EFITA WCCA CIGR
2013 Conference
June 23-27, 2013
TORINO, ITALY
Sustainable Agriculture through ICT innovation

A Smart WSN Gateway with an Automatic Data Backup Mechanism for Large-scale Monitoring in Greenhouses

Yu-Chi Chang[1], Jie-Jyun Wan[1], Chia-Pang Chen[1], Cheng-Long Chuang[2], Hsun-Yi Chen[1], Chwan-Lu Tseng[3], and Joe-Air Jiang[1*]

[1] Department of Bio-Industrial Mechatronics Engineering, National Taiwan University, Taipei, Taiwan
No. 1, Sec.4, Roosevelt Road, Taipei 106, Taiwan
[2] Intel-NTU Connected Context Computing Center, National Taiwan University, Taipei, Taiwan
No. 1, Sec.4, Roosevelt Road, Taipei 106, Taiwan
[3]Department of Electrical Engineering, National Taipei University of Technology,
No.1, Sec.3, Chung-Hsiao East Road, Taipei 106, Taiwan
[*] Email of the corresponding author: jajiang@ntu.edu.tw

ABSTRACT

To efficiently monitor large-scale greenhouses, gateways in monitoring systems are designed to manage sensor nodes in different subareas of a sensing field in order to acquire real-time sensing data. It is a challenge to maintain the whole monitoring system in the large-scale greenhouse. Electronic monitoring devices deployed in a greenhouse may fail due to a lack of energy. This paper proposes an automatic data backup mechanism for WSN gateways to recover the monitoring data of sensor nodes in the subareas where their gateways fail. Gateways with an automatic data backup mechanism will start a monitoring procedure in every new round based on a fixed schedule to exchange their working status packets. As a result, the lost monitoring data of sensor nodes caused by a failed gateway can automatically be restored, and the data completeness can be effectively improved and eventually extending the lifetime of large-scale monitoring WSN.
Keywords: WSN, large-scale monitoring, data completeness

1. INTRODUCTION

In recent years, there has been a great progress on wireless communication technology and the applications of wireless networks have become necessities for modern life. Especially, wireless sensor networks (WSNs) [1], [2] are rapidly developed and applied to many areas like medical devices [3], military [4], and agriculture [5]. In particular, using centralized approaches, where data collected from each sensor is sent to a central base station, is not efficient when being applied to large wireless sensor networks, due to high rates of data collision and retransmission.

This paper proposed a great method to improve large-scale environmental surveillance in a greenhouse. Smart gateways were designed to manage sensor nodes in four different subareas of a sensing field for acquiring real-time sensing data. An automatic

Yu-Chi Chang, Jie-Jyun Wan, Chia-Pang Chen, Cheng-Long Chuang, Hsun-Yi Chen, Chwan-Lu Tseng, and Joe-Air Jiang. "A Smart WSN Gateway with Automatic Data Backup Mechanism for Large-scale Monitoring in Greenhouse". EFITA-WCCA-CIGR Conference "Sustainable Agriculture through ICT Innovation", Turin, Italy, 24-27 June 2013.

data backup mechanism was proposed for gateways to recover the monitoring data of sensor nodes in the subareas where their gateways failed. Through this mechanism, gateways would know whether other gateways were alive. When one (or more) gateways malfunctioned, remaining active gateways chose a suitable gateway as a candidate gateway. The selected gateway would take over the sensor nodes originally controlled by the failed gateway. Moreover, the smart gateways communicated with other and formed a network to exchange their information. The smart gateways in this paper also developed channel assignments and remote settings to monitor a greenhouse for users and to record the status of system operation for further data analysis. Such a design may improve data completeness.

2. RELATED WORK

In order to avoid packet loss, fault detection methods have been widely proposed by many existing studies. Some studies detected errors by monitoring node behavior. For example, Peng et al. [6] presented a history data and neighbors algorithm for node fault detection in fault management. This method served as a support for sensor network routing and optimization to maintain the system available. In [7], the authors proposed an approach that allowed a node to run a self-diagnosis program based on the measures of accelerometers, which determined whether a node had a hardware malfunction. In [8], a protocol named ‘fault tolerant sink (FTS)’ was developed to detect failure and recover a sink from an error state, so the sink could restart by including a backup sink scheme to replace the failed sink. This study probes into the task of gateway fault detection. In this study, the proposed mechanism provides the detection and identification by checking the working status packets.

3. MATERIALS AND METHODS

The main function of a gateway in a WSN was to control wireless senor nodes to collect sensing data. The sensing data included environmental information, such as temperature, relative humidity, and illumination. All of the collected data was sent to a backend database. The following subsections show the hardware and software of the gateways.

