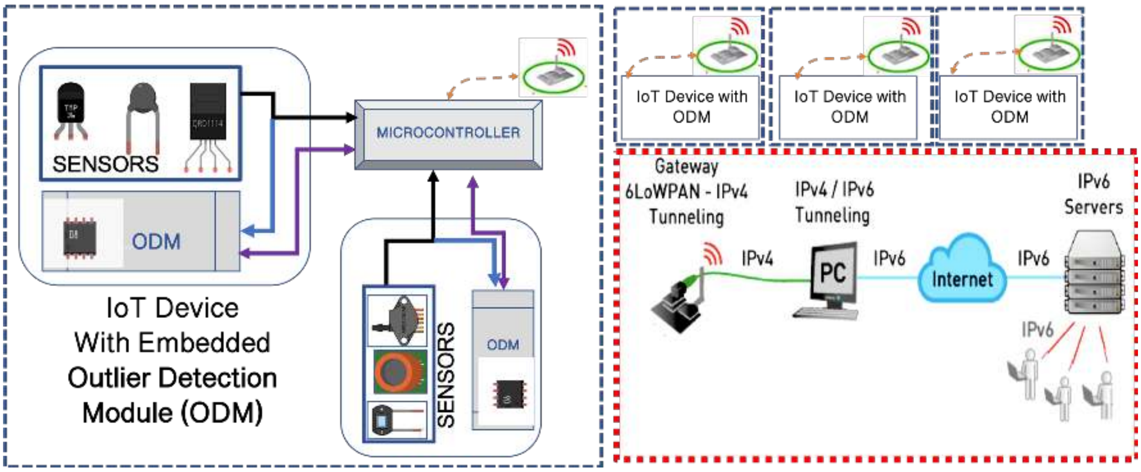

Figure 6. Outlier detection model for IoT sensors.

The multi-agent deep reinforcement learning uses multi-agents in learning and transfers learning between the agents [50,51]. Consider a set of heterogeneous sensors connected to a time-invariant IoT system. Even though the sensors within the IoT systems are diverse (in operation characteristics), all the responses from the sensors depend on the common physical system and a linear relationship exists between the physical parameters measured by these sensors. This relationship is utilised to evaluate the "optimal fitness" of the sensor measurements. In this method the agents (allocated for each sensor) share information to the dependent agents, to analyse the patterns.

Each individual agent within the ODM trains itself from the inputs, which are the outputs shared by other agents to check whether their outputs are consistent and have a linear relationship, as shown in Figure 7.

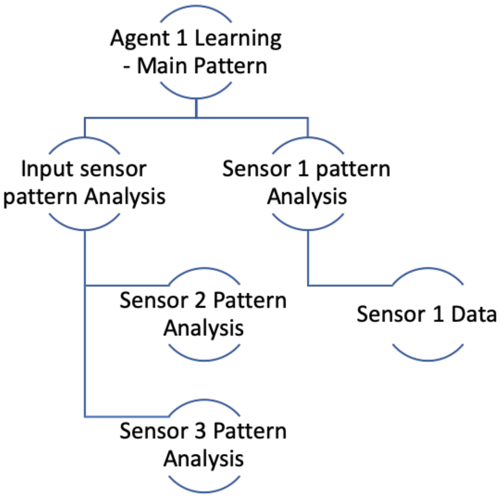

Figure 7. Learning process structure of an agent.

When the agents notice any inconsistencies in the linear relationships between the sensors (within individual IoT module), the ODM will identify the sensor outlier, fault or error. The pseudo-code of the implemented algorithm is shown below in Algorithm 1.

