Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

Fog Computing-Based 5G LPWAN Anomaly Detection for Smart Cities

R. Santhana Krishnan

Assistant Professor, Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Cheranmahadevi, Tirunelveli, India

E-mail: santhanakrishnan86@gmail.com

Abstract

Known for excellent convenience and abundant facilities, smart cities offer CCTV, delivery robots, security robots, and so on to its residents. Along with the collaboration of IoT (Internet Of Things), the innovation of smart city has gained immense attraction at present. Besides, the risks and challenging in the field of telecommunication still persists as the implemented wireless networks results in traffic and anomaly behaviour. Such issues become critical in case of large-scale infrastructure networks like WSN's. As such circumstances, to perform efficient health and environment monitoring, the need for a next generation networked system raises. As the traditional anomaly detection schemes doesn't work out for delay-sensitive environments due to increased latency, we propose a scalable, hybrid spatiotemporal anomaly detection approach that can effectively detect potential anomalies in the network. With the use of real-time stream processing, and other methodologies like Software-Defined Networking (SDN), a Fog Computing-based 5G low-power Wide Area Network (LPWAN) solution is developed and tested on a Antwerp's City of Things testbed. The proposed approach is found to be beneficial when deployed in a real network environment with nearly 1800 sensor nodes.

Keywords: Anomaly detection, sensor nodes, WSN, smart city, IoT, fog computing, infrastructure networks

1. Introduction

At present, smart city is becoming a reality where a person's quality of life is enhanced by offering services that is based on data gathered from sensing network, and IoT. Besides, the gathered data is also useful for the public administration in providing additional services, efficiency, and cost reduction. For efficient working, latest technology, and

DOI: https://doi.org/10.36548/jucct.2022.3.003
Received: 19.07.2022, received in revised form: 18.08.2022, accepted: 04.09.2022, published: 15.09.2022

advanced communication protocols are implemented for the data-driven management purpose. For urban data gathering, WSN, and RFID cards are used. For fulfilling the innovation effort and emergence of new applications, Wireless Sensor Network (WSN) is best suited for deployment on streets. Although such deployments offer surplus benefits, security issues and attacks in the control systems has caused a huge impact as per studies in United States [1, 2] where the lack of cryptographic and authentication systems in WSN was the primary cause.

Another cause for such anomalies in network is due to external outsourcing public services. Induced by two factors like – 1. Lack of visibility over the potential security threats, and 2. Loss of control over network devices, outsourcing in terms of both administration and deployment has increased the chances of anomalies. Even though security countermeasures and system logs are operated in a correct manner by external providers to overcome the issue, the smart city administrators find difficulty in analysing and interpreting whether the received data is precise or accurate. As per the survey by Royal Academy of Engineering [3], it is found that data quality is one of the six major barriers that affect the smart city infrastructure and implementation. To improve the data quality, implementing the appropriate anomaly detection technique is mandatory to ensure smoother functioning of the network or the process. The basic process or overview of the procedure followed in WSN-based anomaly detection is given in Figure 1.