3.1. Hardware of gateways

Beagleborad-xM

In this study, the proposed system employed a Beagleboard-xM produced by the Digi-Key Corporation as the gateway. The specification of the Beagleborad-xM is shown in Table 1.The Beagleborad could equip with additional modules, and all modules could be activated via a program designed by Qt. The Beagleboard-xM used a base node to communicate with sensor nodes and transmit collected data to a backend database through the Internet.[9]

Base node

The base node was the interface for the gateway to communicate with senor nodes. The proposed wireless sensing network system employed the Octopus II as the node. The MCU of the Octopus II was constructed by MSP430F1611 manufactured by the Texas Instruments. The Octopus II used a low power-consumption CC2420 communication chip whose frequency was 2.4 GHz and followed the ZigBee specification and the IEEE 802.15.4 protocol. [10]

3.2. Gateway Software

The proposed gateways with the automatic data backup mechanism started a monitoring procedure in every new round based on a fixed schedule, shown in figure 4. The monitoring procedure would begin every thirty minutes to collect the real time environmental information in a large-scale greenhouse. In the beginning of a new session, the gateway checked up whether the Internet was available for connecting with the backend server. The gateway initialized system parameter settings, such as checking the RF value and quality of nodes. The next process was a handshake procedure, which was designed for the gateways in each subarea to exchange their working status packets. The working status packets included the network information regarding the gateway ID, controllable nodes, and the location of the gateways. By checking the working status packets, the gateways, which operated normally, would know malfunctioned sub-networks and build a malfunctioned gateway table to store the number of the gateways. Then, the gateways started to collect environmental data in their subareas. If any gateway malfunctioned, according to the malfunctioned gateway table and the working status information, the remaining gateways would choose a suitable candidate gateway to resume the control of the subarea where a gateway malfunctioned. As a result, the lost monitoring data of sensor nodes caused by a failed gateway could be automatically restored. The final procedure was for the gateway transmitting the sensing data to the backend server through the Internet. However, if the gateway could not build the connection with the server, the gateway would transfer the data to a helper gateway. In other words, the helper would upload the transferring data to the backend server. After all the procedures ended, the system would wait for the next round.

3.2.1 The Automatic Data Backup Mechanism

An automatic data backup mechanism was proposed to improve the data completeness and extend the lifetime of large-scale WSN-based monitoring systems. In order to efficiently monitor a large monitoring area, the monitoring area was divided into different subareas, and gateways were designed to manage sensor nodes in these subareas. In other words, the gateway in each subarea would organize sensor nodes into a sub-network. The originally large-scale monitoring network could be distributively controlled.

Through this mechanism, the gateways were able to know other gateways' working status. They exchanged the operating information packets with each other, including the information regarding the gateway ID, controllable nodes, and the Internet status. If a gateway malfunctioned, other gateways would not receive the working status packets of the gateway, and they would try to recover the sensing data in the sub-network by

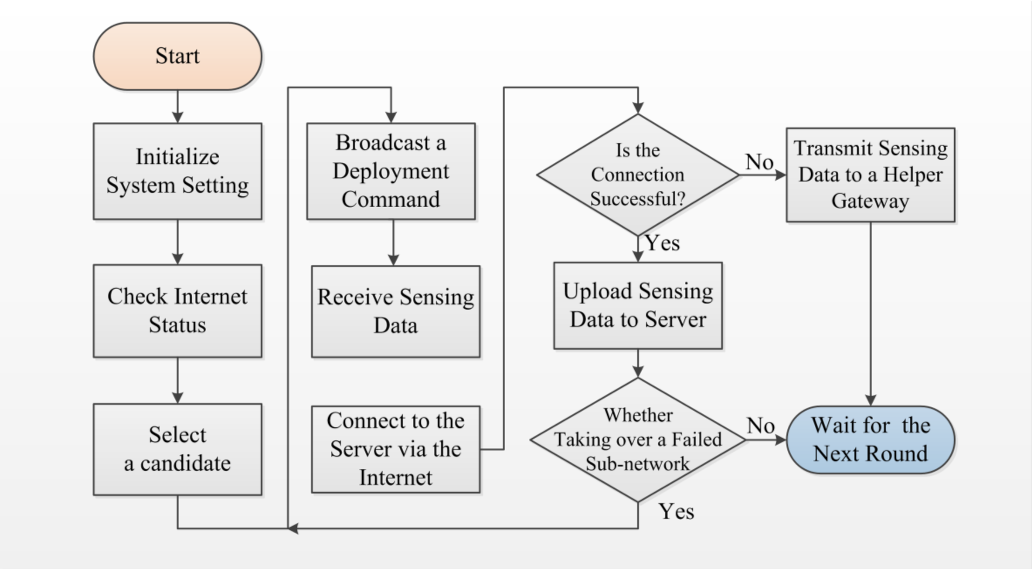


Fig.4 The program procedure of the gateway with the automatic data backup mechanism