Algorithm 1: Multi-agent distributed deep reinforcement learning-based outlier detection.

```
Inputs: Sensor 1 data, Dependent sensor data (Sensor 2, Sensor 3,..., Sensor $n$)
Result: Sensor anomalies detection in an IoT module
Initialise the agent memory based on the previous patterns;
while TRUE do
    analyse the current and memory patterns;
    Check the main pattern and individual patterns of fellow sensors;
    if detects anomalies then
        check which sensor/s affected;
        check for noise/sensor failure/type of errors;
        share the anomaly information with other agents to get informed about the failure/s;
    else
        update and initialise the agent memory;
    end
    fellow agents verify the shared anomalies to confirm the error report;
    send alert for corresponding sensor to repair/replace;
    update the agent memory;
end
```

8. Future Research Direction

In this section, the open research questions and the future research directions in developing the sensor faults, outlier detection models for IoT is discussed. The future research is directed toward tackling three areas: analysing the sensor's produced spatial-temporal data in real time, developing IoT—sensors relevant to Outlier Detection Modules (ODM) and developing an IoT prototype with embedded ODM for testing, as shown in Figure 8 below.

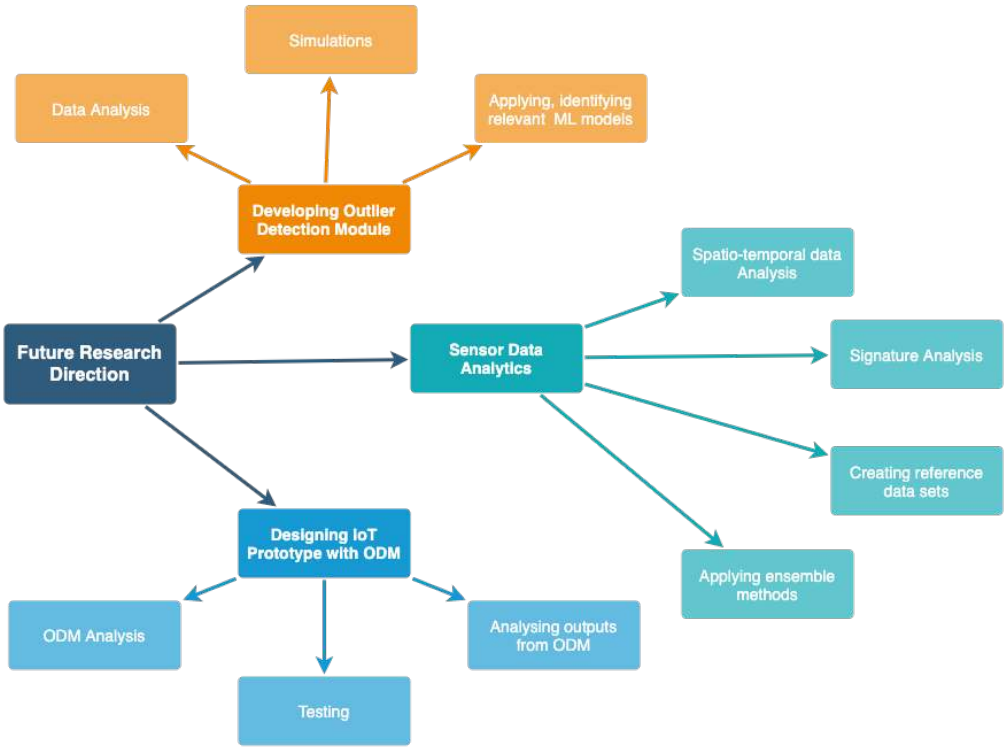
Simulations
Data Analysis
Applying, identifying relevant ML models
Developing Outlier Detection Module
Spatio-temporal data Analysis
Future Research Direction
Sensor Data Analytics
Signature Analysis
Creating reference data sets
Designing IoT Prototype with ODM
Applying ensemble methods
ODM Analysis
Analysing outputs from ODM
Testing

Figure 8. Future research directions in designing and developing Outlier Detection Modules (ODM) for the IoT.