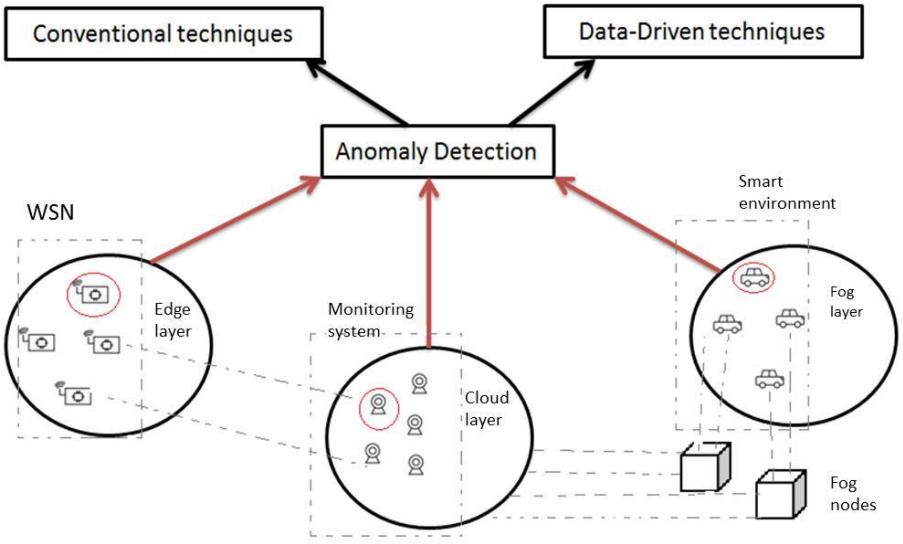

Figure 1. Basic Anomaly detection process

When it comes to smart city, carrying out anomaly analysis with the help of network status information is quite challenging task as there might be multiple WSN deployments

operating on different objectives. Also, when different WSN's are operating in different parts of the city at same time, it is hard for the external providers to provide exact and correct details to the council administrators. Taking into account of all the above-discussed challenges and risks, a Fog Computing-based 5G low-power Wide Area Network (LPWAN) solution is presented in this paper. This architecture is designed for "Antwerp's City of Things" testbed and tested for the Air Quality monitoring application carried out in a smart city.

2. Related Works

As an effort to carry out the anomaly detection process in smart cities, various techniques are available where a few are discussed in this section. The authors in reference [4] have proposed a real-time Intrusion Detection System integrated with mini-firewall for WPAN network with IoT feature. For car parking in smart city, a temporal clustering-based method is presented by Zheng in [5]. When it comes to smart city concept, the use and management of smart grid plays a vital role. Where, the authors in [6] have presented a supervised statistical-based anomaly detection scheme for interpreting the smart grid data.

Another milestone in the inference and focus on anomaly detection are the smart city-based research projects where SOCIOTAL project discussed in reference [7] is the best example. Completely oriented on hyperellipsoidal models, unusual patterns in environmental data gathered from the deployed IoT sensors are identified effectively. Likely, following the same methodology, the cloud platform is replaced by the Fog-computing approach in [8] by Rathore et.al. If it is to reduce latency and energy conservation in a sensor network, another Fog-based detection scheme employing hyperellipsoidal clustering algorithm is found to be beneficial that is oriented on simulation studies. Also, reference [9, 10] elaborates about the City Pulse project that gives an overall view regarding the various analytics tools used in different phases like data aggregation, decision support, and event detection.

Challal et.al [11] proposes a secured mechanism based on path redundancy that provides varied features like fault & intrusion tolerance routing scheme. Its performance was also compared with the similar techniques pertaining to factors like resiliency, energy consumption, and failure. Asymmetric cryptographic techniques are potential to defend the integrity attacks where in reference [12], the authors have developed a SSL protocol for wireless sensor network infrastructure.

3. Proposed Work

The process of detecting unexpected behaviour or abnormal patterns in dataset or collected information is called as outlier or anomaly detection. Previously, such detection techniques were used to remove the outliers and were also termed as data cleansing. Anomaly detection is classified into three types: 1. Supervised, 2. Semi-supervised, and 3. Unsupervised.

- Supervised: In the supervised detection method, a fully labelled training set is utilized where each sample is considered as abnormal or normal. If anomalies are known beforehand, this category can be used and hence is application-specific.

- Semi-Supervised: In this category of detection, the training set comprises of small amount of labelled and unlabelled samples.

- Unsupervised: If anomalies aren't known in advance, unsupervised detection algorithms can be used. No training set is required in this category and hence estimation on normal and abnormality is given as final result. There are many types of unsupervised anomaly detection methods available like Scikit-Learn that are usually developed by coding language like Python.

In the proposed work, unsupervised clustering anomaly detection methodology is used where the fog computing paradigm is introduced in place of the computational resources on the edges of each network. Such arrangement reduces latency and offers high mobility. For the IoT applications, centralized solutions are not suitable as enormous volume of data is generated and hence in the work, IoT sensors communicate with the gateway linked to the fog layer. The fog resources in turn communicate with the cloud layer that forms the top-level management module. Every IoT application is to be allocated with a particular set of computational resources.

