Measurement of Component Performance (Sensor) on Internet of Thing (IoT)

Sharipuddin
Department of Computer Engineering
STIKOM Dinamika Bangsa Jambi &
faculty of Engineering Universitas
Sriwijaya
Indonesia
sharip_udin@yahoo.co.id

Kurniabudi
Department of Computer Engineering
STIKOM Dinamika Bangsa Jambi &
faculty of Engineering Universitas
Sriwijaya
Indonesia
kbudiz@yahoo.com

Benni Purnama
Department of Computer Engineering
STIKOM Dinamika Bangsa Jambi &
faculty of Engineering Universitas
Sriwijaya
Indonesia
bennipurnama@stikom-db.ac.id

Dimas Wahyudi
Faculty of Computer Science
Universitas Sriwijaya
Indonesia
mail.dimaswahyudi@gmail.com

Fepiliana
Faculty of Computer Science
Universitas Sriwijaya
Indonesia
fepilianasugianto@gmail.com

Sri Suryani
Faculty of Computer Science
Universitas Sriwijaya
Indonesia
srisuryani57@gmail.com

Deris Stiawan
Faculty of Computer Science
Universitas Sriwijaya
Indonesia
deris.stiawan@gmail.com

Darmawijoyo
Faculty of Mathematics and Natural
Science
Universitas Sriwijaya
Indonesia
darmawijoyo@yahoo.com

Rahmat Budiarto
College of Computer Science & IT,
Albaha University
Saudi Arabia
rahmat@bu.edu.sa

***Abstract*— This study presents the testing of several devices (sensors) in obtaining sensor performance, there are several experiments and evaluations of the results obtained in the topology. Each sensor must be able to provide some results in the form of accuracy, reliability, range, and resolution. The accuracy and reliability have very important role in producing accurate data. With several explanations and analysis, it is expected to produce a reference for advanced development and policies making in the deployment of IoT system, especially in multi-sensing IoT systems. This work obtain the dataset through several stages, namely building topology (system design), data capture, and feature extraction. Wi-Fi and XBee communication protocols are used. In Wi-Fi protocol, the TCP traffic gives the greatest value compared to other traffic on normal data as well as attack data. In XBee protocol, the Low Rate Wireless PAN IEEE 802.15.4 protocol has an average of 83.96 percent for normal data and 98.73 percent for attack data, respectively. The results of attribute reading experiments, the XBee protocol achieves eighteen attributes whereas the Wi-Fi protocol only seventeen attributes.**

Keywords—IoT, Sensing, IOT Architecture

I. INTRODUCTION

IOT is a concept where an object which has ability to transfer data over the network without requiring human to human or human to computer interactions such as human with heart implants monitor, livestock with biochip transponder or a car equipped by built-in sensors that alert the driver when the tire pressure is low [1]. So far, IoT is most closely related to machine-to-machine (M2M) communications in manufacturing and electricity, oil and gas. Products are built with M2M communication capabilities which are often called smart or "smart" systems. (example: smart labels, smart meters, smart grid sensors).

The development of IoT will be significant in the home and business application in terms of improving the quality of life and supporting the world economy. For example in the fields of education, health, industry, smart home and others[2]. IoT consists of several elements, namely (i) Identification, (ii) Sensing, (iii) Communication, (iv) Computation, (v) Service and (vi) Semantic, and each element interacts with the other.

IoT with various application capabilities in it can facilitate human activities and combined with intelligent systems can provide intelligent services that are the integral components of the environment. IoT services work based on the flow of data obtained from various sensors and actuators. Therefore, the factor of accuracy and reliability of a sensor installed on the IoT has an important function in producing a good IoT service[3].

