A review on WSN and Data Anomaly

Naresh Kumar, Professor, Department of Computer Science & Engineering, Galgotias University

Abstract

Wireless Sensor Networks are critical and vital platforms for the future, particularly with the recent emergence of the idea "Internet of Things." They are utilised in a variety of applications in business, health care, the environment, and the military for monitoring, tracking, and regulating. However, the quality of sensor node data is impacted by anomalies that arise for a variety of causes, including node failures, reading mistakes, odd occurrences, and malicious assaults. As a result, anomaly detection is an essential technique for ensuring the quality of sensor data prior to its use in decision-making. We discuss the difficulties associated with anomaly detection in WSNs and the needs for developing efficient and effective anomaly detection algorithms in this paper. Following that, we examine recent advances in data anomaly detection research in WSNs and group existing detection techniques into five broad categories based on the detection methodologies utilised to construct these systems. The many state-of-the-art models for each class are discussed in detail, as well as their shortcomings, in order to generate suggestions for future developments. Additionally, the studied alternatives are contrasted and rated in terms of their compliance with the specified criteria. Finally, the overall limits of present techniques are highlighted, along with potential avenues for future study.

Keywords: IOT, Data, Anomaly.

Introduction

Wireless sensor networks (WSNs) are a small, low cost, low energy and versatile sensor network which is intensively used for monitoring a phenomena, tracking an item or controlling a process[1]. In numerous application sectors WSNs are employed, including: home automation for personal applications, sales tracking for commercial applications; industrial applications such as architecture and control; and military applications such as enemy target surveillance and tracking[1-3]. One new idea that seems to be the future of WSNs is the Internet of Things (IoT) which hopes that every thing in human existence is equipped with sensors that interconnect, making living more easier[4]. With IoT, sensor nodes dynamically connect to the internet and utilise the internet infrastructure to work together and execute their work[5]. According to[6], a "global network of interconnnded things, based on established communication protocols," is likely to constitute the future Internet known as IoT. One of the most significant aspects of the IoT paradigm[7] are the WSNs, as it acts as a digital skin that gives any computational system access to information about the physical world. Various technologies are developing to integrate WSNs with IoT, such the IETF 6LowPAN standard[8], which enables for IPv6 packets to be sent to computer-based networks.

WSNs from diverse disciplines have been explored, including networking, embedded systems, processing of information, distributed systems and signal processing. This has led to the development of a wide

range of research topics including routing protocols, location strategies, hardware design sensing, query processing, data mining, information processing, security and privacy..

Sensor Data

For decision-makers, sensor data analytics are of great relevance. [9] The objective of the WSN use was not only to gather data from the deployment area, but also, most significantly, to analyse this data in a timely way, so that crucial choices may be taken. The data quality thus represents the genuine status of the world of WSN applications. The raw measurements taken by sensor nodes, in particular large-scale WSNs, are typically deficient and inaccurate[10]. These incorrect sensor measures might be made for causes associated with the sensor device itself or the detecting environment. Resource restrictions on the storage, energy, processing, and bandwidth of sensor devices may lead to nodes failure and hence report abnormal results. Other environmental considerations include the severity and problems of the deployment location, which may result in incorrect data [11–13]. Malicious attacks such as denial of service, sinkhole, black hole, selective transmission, and wormhole assaults [3,14–20] might potentially lead to erroneous, low-quality data generation. In addition, physical disruptions such as destruction or migration of human or animal sensor devices might disrupt the process of data collecting and lead to abnormal measures[1]. [1].

Anomalies are characterised as imprecise or incomplete data measurements resulting from the above factors. An anomaly is described in [21] as an observation that is discordant with the remaining datasets. In [22] the identification of anomalies is described as a procedure for discovering data patterns that are different from the anticipated behaviour. The subject of anomaly detection has been investigated from several angles such as data security, data mining or pattern recognition. In the literature the phrase "anomaly" is differently known as outliers, defects or deviations.