In a traditional anomaly detection process, the sensors directly send the data to the cloud followed by implementation of detection algorithm within the cloud. But, in the present proposed system, every IoT sensor sends its sensed data to any one of the fog resource and the detection tasks takes place. If unusual or abnormal behaviour is noticed in the received data, the fog resource sends alert to the cloud layer. Finally all the fog resources send data to the cloud layer that is combined to carry out the global anomaly detection operation. The

final result is then displayed on the central dashboard in control room. Figure 2 shows the overall high-level process taking place in the proposed work.

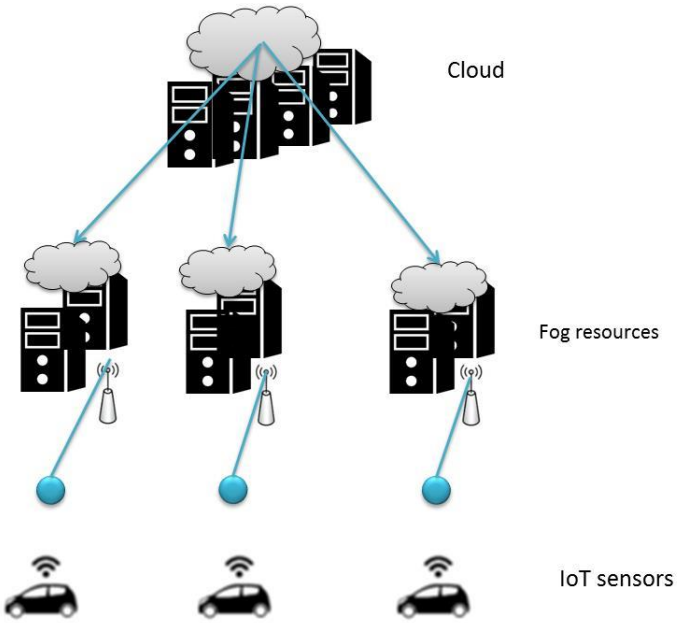

Figure 2. High-level view of the proposed anomaly detection method

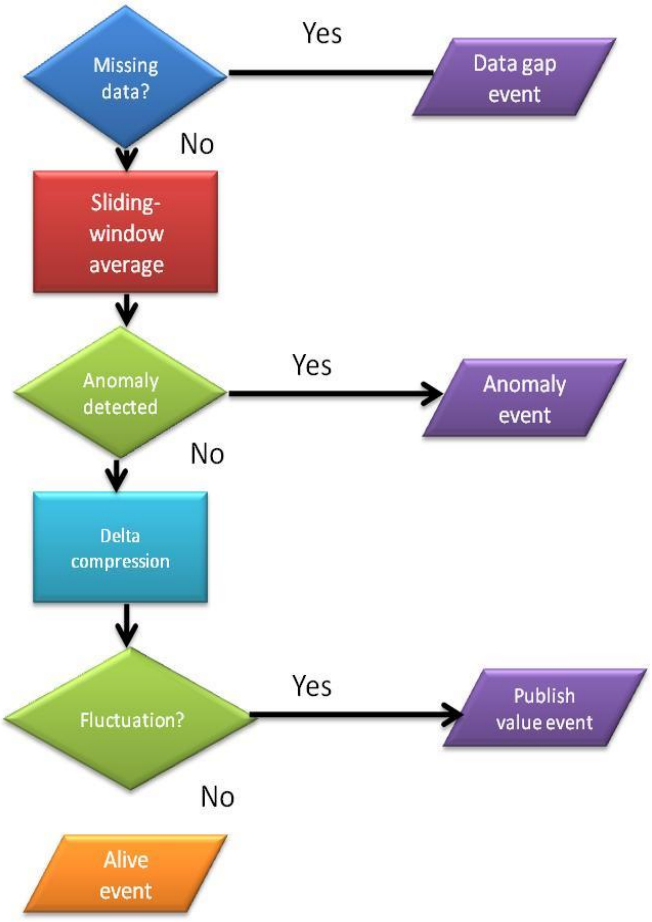

Figure3. Flow chart of the proposed scheme

To tackle new business opportunities, and fulfil the stringent requirement related to IoT applications, 5G enhanced LPWAN architecture is the best choice. The detailed flowchart of the entire process is given in Figure 3 if the fog resource finds that a data is missing, it checks the sliding window average followed by Mini-LISA computations. If the anomaly isn't detected though, delta compression is followed and the decision is taken accordingly.