The use of sensor devices on IoT is very important because it serves as a device to generate data. On the other hand, the sensor is also a powerful medium in terms of attacking devices on IoT. This fact is supported by several special studies that discuss censorship of attacks. authors [4][5] mentions that sensors can be used to carry out attacks by sending a message that generates malware into an IoT device. Other research results succeeded in getting information on IoT that was encrypted by a way of describing the package [6]. The attack on the sensor is easy because it does not require a difficult tool to be able to access the sensor [7]. Sensor manufacturers have not yet fully understood the threats on IoT and may generate risks to IoT application systems. Another study on IoT sensors discusses the ability to recognize anomaly package patterns [8] and the development of IDS to detect anomaly packages when the sensor is activated [9]. In addition, in a number of specialized studies, sensing is a serious challenge that can damage the IoT system[10], then improper sensor installation will cause damage to the IoT system[11].

978-1-5386-5721-8/18/$31.00 ©2018 IEEE

It is understandable that sensors must have resistance against the attacks both from within and from outside the IoT system. We also must to have knowledge about the types of attacks on sensors that result in a shock to the device and IoT applications. Therefore, the focus of this study is to test the ability of the sensors to measure the accuracy and reliability of the IoT system to be developed, to ensure that the sensor design, data reception, and delivery are in line with the needs. This research is a description of the important of sensors in data sensing and data transmission on IoT systems. The expected contribution in this study include (i) producing a measurable reliability of each tested sensor using several operating systems, and (ii) producing dataset of each sensor for normal and anomaly/attacks data types.

II. Internet Of Things (IoT) Architecture

The survey by [2] stated that there are five layers of IoT system development that must be followed.

- *Objects Layer*
  This layer contains the device (sensor) and also the actuator on the IoT system which aims to obtain data and as a place to process information. Sensors and actuators at this layer function as querying location, temperature, weight, motion, vibration, acceleration, humidity, etc.

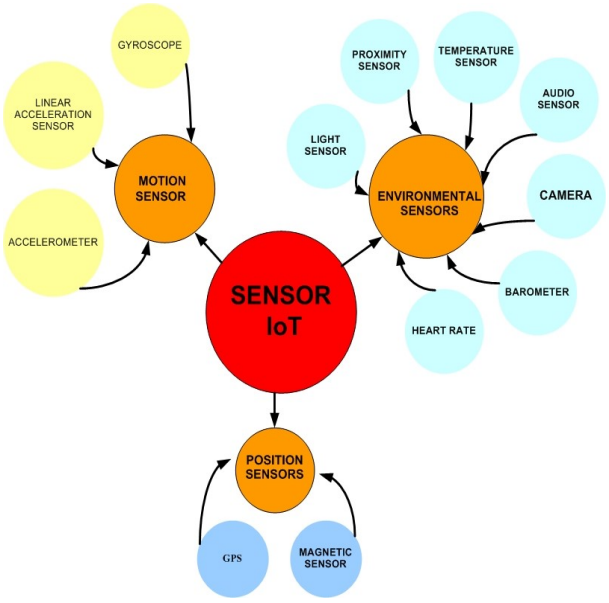

Fig 1. Types of IoT Sensor.

- *Object Abstraction Layer*
  This layer serves as to transfer data from the Objects Layer to the Service Management Layer. Data can be transferred with technologies such as RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, etc. In addition, other functions such as cloud computing and data management processes.
- *Service Management Layer*
  This layer serves as a decision-making and provides services. Requests to this layer is on the form of IP address and name of the applications.
- *Application Layer*
  The application layer functions as a service provider requested by the user such as temperature data and humidity data. The most important thing in this layer is having the ability to provide high-quality smart services.
- *Business Layer*
  This layer is responsible for managing the entire IoT system in the form of systems and services. Besides, this layer has the responsibility of building business models, graphics, flowcharts based on the data received from the application layer. Furthermore, this layer serves as comparing the output of each layer with the output that is expected to improve service and maintain user privacy.

III. Research Method

The data in this study were obtained through several stages. The first stage is the system development by building topology that we will later use as a research dataset. The second stage is to process the dataset extraction. The third stage, feature selection is to get strong features that will be used in the last stage. The last or fourth stage is to make the engine detection of the features generated in the third stage. This research is still in the early stages of making topology and features extraction. Figure 2 shows the design of IoT system for this research.

