Development of Wireless Sensor Node Addressing and Data Packet Collision Avoidance Scheme

Nurulidayu Binti Sainuddin, Ali Mohammed Abdal-Kadhim, Kok Swee Leong

Abstract*: Wireless sensor network (WSN) consists of autonomous sensor devices that are spatially distributed in a wide area. Wireless sensor network is built up from a large number of sensor nodes that are assigned to a specific tasks and most probably is monitoring and reporting tasks. However, since the network might be expanded to hundreds, thousands or even millions of sensor nodes, there will be a high chance for the data from different wireless sensor nodes to collide with one another. Therefore, a proper node addressing scheme is needed to synchronize the data packages transmissions to the sink station. In this paper, a seven bytes addressing string scheme is proposed to encapsulate the node data and assist the sink station in identifying the data packages sources. The addressing string will be created in the wireless sensor node which it contains the node ID, package ID and the node data as well. The package ID is included to detect collided packages within the network. The data packages collision is avoided by allowing the sensor node to access the RF channel and transmit the data at a random time. The experimental results reviled that the proposed scheme was successfully addressed the wireless sensor node and make node identification at the sink station easy.

Keywords* : Wireless Sensor Network (WSN), Sensor node addressing, collision avoidance, data package, Radio frequency.

I. INTRODUCTION

Revolution of communication gathering technology has brought Wireless sensor network (WSN) as a new alternative technology that offers reliability and efficiency of information and communication system. WSNs can be considered as a promising sensing technology for many applications such as healthcare monitoring [1], environmental monitoring [2], industrial machinery monitoring [3], … etecetra. It is easy to deployed, low cost, flexible and reliable [4-5]. However, there are few issues that can affect the performance of the WSNs such as energy consumption [6], security[7], scalability and synchronization [8], … etecetra. This paper resolve the issue regarding the packages collision and sensor node identification that occurs during data transmission at the same RF channel. Conventionally, multiple sensor nodes data transmission to the sink station has been achieved by sending the data using different frequency channel as shown in Fig. 1. In this way, there is no collision of data is expected, however, the radio channels is limited and cannot be further expanded [9]. Add on, it will take time for the sink station to multiplex the RF channels to collect data from each node. This issue will become more crucial when there are thousands of nodes in the wireless network. As the number of nodes increase, the number of channel will also increase, and lead to a longer time for sink station to scan the different RF channels to collect the data from each node. Therefore, data transmission is proposed to be done in one frequency channel where every node will be sharing the same path to transmit their packages to reduce the multiplexing time of the sink station.

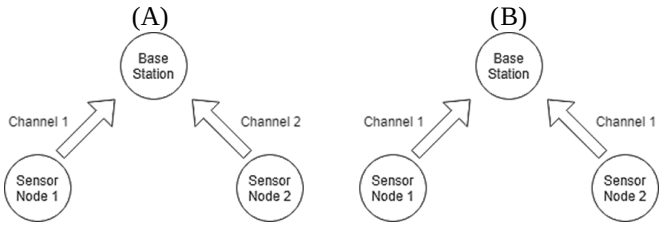

Fig. 1: Transmission method, A: Conventional method, B: Proposed method

As the WSNs are usually build of a large network of nodes, the probability of collision of data packages between the nodes is high. Occurrence of data packages collision is expected when two or more sensor nodes within the same wireless network are transmitting using the same frequency channel simultaneously [10-11]. Package collision in the network can lower the performance of the system overall as the percentage of data losses, power consumption and wastage in channel bandwidth is increase [12]. This issue also rise up interferences problem, data corruptions due to undelivered data packages to the intended receiver and data package losses.

Previous works have shown numerous efforts has been taken to find the key to collision avoidance. For instance, Chunyang Lei [13] has found that the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based network failed to avoid interference in WSNs efficiently and hence provided a new strategy to avoid such collision by a space-time random access technique

Revised Manuscript Received on July 22, 2019.

Nurulidayu Binti Sainuddin, Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. Email: dayudyaz@gmail.com

Ali Mohammed Abdal-Kadhim, Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. Email: ali.challenger89@yahoo.com

Kok Swee Leong, Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. Email: sweeleong@utem.edu.my

that can reduce more collision percentage in the wireless network. Also, a new communication scheme for IEEE 802.15.4 based WSNs was designed by Prasan and Jang-Ping [14] which their main goal was to reduce the collisions and prevent data transmission at the same time. They had contributed in designing an analytical model for uplink traffic in beacon-enabled slotted CSMA/CA.