Depending on the domain for which they are employed, there are several different anomaly detection systems in conventional (wired) networks. Due to the constraints of energy, processing, bandwidth and storage capacities of these networks, these solutions cannot be translated straight to WSNs. In addition, standard network anomaly detection approaches concentrate on the network layer itself, but our study focuses more on data on WSN's application layer. Therefore it is necessary to amend current procedures or to build new relevant procedures, in particular for WSNs [18,23,24].

Detection Efficacy

The detection efficacy and efficiency of anomaly solutions in WSNs describe the use of the restricted network resources[25-16]. Efficiency of detection is the accuracy of detection, the detection rate and false alarms. Detection efficiency is indicated by the use of energy and memory. Any suggested anomaly detection system should thus take into consideration improving detectability while spending less energy

and storage throughout the detection process. The need of anomaly detection to ensure the quality of sensors data and identify malicious attacks affecting network features and data integrity has inspired earlier research to explore WSN security and anomaly detection models. This section highlights existing WSN anomaly detection surveys and the variations between these surveys.

Rajasegarar and the co-authors suggested a technical categorization of anomaly detection models in WSN in [27,28]. Anomaly detection models were classified in both surveys. In statistical models and in non-parametric models based on detection model approaches. Non-parametric models have been further grouped into SVM (SVM) model based on rules, CUSUM based, data clustering. Statistically based models either known or determined by means of density estimation methods, the underlying density distribution of data kinds (normal or anomalous). In contrast, non-parametric models have no previous knowledge of data kinds and use alternative measurements to record the typical data behaviour matching the future measurement behaviour.

Conclusion

Effective and effective detection of sensor readings abnormalities is a crucial job in order to guarantee the quality of the sensor data obtained for correct judgments. The literature has offered a range of anomalies detection methods, however most of them have poor detection efficiency or high energy usage. In this study, we analysed the obstacles facing the design of an efficient and effective WSN anomaly detection model and identified the needs (RODAC components) for the creation of such models. The criteria include data reduction, online detection, distributed detection, adaptive detection and the use of spatial/time correlations. These needs include A complete assessment of state-of-the-art detection models was presented, which divided them into statistical clustering-based detection strategies, Based on categorization, and based on the closest neighbour.

References

1. Aazam, M., & Huh, E.-N. (2015). Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In X. F. E. T. P. J. H. Takizawa M. Barolli L. (Ed.), *Proceedings - International Conference on Advanced Information Networking and Applications, AINA* (Vols. 2015-April, pp. 687–694). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AINA.2015.254

2. Ahmad, M., Amin, M. B., Hussain, S., Kang, B. H., Cheong, T., & Lee, S. (2016). Health Fog: a novel framework for health and wellness applications. *Journal of Supercomputing*, *72*(10), 3677–3695. https://doi.org/10.1007/s11227-016-1634-x

3. Alam, F., Mehmood, R., Katib, I., & Albeshri, A. (2016). Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT). In S. E. (Ed.), *Procedia Computer Science* (Vol.

58, pp. 437–442). Elsevier B.V. https://doi.org/10.1016/j.procs.2016.09.068

4. Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2016). Internet of Things: A Definition and Taxonomy. In A.-B. K. AlBeiruti N. Al-Begain K. (Ed.), *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 72–77). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/NGMAST.2015.71

5. Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications*, *81*, 111–124. https://doi.org/10.1016/j.jnca.2016.08.007

6. Geller, J., Grudzinskas Jr., A. J., McDermeit, M., Fisher, W. H., & Lawlor, T. (1998). The efficacy of involuntary outpatient treatment in Massachusetts. *Administration and Policy in Mental Health*, *25*(3), 271–285. https://doi.org/10.1023/A:1022239322212

7. Gia, T. N., Jiang, M., Rahmani, A.-M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015). Fog computing in healthcare Internet of Things: A case study on ECG feature extraction. In J. S. L. L. C. R. A. H. J. M. G. G. N. W. Y. Atzori L. Jin X. (Ed.), *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015* (pp. 356–363). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.51

8. He, D., & Zeadally, S. (2015). An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet of Things Journal*, *2*(1), 72–83. https://doi.org/10.1109/JIOT.2014.2360121