For the LPWAN dimensioning, different variables are used and for the architecture purpose, for resources are placed within one hop from the IoT sensors. The upload and download transmission time of the packet is expressed in the below equation:

$$T(upload) = \frac{N}{U}$$

$$T(download) = \frac{N}{D}$$

The propagation time of the packet in a network is given by,

$$P = \frac{C}{3 * 10^8}$$

The total packet delivery time is calculated by the equation:

$$L = T + P$$

Where,

T = Transmission time of a packet,
N = Number of bits Rate in kbps,
U = Upload Data Rate in kbps,
D = Download Data Rate in kbps
P = Propagation time of a packet,
C = Communication range in kms
L = Packet Delivery Time

4. Results and Discussion

The proposed system is evaluated based on the use case that covers the "Antwerp's City of Things" testbed. As discussed above, the introduced concept is tested for the air quality monitoring application that is able to detect harmful traces of compounds in the environment and alert the citizens on air pollution levels. To carry out the evaluation, air quality sensors are mounted on the top of cabs that belong to a private company. Assigned

with the primary tasks of sensing the humidity, and temperature, GPS locations are enabled to know their locations as well. LoRAWAN, DASH7, and SigFox are the three LPWAN technologies used for the communication between the employed IoT sensors. Also, in terms of software, the evaluation is carried out in Python using Scikit-Learn. Figure 4 illustrates the result regarding the schema and topology of the simulated WSN. It indicates the deployed IoT sensors and their GPS location.