The research will also be focused on investigating the computational possible bottlenecks in terms of the ODM. Furthermore, the whole IoTs performance and capacity in accurately identifying the malfunction sensor/s, the source and type of error affecting the sensor/s will be studied. It is anticipated that this research direction could raise many open research questions as follows,

- *What would happen if the ODM fails?*
- *How to check if ODM is functioning properly?*
- *When should it be used in critical IoT systems? Is there is a need to have a centralised ODM for checking the sensor's ODM's?*
- *How can the developed ML algorithm perform when used in different kinds of environments?*
- *Is there a need to have a standardised protocol for detecting IoT sensor's faults and outliers in this IoT-populated Industry 4.0 era?*

9. Conclusions

Detecting outlier and sensor fault or failures are extremely important in the Internet of things. In this paper, different outlier and sensor operational anomaly detection techniques are discussed in detail. As the Internet of Things are very different from the wireless sensor networks, there is a huge necessity for developing adequate protocols and techniques to address unique challenges and constraints of IoT. The paper discusses and provides an easier and concise summary of the techniques that could be used for detecting sensor outliers in IoT. This survey confers both the pros and cons of five outlier and fault detection categories.

A multi-agent distributed deep reinforcement learning-based outlier detection model is presented along with the required hardware and architecture. As for future work, we aim to elaborate and present a comparative study based on mathematical models, simulation results using IoT simulators and the experimental results. The aim of the research is to help choose a suitable method to provide the highest accuracy in detecting sensor faults and outliers in IoT context.

Author Contributions: Conceptualisation, A.G.; Data curation, A.G.; Investigation, A.G., T.W. and M.A.; Methodology, A.G., T.W., M.A. and J.G.; Resources, T.W. and M.A.; Writing—original draft, A.G.; Writing—review & editing, A.G. and J.G. All authors have read and agree to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Alkhatib, H.; Faraboschi, P.; Frachtenberg, E.; Kasahara, H.; Lange, D.; Laplante, P.; Merchant, A.; Milojicic, D.; Schwan, K. What will 2022 look like? The IEEE CS 2022 report. *Computer* **2015**, *48*, 68–76. [CrossRef]
2. Ukil, A.; Bandyoapdhyay, S.; Puri, C.; Pal, A. IoT healthcare analytics: The importance of anomaly detection. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 994–997.
3. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
4. Ibarra-Esquer, J.E.; González-Navarro, F.F.; Flores-Rios, B.L.; Burtseva, L.; Astorga-Vargas, M.A. Tracking the evolution of the internet of things concept across different application domains. *Sensors* **2017**, *17*, 1379. [CrossRef] [PubMed]
5. Dai, H.N.; Wang, H.; Xu, G.; Wan, J.; Imran, M. Big data analytics for manufacturing internet of things: Opportunities, challenges and enabling technologies. *Enterp. Inf. Syst.* **2019**, 1–25. [CrossRef]
6. Gaddam, A.; Lundqvist, K.; Citizen, J.; Calixto, D. IoT and wireless sensor network for interactive waka structure. In Proceedings of the 2017 Eleventh International Conference on Sensing Technology (ICST), Sydney, NSW, Australia, 4–6 December 2017; pp. 1–4.
7. Gaddam, A.; Al-Hrooby, M.; Esmael, W. Designing a wireless sensors network for monitoring and predicting droughts. In Proceedings of the 8th International Conference on Sensing Technology, Liverpool, UK, 2–4 September 2014; pp. 210–215.