It has been proven by P. Srivalli [15] through S-MAC protocol that by allocating a different transmission time to broadcast a message for many-to-one communication can reduce collision. This protocol followed contention-based protocol such as 802.11 together with virtual and carrier sense and Request-to Send (RTS)/Clear-to-Send (CTS) exchange. They proposed that the transmission time for every node will be given by the source node, which each node will take time to turn into sleep mode and thus avoid collision between each other. Similar work had been done by Kumaran [16] where he proposed a sensor-MAC (S-MAC) with a sleeping schedule. The protocol proposed manage to achieved good collision avoidance by utilizing contention scheme together with combined scheduling. Inspired by the inverse problem of mutual synchronization among fireflies to avoid collision, Haito Zhao [12] proposed an evolutionary-MAC (E-MAC) scheme where the next transmission time will be decided by the source node so that collision between nodes' transmission can be reduced. However, the next transmission time will be decided by the source node only after the collision had taken place, where the source node will adjust its transmission time so no clashing will take place again. All the authors mentioned have been focusing on the collision avoidance only, however there is no detection of data package losses due to the collision. Therefore, this paper works on the collision avoidance along with addressing scheme to resolve the issue so that data losses identification can be done. In addition, the issue mentioned also can be solve with only a simple addressing and random time transmission.

II. PROPOSED METHOD

An autonomous wireless sensor node based on Atmega328P with temperature and flame sensor, with 433MHz RF (UART) Transceiver Module-1km has been designed to test the proposed method. Moreover, a sink station is designed based on ESPresso Lite V2.0 from Espressif System's ESP8266 WROOM-02 WiFi module with the 433MHz RF (UART) Transceiver Module-1km. The sink station communicates with the wireless sensor nodes via the same RF module at the same frequency channel, and it uses the WiFi module to upload the received data to the cloud after analyze it. The sensor node is assumed as an end-user node where each node will not receive any data send by another sensor node, but will communicate directly to the sink station. Since multiple sensor nodes are going to send multiple data packages to the sink station through the same channel, thus data package collision is expected. Due to the fact that the sensor node has to spend most of its operating time in low power mode to conserve the energy [17], therefore, a random low power time is proposed here to tackle the collision issue. Regarding the main contribution of this paper, a new addressing scheme is proposed as shown in Fig. 2.

Node ID	/	Package ID	/	Sensor Data 1	/	Sensor Data 2

Fig. 2: The proposed Sensor node addressing string

The proposed addressing scheme is encapsulating the node data package with extra addressing and package sequence variables, making the node identification at the sink station easier. The addressing scheme is consisting of 7 bytes' length string in which it is created by the node and will be transmitted to the sink station. The length, number and the location of the string bytes are constant in each node, but only the bytes values will varied in according to the node address and sensors values. The first byte of the string is allocated to store the node address and it should be unique within the network overall. The following byte is the package id byte in which it holds the node package sequence to identify data losses due to collision during the transmission. The proposed addressing scheme in this paper supports only two sensor data: which is sensor data 1 that holds the temperature data, and sensor data 2 that holds the humidity data as shown in Fig. 2. However, this addressing scheme can support more of sensor data by adding on more byte at the end of the addressing string separated by a special character. All previously mentioned bytes are separated with a special character to isolate the node address string bytes so that the analyzing process of the addressing string at the sink station will be easier. An example of addressing string is shown below on Fig. 3:

1	/	1	/	30	/	44

Fig. 3: Example of addressing string

The addressing string example given in Fig. 3 above is created by the wireless sensor node (as shown in the wireless sensor node routine pseudo code below) and will be transmitted to the sink station. The sink station therefore can be able to differentiate the source of the received addressing string by analyze and scan through it (as shown in the sink station routine pseudo code below). Thus, Fig. 3 shows that the sink station received the first addressing string from sensor node 1, where the node environment temperature is 30◦C and the flame sensor value is 44.