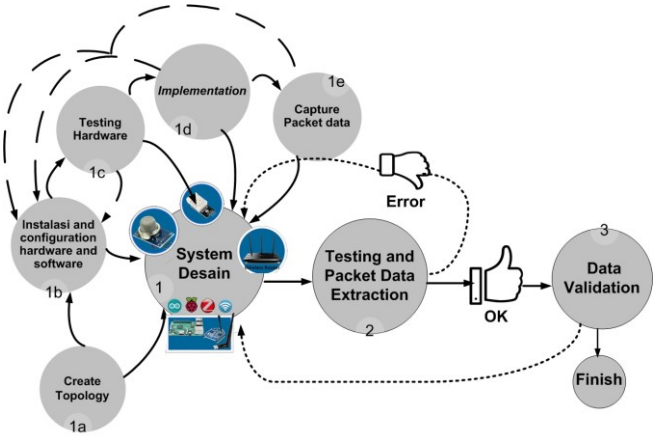

Fig 2. Design of the proposed IoT system.

A. System Design

The research uses several hardware such as DHT22 sensor, MQ2 sensor, Fundulno sensor, soil moisture sensor and other types of sensors. Several nodes and middleware1 that use XBee version 1, middleware2 which uses XBee version 2, wemos D1 and wireless routers as the connecting media between middleware and a PC acts as a monitoring server. Figure 3 illustrates the topology of the topology for the IoT system testbed.

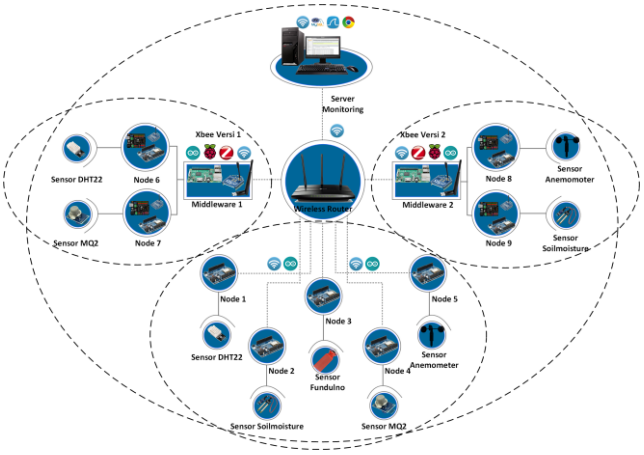

Fig 3. Testbed topology.

B. *Data Capture*

The experiments aims to produce two type of dataset, namely normal dataset and anomaly/attack dataset. The type of attack used in this study is DDOS. Figure 4 illustrates the simulation attempts to get a normal and anomaly/attack dataset. The patterns of normal and (DDOS) packets of the obtained data will be analyzed thru their attributes, so that manually one is able to distinguish normal data from anomaly/attacks data.

Fig 4 Sensors for monitoring environment in IoT-based system

C. *Feature Extraction*

Having done building the topology and getting the dataset, the next step is to read the attributes by the way of the extraction process captured from the traffic to obtain information about the types of data packets. The resulting raw data is difficult to read and understand and there are also some hidden patterns so that little information is used to identify a data packet pattern, then Extraction Feature is used to help identifying a data packet [12]. Figure 5 shows the flow of the raw data extraction process.

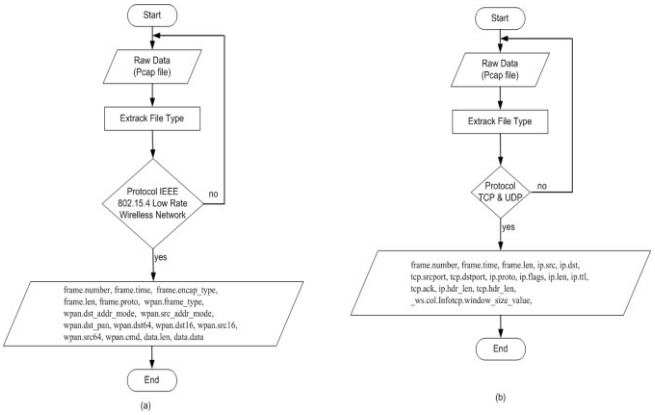

Fig 5. Feature Extraction Process (a) on XBee, (b) on Wi-Fi.