8. Perera, C.; Liu, C.H.; Jayawardena, S.; Chen, M. A survey on internet of things from industrial market perspective. *IEEE Access* **2014**, *2*, 1660–1679. [CrossRef]
9. Bughin, J.; Chui, M.; Manyika, J. An executive's guide to the Internet of Things. *McKinsey Q.* **2015**, *4*, 92–101.
10. Nolan, K.E.; Guibene, W.; Kelly, M.Y. An evaluation of low power wide area network technologies for the Internet of Things. In Proceedings of the 2016 international wireless communications and mobile computing conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 439–444.
11. Javed, B.; Iqbal, M.W.; Abbas, H. Internet of things (IoT) design considerations for developers and manufacturers. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 834–839.
12. Madakam, S.; Ramaswamy, R.; Tripathi, S. Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164. [CrossRef]
13. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horizons* **2015**, *58*, 431–440. [CrossRef]
14. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
15. Goyal, N.; Dave, M; Verma, A.K. A novel fault detection and recovery technique for cluster-based underwater wireless sensor networks. *Int. J. Commun. Syst.* **2018**, *31*, 3485–3502. [CrossRef]
16. Mahmoud, S.M.; Lotfi, A.; Langensiepen, C. Behavioural pattern identification in a smart home using binary similarity and dissimilarity measures. In Proceedings of the 2011 7th International Conference on Intelligent Environments, Nottingham, UK, 25–28 July 2011. [CrossRef]
17. Xie, M.; Han, S.; Tian, B.; Parvin, S. Anomaly detection in wireless sensor networks: A survey. *J. Netw. Comput. Appl.* **2011**. [CrossRef]
18. Kullaa, J. Detection, identification, and quantification of sensor fault in a sensor network. *Mech. Syst. Signal Process.* **2013**. [CrossRef]
19. Ghorbel, O.; Abid, M.; Snoussi, H. Improved KPCA for outlier detection in Wireless Sensor Networks. In Proceedings of the 2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP 2014), Sousse, Tunisia, 17–19 March 2014; pp. 507–511. [CrossRef]
20. Ghorbel, O.; Jmal, M.W.; Ayedi, W.; Snoussi, H.; Abid, M. An overview of outlier detection technique developed for wireless sensor networks. In Proceedings of the 2013 10th International Multi-Conference on Systems, Signals and Devices (SSD 2013), Hammamet, Tunisia, 18–21 March 2013. [CrossRef]
21. Zhang, Y.Y.; Chao, H.C.; Chen, M.; Shu, L.; Park, C.H.; Park, M.S. Outlier detection and countermeasure for hierarchical wireless sensor networks. *IET Inf. Secur.* **2010**, *4*, 361. [CrossRef]
22. Ayadi, A.; Ghorbel, O.; Obeid, A.M.; Abid, M. Outlier detection approaches for wireless sensor networks: A survey. *Comput. Netw.* **2017**, *129*, 319–333. [CrossRef]
23. Sharma, A.B.; Golubchik, L.; Govindan, R. Sensor faults. *ACM Trans. Sens. Netw.* **2010**. [CrossRef]
24. Thierer, A.; Castillo, A. *Projecting the Growth and Economic Impact of the Internet of Things*; George Mason University: Arlington, VA, USA, 2015. [CrossRef]
25. Branch, J.W.; Giannella, C.; Szymanski, B.; Wolff, R.; Kargupta, H. In-network outlier detection in wireless sensor networks. *Knowl. Inf. Syst.* **2013**. [CrossRef]
26. Pachauri, G.; Sharma, S. Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms. *Procedia Comput. Sci.* **2015**. [CrossRef]
27. Ye, J.; Stevenson, G.; Dobson, S. Detecting abnormal events on binary sensors in smart home environments. *Pervasive Mob. Comput.* **2016**. [CrossRef]
28. Afsar, M.M.; Tayarani-N, M.H. Clustering in sensor networks: A literature survey. *J. Netw. Comput. Appl.* **2014**. [CrossRef]
29. Li, X.; Huang, S.; Yin, S.; Zhou, Y.; Zhang, M.; Zhao, Y.; Zhang, J.; Gu, W. Design of K-Node (Edge) Content Connected Optical Data Center Networks. *IEEE Commun. Lett.* **2016**, [CrossRef]
30. Hida, Y.; Huang, P.; Nishtala, R. *Aggregation Query under Uncertainty in Sensor Networks*; Tech. Rep; Department of Electrical Engineering and Computer Science, University of California: Berkeley, CA, USA, 2004.
31. Hnat, T.W.; Srinivasan, V.; Lu, J.; Sookoor, T.I.; Dawson, R.; Stankovic, J.; Whitehouse, K. The hitchhiker's guide to successful residential sensing deployments. In Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (SenSys '11), Seattle, WA, USA, April 2011. [CrossRef]