- Wireless sensor node routine pseudo code:
  1. Initialize the sensor node MCU.
  2. Enter low power mode for random time.
  3. Create a seven bytes string.
  4. Include the node ID in the first byte of the string.
  5. Include special character to the following byte.
  6. Include package ID to the third byte of the string.
  7. Include special character to the following byte.
  8. Read the data from sensor 1.
  9. Include sensor 1 data to the fifth byte of the string.
  10. Include special character to the following byte.
  11. Read the data from sensor 2.
  12. Include sensor 2 data to the seven byte of the string.
  13. Transmit out the addressing string to the sink station.
  14. Jump to 2.

Pseudo code above explains how the wireless sensor node will behave according to the proposed addressing scheme. After the node MCU has been initialized, the node will turn into low power mode for a random time so that the sensor nodes will not access the RF channel at the same time for transmission, which leads to mitigate and avoid the data package collision with other sensor nodes' data package. The sensor node will directly create the seven bytes string after it wake up from the low power mode. As it is cleared, the first byte holds the identity of the source of the received data package. The package ID byte that shows the sequence of the node package will be stored in the third byte of the string. The sensor node will then read the data from the temperature sensor, process it, and stores the processed value in the allocated byte (sensor data 1). Same goes to the second sensor data, where the sensor node will read the data from the flame sensor, process it, and stores the processed value in the other allocated byte (sensor data 2). Each bytes mentioned above are separated by a special character to ease the analyzing and scanning process at the sink station. After all the bytes have been completely filled, the sensor node will transmit out the addressing string to the sink station then turns to low power mode again to start with another cycle.

- Sink station routine pseudo code:
  1. Initialize the sink station MCU.
  2. Wait for incoming addressing string.
     a. If addressing string received go to 3.
     b. Else, jump to 2.
  3. Scan through the incoming addressing string and divide it into 4 main bytes according to the special character separators.
  4. Check the first byte to identify the node ID.
  5. Check the second byte to identify the package ID.
  6. Check the third byte to identify the temperature value.
  7. Check the fourth byte to identify the flame value.
  8. Upload the analyzed data to the cloud.
  9. Jump to 2.

Based on pseudo code above, after the sink station initialized, it will wait for the incoming addressing string from the nodes. If there is any addressing string received, it will scan the addressing string and divide it into 4 main bytes according to the special character location. Note that only the node ID, package ID and the sensor data from every sensor in the system will be taken into account, since the separator used only for making the string analysis by the sink station easier. In case that there is no addressing string received, the sink station will be continue waiting. In analyzing the string, the sink station will identify the node ID from the first byte of the string, then continue with the second byte of the string, which is representing the package sequence of the node. The last two bytes are representing the node sensors data. After the sink station finish analyze all the addressing string, it will upload the analyzed data to the cloud for remote monitoring, and then it will continue to wait for an incoming addressing string form other sensor nodes. The position and the sequence of the addressing string byte will be fixed in all the wireless sensor nodes so that the sink station easily identify the node address and the package sequence as well.

III. RESULT AND DISCUSSION

The proposed wireless sensor node and the sink station were successfully prototyped as shown in Fig. 4 and Fig. 5 respectively. The proposed addressing scheme algorithm is implemented in the sensor node and sink station as stated in the methodology. The testing and the evaluation of the system had been done in a controlled laboratory environment. The result shown in Fig. 6 proved that the sink station was able to detect and differentiate the multiple node data with the help of the proposed scheme, however, the sensor nodes were sharing the same radio channel to talk to the sink station. The sensor nodes take turns to transmit their data through a random transmission time, and hence avoid collision from happen. Add on, with the proposed addressing scheme, the package ID will help in detecting the occurrence of the packages collision and data losses if happened. Therefore, it is easy for the operator to clarify if there is any collision happened from the package lost ID.

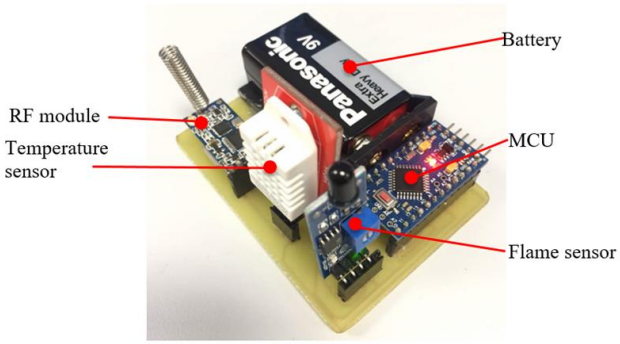

Fig. 4: Wireless sensor node prototype.