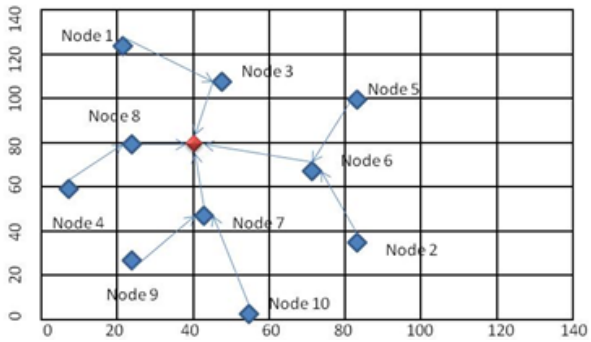

Figure 4. Location and topology details of the IoT sensors

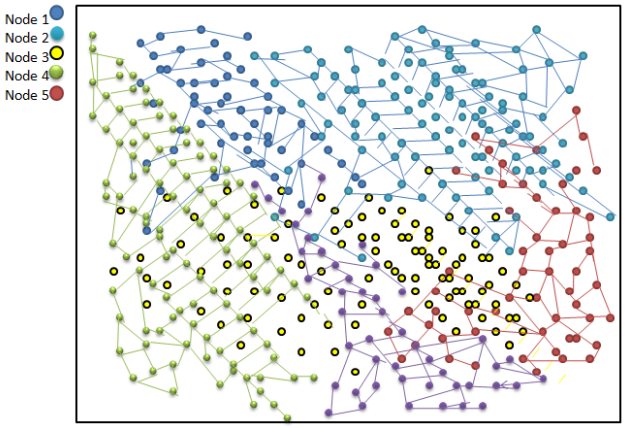

Figure 5. Observed actual values in the network

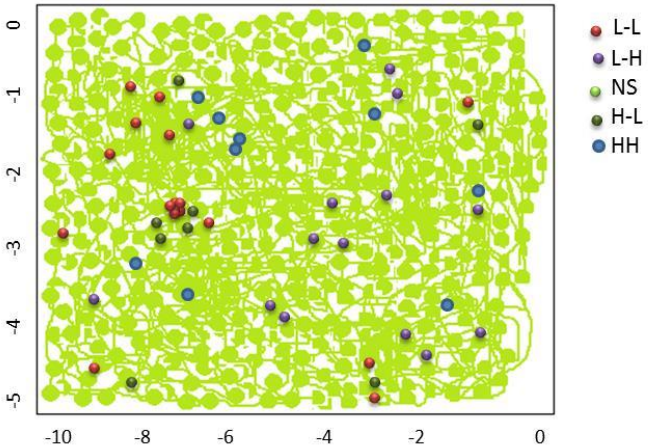

Figure 6. Significant high-level and low-level outliers

Once the movement or operation is complete, all the data are gathered from the IoT sensors and the cluster map of each node and the actual observed values from the network is represented in the Figure 5. Similarly, the high-level and low-level outliers are made statistically significant for easy understanding in Figure 6.

5. Conclusion

Anomaly detection in the smart city infrastructure is a challenging task at present. Although various efforts and techniques are put forward to reduce the complexity, the security of the network and data quality is still at stake. So, to facilitate anomaly detection process in WSN, we have proposed a 5G low-power Wide Area Network (LPWAN) that constitutes the advantages of Fog computing technology in this paper. While all the previous or traditional techniques have focused on cloud computing, the developed low-power technology scheme proves to work efficient based on the results. Additionally, the discussed approach was implemented in the "City of Things" platform and evaluated with unsupervised clustering and outler detection algorithm for the purpose of air quality monitoring.

References

[1] Perlroth, N. Smart City Technology May Be Vulnerable to Hackers. Available online:http://bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers/(accessed on 8 February 2016).

[2] Ghena, B, Beyer, W, Hillaker, A, Pevarnek, J.; Halderman, J.A. Green lights forever: analysing the security of traffic infrastructure. In Proceedings of the 8th USENIX Workshop on Offensive Technologies, San Diego, CA, USA, 19 August 2014.

[3] Smart Infrastructure: The Future; Technical Report; The Royal Academy of Engineering: London, UK, 2012.

[4] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," Ad hoc networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[5] Y. Zheng, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Smart car parking: temporal clustering and anomaly detection in urban car parking,"in Intelligent Sensors, Sensor Networks and Information Processing(ISSNIP), 2014 IEEE Ninth International Conference on. IEEE, 2014, pp. 1–6.

[6] X. Liu and P. S. Nielsen, "Regression-based online anomaly detection for smart grid data," arXiv preprint arXiv:1606.05781, 2016.

[7] (2017) SOCIOTAL project. An EU FP7 funded STREP project addressing the objective FP7-ICT-2013.1.4 “A reliable, smart and secure Internet of Things for Smart Cities”. [Online]. Available: http://www.sociotal.eu

[8] P. Rathore, A. S. Rao, S. Rajasegarar, E. Vanz, J. Gubbi, and M. Palaniswami, “Real-time urban microclimate analysis using internet of things,” IEEE Internet of Things Journal, 2017.

[9] (2017) CityPulse: Real-Time IoT Stream Processing and Large-scale Data Analytics for Smart City Applications. [Online]. Available: http://www.ict-citypulse.eu

[10] D. Puiu, P. Barnaghi, R. Toenjes, D. K¨umper, M. I. Ali, A. Mileo, J. X. Parreira, M. Fischer, S. Kolozali, N. Farajidavar et al., “Citypulse: Large scale data analytics framework for smart cities,” IEEE Access, vol. 4, pp. 1086–1108, 2016.

[11] Challal, Y.; Ouadjaout, A.; Lasla, N.; Bagaa, M.; Hadjidj, A. Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. J. Netw. Comput. Appl. 2011, 34, 1380–1397.

[12] Jung,W.; Hong, S.; Ha, M.; Kim, Y.J.; Kim, D. SSL-Based lightweight security of IP-based wireless sensor networks. In Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops, Bradford, UK, 26–29 May 2009; pp. 1112–1117.

Author’s biography

R. Santhana Krishnan is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Cheranmahadevi, Tirunelveli, India. His area of research includes WSN, IoT, MANET and Machine learning.