32. Van Zoest, V.M.; Stein, A.; Hoek, G. Outlier Detection in Urban Air Quality Sensor Networks. *Water Air Soil Pollut.* **2018**. [CrossRef] [PubMed]
33. Ahmed, M.; Naser Mahmood, A.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, [CrossRef]
34. Munir, S.; Stankovic, J.A. FailureSense: Detecting sensor failure using electrical appliances in the home. In Proceedings of the 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2014), Philadelphia, PA, USA, 28–30 October 2014. [CrossRef]
35. Jun, H.B.; Kim, D. A Bayesian network-based approach for fault analysis. *Expert Syst. Appl.* **2017**. [CrossRef]
36. Bharti, S.; Pattanaik, K.K.; Pandey, A. Contextual outlier detection for wireless sensor networks. *J. Ambient. Intell. Humaniz. Comput.* **2019**. [CrossRef]
37. Balaban, E.; Saxena, A.; Bansal, P.; Goebel, K.F.; Curran, S. Modeling, detection, and disambiguation of sensor faults for aerospace applications. *IEEE Sens. J.* **2009**. [CrossRef]
38. Zheng, H.; Feng, Y.; Gao, Y.; Tan, J. A robust predicted performance analysis approach for data-driven product development in the industrial internet of things. *Sensors* **2018**, *18*, 2871. [CrossRef]
39. Choi, J.; Jeoung, H.; Kim, J.; Ko, Y.; Jung, W.; Kim, H.; Kim, J. Detecting and identifying faulty IoT devices in smart home with context extraction. In Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2018), Luxembourg, 25–28 June 2018. [CrossRef]
40. Rajasegarar, S.; Leckie, C.; Palaniswami, M. Anomaly detection in wireless sensor networks. *IEEE Wirel. Commun.* **2008**. [CrossRef]
41. Chen, B.R.; Peterson, G.; Mainland, G.; Welsh, M. Livenet: Using passive monitoring to reconstruct sensor network dynamics. In Proceedings of the International Conference on Distributed Computing in Sensor Systems, Santorini, Greece, 11–14 June 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 79–98.
42. Kodeswaran, P.; Kokku, R.; Sen, S.; Srivatsa, M. Idea: A system for efficient failure management in smart IoT environments. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2016), Singapore, 15–19 June 2016. [CrossRef]
43. Duche, R.N.; Sarwade, N.P. Sensor node failure detection based on round trip delay and paths in WSNs. *IEEE Sens. J.* **2013**, *14*, 455–464. [CrossRef]
44. Ni, K.; Srivastava, M.; Ramanathan, N.; Chehade, M.N.H.; Balzano, L.; Nair, S.; Zahedi, S.; Kohler, E.; Pottie, G.; Hansen, M. Sensor network data fault types. *ACM Trans. Sens. Netw.* **2009**. [CrossRef]
45. Ding, M.; Chen, D.; Xing, K.; Cheng, X. Localized fault-tolerant event boundary detection in sensor networks. In Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005; Volume 2, pp. 902–913.
46. Fang, L.; Dobson, S. Unifying sensor fault detection with energy conservation. In Proceedings of the International Workshop on Self-Organizing Systems, Palma de Mallorca, Spain, 9–10 May 2013; Springer: Berlin/Heidelberg , Germany, 2013; pp. 176–181.
47. Kapitanova, K.; Hoque, E.; Stankovic, J.A.; Whitehouse, K.; Son, S.H. Being SMART about failures: Assessing repairs in SMART homes. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, PA, USA, 4–9 September 2012; pp. 51–60.
48. Stella Mary, P.; Arockiam, L. A Robust Architecture for Detecting Outliers in IoT Data using STCPOD Model. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2017**, 2, 659–664.
49. Wang, C.; Vo, H.T.; Ni, P. An IoT Application for Fault Diagnosis and Prediction. In Proceedings of the 2015 IEEE International Conference on Data Science and Data Intensive Systems, Sydney, NSW, Australia, 11–13 December 2015. [CrossRef]
50. Smith, P.; Hunjet, R.; Khan, A. Swarm learning in restricted environments: An examination of semi-stochastic action selection. In Proceedings of the 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV 2018), Singapore, 18–21 November 2018; pp. 848–855. [CrossRef]
51. Mousavi, S.S.; Schukat, M.; Howley, E. Deep reinforcement learning: An overview. In Proceedings of the SAI Intelligent Systems Conference, London, UK, 21–22 September 2016; Springer: Cham, Switzerland, 2016; pp. 426–440.