IV. Experimental Results and Discussion

The test results on topology with two types of data packets, namely normal and anomaly are presented in Figure 6 and Figure 7 with a length of data observation of five minutes. The results obtained show that the data on Wi-Fi is much larger compared to XBee data.

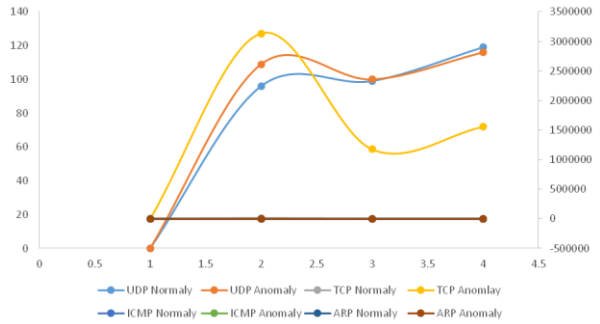

Fig 6. Experimental results on Wi-Fi (TCP/UDP)

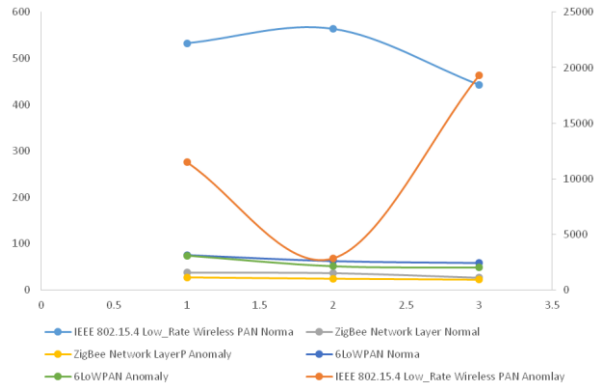

Fig 7. Experimental results on ZigBee (IEEE 802.15.4 Low_Rate Wireless PAN, ZigBee Network Layer and 6LoWPAN)

In Figure 6 and Figure 7, it can be seen that the data on communication with Wi-Fi is more sensitive than XBee. This refers to [13] which explains the characteristics of communication equipment. Band frequency on Wi-Fi is 2.4 GHz and 5 GHz while XBee is only at 2.5 GHz frequency. The data rate for Wi-Fi is 100 MBps and XBee is 1-100 MBps. Thus, it can be stated that the data in Wi-Fi is greater than the data in XBee by considering that the number of devices used is more with Wi-Fi communication compared to XBee.

TABLE 1 EXPERIMENTAL RESULT ON WI-FI

Traffic Types	Number of Packet Data	
	Normal	*Anomaly*
UDP	96	109
	99	100
	119	116
TCP	11728	3134653
	1376	1174350
	1342	1554940
ICMP	500	0
	0	0
	0	0
ARP	457	626
	424	609
	641	650

Table 1 shows that of the four types of traffic are tested. TCP traffic has the greatest result, which is 76.00 percent for normal data while for attack data is 99.96 percent. Interestingly, we observed quite significance ARP traffic of 18.80 percent on normal data while 0.04 percent on attack data. This will be our focus further because this broadcast traffic will burden the traffic.

