Node-based versus Server-based Data Validations in Internet of Things

Naemah Mubarakah¹*, Poltak Sihombing², Suherman Suherman³, Soeharwinto⁴
¹,³,⁴Electrical Engineering Department, Universitas Sumatera Utara, Medan-Indonesia
²Faculty of Computer Science, Universitas Sumatera Utara, Medan-Indonesia

*naemah@usu.ac.id

Abstract. Internet of Things (IoT) collects and sends data over TCP/IP network for the intended application. Some applications designed sensors to be lost after battery exhausted. Therefore, battery lifetime is important. On the other hand, data quality can be disrupted by the harsh environment and interfering noises, so that the transmitted data may be invalid. Transmitting invalid data may exhaust battery sooner, while implementing validation algorithm may absorb more power. This paper proposed a simple peak detection method in IoT sensor to avoid transmitting invalid data. The experimental evaluation was set up and the method was compared to server-based support vector machine classifier. The results show that the proposed method is able to cancel 86% error data transmission with 1.25% power savings.

1. Introduction

The progress on some technologies such as sensors, actuator, and embedded computing enable distributed small devices controlling many applications. Those devices can be controlled and connected remotely through TCP/IP network. The internet of things is emerged to satisfy networking requirements to interconnect those devices, including sensor and interconnection framework [1].

Wireless World Research Forum projected that there are 7 trillion wireless devices around the world serving about 7 million people [2]. IoT enables collaborations and cooperation among those wireless devices, allows self-organizing and adaptive operation as well as intelligent applications [3]. Wireless sensors are implemented mainly for wireless sensor networks (WSNs), radio identification network (RFID)[12], machine-to-machine (M2M), supervisory control and data acquisition (SCADA) and other applications. IoT is expected to cover anything any device, anytime any context, anyone anybody, any service any business, any path any network, and any place anywhere [4].

Figure 1 shows the essential component in IoT [4]. The architecture contains sensors at the network edge (layer 1). These sensors route data to the edge sensor (layer 2) which forward all data to sensor static sensor referred to as sink node (layer 3). Sink node sends data to receiver with low processing capabilities such as mobile node or a single personal computer (layer 4). In order to
maximize the work, data may forwarded to a high processing unit such as servers (layer 5). At the end, data may be stored, shared and processed at the cloud (layer 6). Middleware is required to integrate those systems in order to accommodate various applications and requirements. Survey performed by Razzaque et al [5] showed that some middleware architecture have been proposed to support multi-propose IoT networks. However, mostly is WSN-centric. The research also said that there no middleware framework thas is available to cover all IoT applications.

Sensor node has limitation mainly related to processing capabilities and electrical supply. Those sensors are mainly using wireless link to connect, so they are mostly unreachable for recharging purpose [6]. Even though many energy-saving methods proposed, including the use of energy harvesting, steps on energy efficient are still pressing and to increase battery and network lifetime for IoT application [7]. As the consequence, techniques and methods used in IoT should consider energy limitation and efficiency.

Other emerging problem is the irregularity of radio link that potentially causes disturbances and interferences to the transmitted data. The quality of the transmitted data surely influences the applications [8]. Even its importance for application performances, study on this matter is still limited. On the other hand, data quality implementations are mainly performed in database level. Some issues related to data quality covers accuracy, currency, and completeness [9]. Quality guarantee is generally performed in database which is more stable and well defined. There is few work found on real-time data validation, implemented during data generations. Meanwhile, pervasive system performances depend on data acquisition and energy consumption. So this topic is still challenging.

Data quality can be measured as data validity as well as data integrity. Validity means data represent the unit that is measured. While integrity guarantees that data is free of separation, privileges, virus free, and intrusion free [10]. This paper focuses on real-time data validation on IoT, by comparing validation process in wireless sensor node and validation process in server. Trade-off between microcontroller capabilities and energy limitation were assessed through implementations. A lightweight validation system is proposed.

Fongen [10] collected sensor data in the IoT/ WSN applications. It showed that during data collection, some collected values are not correct. This event leads to incorrect data received by server which decreases the accuracy and reliability. Fongen [10] stated that the statistical observation for data outliers exerts lower complexity rather than supervisor and cluster method. However, the statistical methods cannot be performed real-time as it is performed in a fixed collected data. Work on [2] implemented one class quarter sphere support vector machine (OCSVM) for detecting outliers. However, the method is to complex for real-time applications. Xiong et al [3] used one-class principal component classifier. It has lower computational cost than OCSVM but requires retraining. Lower layer such as transport layer [11] may also be used for validation. This paper proposes a lightweight data validation based on peak detection.

2. Drone design and measurement method
In order to evaluate the proposed method, a simple IoT device implemented by using ESP8266 module is set up. This wireless sensor collects temperature data and sends it to a server by using a 802.11 network. Figure 2 shows the designed circuit.

![Figure 2. The IoT node](image)
In order to simulate errors, an interfering circuit was designed as in Figure 3. This circuit periodically turns the light-bulb on so that the measured temperature increases as an error. The effectiveness of the method is also measured in term of energy consumption. The current and voltage measurement device is arranged by using arduino as in Figure 4.