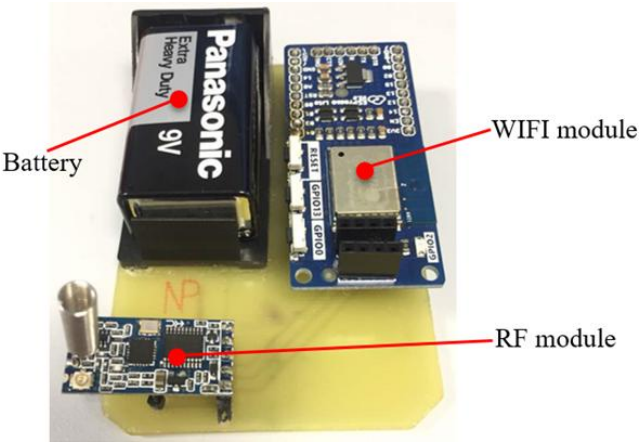

Fig. 5: Sink station prototype.

Fig. 6 shows that the base station is able to differentiate and analyze the address string that came from the different sensor nodes. From the first address string, the base station succeeds to identify that the address string came from sensor node 1 based on the first byte of the address string. Followed by the second byte, it shown that this is the first addressing string send by the sensor node with temperature data and the flame sensor value that is allocated on the third and fourth byte respectively.

During this period, there is no flame detected based on the value of the flame sensor. The second and third addressing string show that the second and third package send by sensor node 1 were received by the sink station. There were no significant changes in the temperature and flame sensor value. To test the functionality of the sensor node 2 with it sensors, the flame sensor was triggered with flame. Therefore, there is a drastic increase in the temperature and flame sensor value shown in the fourth received address string.

Fig. 6: Sink station response.

IV. CONCLUSION

Data packages transmission by numerous wireless sensor nodes to the sink station through a single radio frequency channel can disrupt the wireless sensor network due to collision of the data packages that been send simultaneously. Therefore, this paper proposed an addressing string scheme to assist the sink station in identifying the data package sources and avoid collisions. It has been successfully achieved by making the sensor nodes transmit their data packages through a random transmission time. To prove the concept of the proposed method, two identical wireless sensor nodes equipped with temperature and flame sensor with a sink station have been design as transmitter and receiver. From the result shown, the addressing string has been successfully implemented in the wireless sensor network designed and the sink station is able to differentiate and analyze the source of the received addressing string. Lastly, collision has been avoided by random transmission time proposed in this paper.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of this work by the Malaysian Ministry of Higher Education under the research grant PRGS/1/2016 /TK10/FKEKK-CETRI/02/T00016, UTeM-Industry Matching GLUAR/ IMPRESSIVE /2017/FKEKK-CETRI/I00024 and the facility support by the Faculty and Advanced Sensor and Embedded Control Systems (ASECs) Research Group, CeTRI, UTeM.