9. Hiremath, S., Yang, G., & Mankodiya, K. (2015). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. *Proceedings of the 2014 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare Through Innovations in Mobile and Wireless Technologies", MOBIHEALTH 2014*, 304–307. https://doi.org/10.1109/MOBIHEALTH.2014.7015971

10. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Z. L.-J. Bahsoon R. (Ed.), *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015* (pp. 21–28). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SERVICES.2015.12

11. Hussain, A., Wenbi, R., Da Silva, A. L., Nadher, M., & Mudhish, M. (2015). Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems*

and Software, *110*, 253–263. https://doi.org/10.1016/j.jss.2015.08.041

12. Jara, A. J., Alcolea, A. F., Zamora, M. A., Gómez Skarmeta, A. F., & Alsaedy, M. (2010). Drugs interaction checker based on IoT. *2010 Internet of Things, IoT 2010*. https://doi.org/10.1109/IOT.2010.5678458

13. Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In K. L. Latkoski P. Cvetkovski G. (Ed.), *17th IEEE International Conference on Smart Technologies, EUROCON 2017 - Conference Proceedings* (pp. 763–768). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EUROCON.2017.8011213

14. Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare: Potential Applications and Challenges. *IT Professional*, *18*(3), 2–4. https://doi.org/10.1109/MITP.2016.42

15. Lee, Y. H., Jang, M., Lee, M. Y., Kweon, O. Y., & Oh, J. H. (2017). Flexible Field-Effect Transistor-Type Sensors Based on Conjugated Molecules. *Chem*, *3*(5), 724–763. https://doi.org/10.1016/j.chempr.2017.10.005

16. Mandula, K., Parupalli, R., Murty, C. H. A. S., Magesh, E., & Lunagariya, R. (2016). Mobile based home automation using Internet of Things(IoT). *2015 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2015*, 340–343. https://doi.org/10.1109/ICCICCT.2015.7475301

17. Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V, Gomes, P. H., Libralon, G. L., Meneguete, R. I., Filho, G. P. R., Giancristofaro, G. T., Pessin, G., Krishnamachari, B., & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

18. Moosavi, S. R., Gia, T. N., Rahmani, A.-M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. In S. E. (Ed.), *Procedia Computer Science* (Vol. 52, Issue 1, pp. 452–459). Elsevier B.V. https://doi.org/10.1016/j.procs.2015.05.013

19. Muhammad, G., Rahman, S. M. M., Alelaiwi, A., & Alamri, A. (2017). Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. *IEEE Communications Magazine*, *55*(1), 69–73. https://doi.org/10.1109/MCOM.2017.1600425CM

20. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2017). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design, ICED 2016*, 321–326. https://doi.org/10.1109/ICED.2016.7804660

21. Ndiaye, M., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). Software defined networking for improved wireless sensor network management: A survey. *Sensors (Switzerland)*, *17*(5).

https://doi.org/10.3390/s17051031

22. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., & Chen, Q. (2015). Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. *Enterprise Information Systems*, *9*(1), 86–116. https://doi.org/10.1080/17517575.2013.776118

23. Rahmani, A.-M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., & Tenhunen, H. (2015). Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 826–834. https://doi.org/10.1109/CCNC.2015.7158084

24. Rajandekar, A., & Sikdar, B. (2015). A survey of MAC layer issues and protocols for machine-to-machine communications. *IEEE Internet of Things Journal*, *2*(2), 175–186. https://doi.org/10.1109/JIOT.2015.2394438

25. Roehrs, A., Da Costa, C. A., Da Rosa Righi, R., & De Oliveira, K. S. F. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, *19*(1). https://doi.org/10.2196/jmir.5876

26. Singh, R., Singh, E., & Nalwa, H. S. (2017). Inkjet printed nanomaterial based flexible radio frequency identification (RFID) tag sensors for the internet of nano things. *RSC Advances*, *7*(77), 48597–48630. https://doi.org/10.1039/c7ra07191d

27. Yeh, K.-H. (2016). A Secure IoT-Based Healthcare System with Body Sensor Networks. *IEEE Access*, *4*, 10288–10299. https://doi.org/10.1109/ACCESS.2016.2638038