![Interfering circuit](image1)

Figure 3. Interfering circuit

![Power consumption device](image2)

Figure 4. Power consumption device

The interfering unit is set to turn light-bulb in some periods. Light-bulb to sensor distance is also varied to represent degree of disturbances. The proposed validation is by using peak detection. Peak point (Xn) is obtained when it is larger than previous (Xn-1) and next (Xn+1) values as denoted by Equation 1. The outliers are determined by difference, $\partial$, so that outliers are fulfilling the Equation 2.

$$X_{n-1} < X_n > X_{n+1} \quad [1]$$

$$|X_n - X_{n-1}| > \partial \quad \text{and} \quad |X_{n+1} - X_n| > \partial \quad [2]$$

3. Assessment results

Fig. 5 shows the non-validated temperature data generated by the IoT sensor with 5% interferences. Data contains outliers as well as errors which are presented by sparking high measurement results and zero values. In server-based validation, this data is validated by removing the outliers and errors. In Server side, the presented data is as depicted in Figure 5 depending upon the validation technique used. This paper used support vector machine classifier in server-based validation.

![IoT data with 5% interferences](image3)

Figure 5. IoT data with 5% interferences
Figure 6. Validated data in server

The validation for the first evaluated data sequence results 100% cleaned data with 43 errors out of 142 data. In term of power consumption, this paper considers IoT sensor only as server is not critical for low power application. Figure 7 shows the IoT sensor power consumption. Power consumption changes overtime with average power consumption per data retrieval is 0.650544 mW and total power consumption for the period of observed data is 93.028 mW.

Figure 7. IoT power consumption of server-based validation

Figure 8 shows the transmitted data by IoT sensor when data validation as in Equation 1 applied in IoT sensor. Since at time of assessment, the amplitude of outliers and errors are distinguishable, value \( \delta \) is set constant 8°C. As results some outliers and errors are not transmitted which expectedly saving more energy on IoT sensor. The advantage of the peak detection validation technique is that the process is simple and requires low power. The proposed method is unable to detect the sequential outliers or errors as sensor will consider them as normal data. Validation on IoT sensor results 86% unsent error. The proposed sensor node validation is able to save power consumption; with average power consumption per data retrieval is 0.642 mW and total power consumption for the observed period is 91.865 mW (Figure 9). This means that IoT sensor with proposed peak detection validation is able to conserve about 1.25% power.

Figure 8. IoT data with node-based validation
In order to enhance validation performance, the combination of node- and server-based validations is suggested, so both low power consumption in IoT sensor and better validation results are achieved.

4. Conclusions
This paper has proposed IoT sensor node data validation by using peak detection method. The assessment was performed in real environment, but harsh circumstances were simulated by using interfering circuit. The node-based validation method was compared to server-based validation that made use of support vector machine. The results showed that node-based validation unsent 86% of error data, which makes 24% lower valid data than server-based validation. However, the proposed method is able to reduce power consumption about 1.25%, from 93.02mW to 91.865mW. Further improvement was gained when both node- and server-based validations were employed.

Acknowledgement
This research has been supported by TALENTA USU research grant 2020.

References
[1] Palattella M R, Accettura N, Vilajosana X, Watteyne T, Grieco L A, Boggia G, and Dohler M/ 2013. Standardized protocol stack for the internet of (important) things, IEEE Communications Surveys & Tutorials, 15(3), 1389-1406.
[2] Sheng Z, Mahapatra C, Zhu C, and Leung V C. 2015. Recent advances in industrial wireless sensor networks toward efficient management in IoT, IEEE Access, 3, 622-637.
[3] Xiong S, Ni Q, Wang X, and Su Y. 2017. A connectivity enhancement scheme based on link transformation in IoT sensing networks, IEEE Internet Things J., 4(6), 2297–2308
[4] Perera C, Zaslavsky A B, Christen P, and Georgakopoulos D., 2013. Context aware computing for the Internet of Things: A survey, IEEE Commun. Surveys Tuts., 16(1), 414–454.
[5] Razzaque M A, Milojevic-Jevric M, Palade A, and Clarke S. 2016. Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal, 3(1), 70–95. doi:10.1109/jiot.2015.2498900
[6] Diao J, Zhao D, Wang, J, Nguyen H M, Tang, J, and Zhou Z. 2019. Energy-Efficient Boundary Detection of Continuous Objects in IoT Sensing Networks. IEEE Sensors Journal, 1–1. doi:10.1109/jsen.2019.2919580
[7] Olatinwo S O, and Joubert T H. 2019. Energy ef?cient solutions in wireless sensor systems for water quality monitoring: A review, IEEE Sensors J., 19(5), 1596–1625
[8] Suherman S, Ulfa Hasnita, Rambe A H, Mubarakah N, Sembirding R. 2019. Data transmission period consideration in the internet of thing node, International Conf. on Computing and Applied Informatics.
[9] Li F, Nastic S, and Dustdar S. 2012. Data Quality Observation in Pervasive Environments. IEEE 15th International Conference on Computational Science and Engineering. doi:10.1109/iccse.2012.88
[10] Fongen A, and Mancini F. 2015. Integrity attestation in military IoT. IEEE 2nd World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2015.7389102.

[11] Abdurrahman, H., Sitompul, O. S., and Mubarakah, N. 2017. UDP-Lite Enhancement Through Checksum Protection. In IOP Conference Series: Materials Science and Engineering 180(1), 012146). IOP Publishing.

[12] Rahmat R F, Herly E T, Siregar B, Syahputra M F, Sitompul O S 2018 RFID presence monitoring system as an input to measure the workload of employee 4th International Conference on Computer Applications and Information Processing Technology, pp. 1-6