TABLE 2 EXPERIMENTAL RESULT ON XBEE

XBee Protocol Type	Number of Packet Data	
	Normal	*Anomaly*
IEEE 802.15.4 Low_Rate Wireless PAN	533	11477
	564	2830
	443	19304
ZigBee Network Layer	37	27
	36	25
	26	22
6LoWPAN	75	74
	62	52
	58	48

Table 2 shows the results of reading sensor data on XBee devices using three protocols, namely: 1) IEEE 802.15.4 Low_Rate Wireless PAN, 2) ZigBee Network Layer and 3) 6LoWPAN. The test results show that the IEEE 802.15.4 Low_Rate Wireless PAN protocol gives an average of 83.96 percent on normal data and 98.73 percent on attacks data. Whereas, the results of the experiment for the ZigBee Network Layer protocol produces an average normal data and the attack data of 5.37 percent and 0.39 percent, respectively. Experiments using the 6LoWPAN protocol generates 10.67 percent data for normal data and 0.88 percent for attack data.

The findings in this study shown in Table 1 and Table 2 are in line with the results of the study by [9] which found that attack data was detected at 99.90%. In this study, packets sent and received are only in the form of sensor data, without considering any mechanism of receiving or sending streaming data such as VoIP or others (UDP). It means that only TCP traffic is captured and this research uses HTTP Get Request as a part of TCP, so TCP traffic is more dominant compared to other traffic.

This study also uses XBee series 1, (IEEE 802.15.4). XBee resides at the physical and data link layers. Data in the form of data frames technically can be read via serial port. However, in this study data is read and captured with hardware tools in the form of Atmel RZ Raven USB Stick, which is combined with Wireshark. Nevertheless, there are shortcomings in this technique that is the data is not completely captured and causing a lot of data loss.

The next stage is the data validation process, this process aims to read and compare the data obtained from raw data with the results of the extraction process. Then the obtained data will also be searched for the strongest/best values that will be used as guidelines as the basic pattern of a packet data. To simplify the reading of attribute values, these research converts the captured data into CSV format.

Table 3 displays the attributes of the raw data reading by using a feature extraction method, where this process can facilitate the reading of raw data. The results obtained in the form of seventeen attributes on Wi-Fi protocol and eighteen on XBee protocol.

TABLE 3 RESULTS OF READING THE ATTRIBUTES

Raw Data	Attributes
On Wi-Fi	frame.number, frame.time, frame.len, ip.src, ip.dst, tcp.srcport, tcp.dstport, ip.proto, ip.flags, ip.len, ip.ttl, tcp.ack, ip.hdr_len, tcp.hdr_len, _ws.col.Infotcp.window_size_value
On XBee	frame.number, frame.time, frame.encap_type, frame.len, frame.proto, wpan.frame_type, wpan.dst_addr_mode, wpan.src_addr_mode, wpan.dst_pan, wpan.dst64, wpan.dst16, wpan.src16, wpan.src64, wpan.cmd, data.len, data.data

Figure 8 and Figure 9 show the results of data validation between normal raw data and anomaly/attacks raw data against extract results.

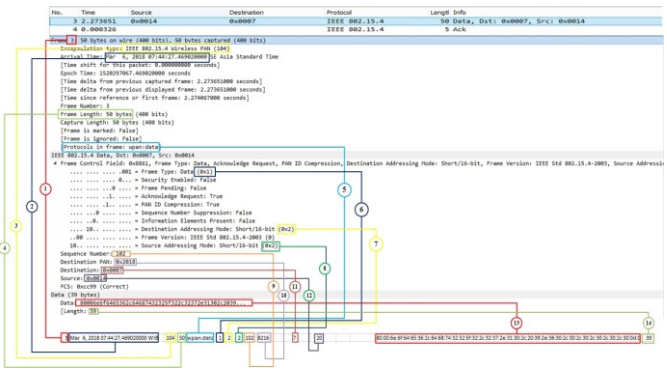

Fig 8. Data validation results of normal raw data against extraction result. (XBee).