REFERENCES

1. G. Shanthi, M. Sundarambal, "FSO–PSO based multihop clustering in WSN for efficient Medical Building Management System", *Cluster Computing*, DOI.org/10.1007/s10586-017-1569-x, 2018.
2. G.Venkatesh, P.Chandramouli, "An IOT Based Environmental Radiation Monitoring Through Wireless Sensors Network", *Helix*, vol. 8, no. 1, pp. 2753- 2756, 2018.
3. M.Y. Aalsalem, W.Z. Khan, W. Gharibi, M.K. Khan, Q. Arshad, "Wireless Sensor Networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges", *Journal of Network and Computer Applications*, vol. 113, pp. 87–97, 2018.
4. M. M. Ibrahiem and S. Ramakrishnan, Wireless Sensor Networks from Theory to Applications. *Taylor & Francis Group*, 2014.
5. J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, 2013.
6. C.W. Hung, and W.T. Hsu, "Power Consumption and Calculation Requirement Analysis of AES for WSN IoT", *Sensors*, vol. 18, no. 1675, pp. 1-11, 2018.
7. S. Ali, T. A. Balushi, Z. Nadir, O.K. Hussain, "WSN Security Mechanisms for CPS", *Cyber Security for Cyber Physical Systems*, vol 768, pp. 65-87, 2018.
8. K. S. Yıldırım, R. Carli, L. Schenato, "Adaptive Proportional–Integral Clock Synchronization in Wireless Sensor Networks", *IEEE Transactions on Control Systems Technology*, vol. 26, no. 2, pp. 610 – 623, 2018.
9. Cytron Technologies, "RF-UART-433-1KM 433MHz RF Transceiver Module(UART)1km", *datasheet*, vol. 1.1, 2014.
10. B. Abid, H. Seba, and S. M'bengue, Collision Free Communication for Energy Saving in Wireless Sensor Networks. *InTech* 2012.
11. P. Dandare, V. Chole, "Detection of Collision Attacks and Comparison of Efficiency in Wireless Sensor Network", *International Journal of Engineering and Computer Science*, vol. 5, no.5, pp. 16400-16406, 2016.
12. H. Zhao, J. Wei, N. Sarkar, and S. Huang, "E-MAC: An Evolutionary solution for collision avoidance in wireless ad hoc networks", *Journal of Network and Computer Applications*, vol. 65, pp. 1-24, 2016.
13. C. Lei, H. Bie, G. Fang, E. Gaura, J. Brusey, X. Zhang and E. Dutkiewicz, "A Low Collision and High Throughput Data Collection Mechanism for Large-Scale Super Dense Wireless Sensor Networks", *Sensors*, vol. 16, no. 1108, pp. 1-16, 2016.
14. P. K. Sahoo, J.P. Sheu, "Design and Analysis of Collision Free MAC for Wireless Sensor Networks With Or Without Data Retransmission", *Journal of Network and Computer Applications*, vol. 80, no. 15, pp. 10-21, 2017.
15. P. Srivalli, N. Nagakumari, G. Anupama, V. Srujana, "Avoidance of Collision and Overhearing in Wireless Sensor Networks", International *Journal of Computer Science and Information Technologies*, vol. 2, no. 5, pp. 2300-2303, 2011.
16. M.S. Kumaran, "Survey on Reliable Transmission in Wireless Sensor Networks", *International Journal of Computer & Mathematical Sciences*, vol. 7, no. 3, pp. 143-145, 2018.
17. A. M. Abdal-Kadhim, and S.W. Kok, "Application of thermal energy harvesting in powering WSN node with event priority-driven dissemination algorithm for IoT applications", *Journal of Engineering Science and Technology*, vol. 13, no. 8, pp. 2569 – 2586, 2018.

AUTHORS PROFILE

Nurulidayu Binti Sainuddin was awarded bachelor degree in Electronic Engineering from the UTeM, Malaysia in 2019, exploring wireless sensor network and internet of things for hydroponic telemetry monitoring applications. Nurulidayu is currently pursuing her master degree at the same university. Her research interest includes scalable multi-hop wireless sensor networks.

Ali Mohammed Abdal-Kadhim received his M. Eng. degree in electronic and computer engineering from the UTeM, Malaysia in 2015, exploring embedded system design and robotics. He is currently pursuing the Ph.D. degree at the same university. His research interest includes embedded system and WSN design for IoT applications based hybrid energy harvesting. He has involved in several projects related to WSN based energy harvesting for telemetry monitoring also authored few papers related to WSNs and energy harvesting.

Kok Swee Leong was awarded Ph.D in Electronics and Electrical Engineering from the Southampton University, UK in 2010, exploring thick-film technologies for fabricating piezoelectric energy harvesting devices. Dr. Kok has been a lecturer in UTeM since 2003 after completing his MSc degree in Electrical, Electronic and System Engineering from UKM, researching on optical planar waveguide fabrication and characterization. He is currently an Associate Professor and also research leader of Advanced Sensors and Embedded Control Systems (ASECs) Research Group under the Center of Telecommunication and Innovation (CeTRI), UTeM. He have been author and co-author for more than 50 publications and reviewing IEEE, IOP, Elsevier and other Scopus indexed journals. His research interest is related to energy harvesting system and applications, MEMS, and thick-film devices fabrication technologies for the application of sensing, actuating and self-powering for wireless sensor network.