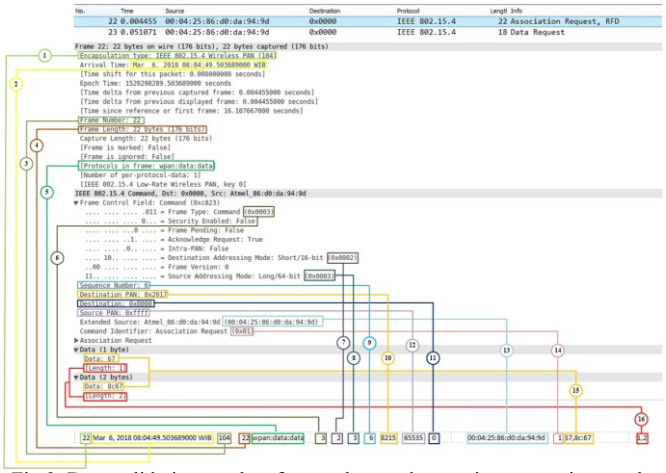

Fig 9. Data validation results of anomaly raw data against extraction result. (XBee).

V. SUMMARY

From the results of the discussion, it can be concluded that on Wi-Fi communication protocol, the TCP traffic is more dominant than other traffic such as (UDP, ICPM, and ARP), where normal data is 76.00 percent while attack data is 99.96 percent. Results on XBee with the Low_Rate Wireless IEEE 802.15.4 protocol PAN normal data and attack data were obtained on average of 83.96 percent for normal data and 98.73 percent for attack data. While the results of the experiments for the ZigBee, the Network Layer protocol generated normal data and attacks of 5.37 percent and 0.39 percent, respectively. Experiments using the 6LoWPAN protocol produced 10.67 percent data for normal data and 0.88 percent for attack data.

For the future, this research will analyze and conduct experiments on sensors using several other communcation protocols so that we can see which protocols are better. We also think of observing the effects of temperature and humidity sensing so that the expected results can really be referenced for further research and further development on IoT sensor industries.

ACKNOWLEDGMENT

This research is supported by STIKOM Dinamika Bangsa through human resource development program and collaboration with Comnet Lab Universitas Sriwijaya.

REFERENCES

[1] S. Li, L. Da Xu, and S. Zhao, “The internet of things : a survey,” vol. 2, no. April 2014, pp. 243–259, 2015.

[2] A. Al-fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things : A Survey on Enabling Technologies, Protocols and Applications,” no. c, 2015.

[3] H. Sándor, B. Genge, and Z. Szántó, “Sensor Data Validation and Abnormal Behavior Detection in the Internet of Things.”

[4] V. Subramanian, S. Uluagac, H. Cam, and R. Beyah, “Examining the Characteristics and Implications of Sensor Side Channels,” pp. 2205–2210, 2013.

[5] R. Hasan, “Sensing-Enabled Channels for Hard-to-Detect Command and Control of Mobile Devices Categories and Subject Descriptors.”

[6] S. Merino, D. Pozo, D. Kamel, A. Moradi, and G. Horst, “Side-Channel Attacks from Static Power : When Should We Care ?” pp. 145–150, 2015.

[7] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, “Soundcomber : A Stealthy and Context-Aware Sound Trojan for Smartphones.”

[8] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, and M. Stanley, “A Brief Survey of Machine Learning Methods and their Sensor and IoT Applications.”

[9] S. Hariri, “Anomaly behavior analysis for IoT sensors,” no. November 2016, pp. 1–15, 2017.

[10] T. U. Darmstadt, “Security and Privacy Challenges in Industrial Internet of Things Invited.”

[11] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android Permissions : User Attention, Comprehension, and Behavior,” 2012.

[12] J. Song, H. Takakura, and Y. Kwon, “A generalized feature extraction scheme to detect 0-day attacks via IDS alerts,” *Proc. - 2008 Int. Symp. Appl. Internet, SAINT 2008*, pp. 55–61, 2008.

[13] N. Chhabra, “Comparative Analysis of Different Wireless Technologies,” *Int. J. Sci. Res. Netw. Secure. Commun.*, vol. 1, no. 5, pp. 13–17, 2013.

978-1-5386-5721-8/18/$31.00 ©2018 IEEE