finding a suitable gateway to take over the sub-network originally controlled by the failed gateway. The suitable candidate should be able to take over the maximum number of sensor nodes, making the whole system have the best successful rate of data delivery. In this study, the gateways would estimate the data delivery rate by using the following equation (1). The equation evaluated the possible data delivery if the gateway was the candidate which took over the sub-network. The gateway with the highest data delivery rate would be chosen to be the candidate. In equation (1),

$$\hat{A}_i = \frac{A_i \times N_i + A(d_{ij}) \times N_j}{N_i + N_j} \tag{1}$$

where $\hat{A}_i$ represents the estimated data, available for the active gateway *i*. The higher $\hat{A}_i$ suggests the higher possibility for the gateway to recover the complete data. *N* is number of nodes controlled by the gateway. The subscript *i* is the active gateway number, and the subscript *j* is the malfunctioned gateway number. A_i is the successful rate of data delivery for the active gateway *i*. The function $A(\cdot)$ shows the data delivery for the gateway controlling the failed sub-network. The distance d_{ij} shows the relative distance between the active gateway and the malfunctioned one. Thus, the successful rate of data delivery between the gateway *i* and *j*, can be obtained by $A(d_{ij})$. By checking the working status packets of active gateways, the gateways could evaluate the estimated successful rate of data delivery, which was the criterion of determining a suitable candidate gateway. The candidate would take over the sub-network originally controlled by a failed gateway.

3.2.2 Automatic wifi detection and data transfer function

The proposed gateway could automatically detect the connection with the Internet via a wifi module. The working status packets also showed the Internet status of the gateway. After receiving the sensing data from sensor nodes, the gateways would gather the data and send the data to a backend server through the Internet. If the Internet was failed, though the gateway was active and the sub-network was normal, the sensing data was not able to be sent to the backend server. This may cause sensing data loss and reduce the data completeness of the monitoring system. In this case, the gateway with failed Internet connection would choose a gateway with the smallest d_{ij} (which was a relative distance parameter for the gateway) whose Internet connection was available to transfer the collected data.

3.2.3 Automatic channels assignment

In order to build communication bridges between gateways, the proposed gateways were equipped with the function of channel assignment. In WSN-based large-scale monitoring, a large number of information packets needed to be transmitted during the monitoring. Thus, each sub-network was assigned with a communicate channel to avoid communication being interfered by others sub-networks. Such a function allowed the gateways to change their communication channels based on different requirements. All the gateways would change into the same communication channel in the gateway handshake procedure, and the candidate gateway would change its communicate channel to the communicate channel of the sub-network that needed to be taken over.

4. EXPERIMENTAL RESULTS

In this section, we present the experimental methods and results to show the efficiency of the automatic data backup mechanism. We have conducted experiments in a greenhouse where a monitoring system was deployed to validate the effectiveness of the proposed method.

4.1. Simulation of the proposed gateway

Before the simulations, we did an experiment to get the relationship between the successful rate of data delivery and the distance between gateways. Such a relationship was important for the proposed gateways to choose a suitable candidate. Given that different RF power and model of communication chips would affect the experimental results, in this experiment, the RF power was set to 25, and CC2420 was used as the model of communication chip in nodes.

Figure 5 shows the regression analysis results between the distance of gateways and data delivery (RDD) in the real site measurement. RDD was used to analyzed the relationship between d_{ij} and $A(\cdot)$ as a function. A general linear regression model with normal error terms can be defined as:

$$Y_i = \beta_0 + \beta_1 X_{i1} + \beta_2 X_{i2} + \ldots + \beta_p X_{ip} + \varepsilon_i. \qquad (2)$$

where Y is the dependent variable, X_{i1} to X_{ip} is the independent variables, β_0 to β_p are parameters to estimate, and ε_i is the error term.

In this study, we chose the second order, i.e. $p = 2$, to obtain the regression equation:

$$y = -0.0011x^2 + 0.0115x + 0.9899. \qquad (3)$$

In figure 5, a downward trend was found when the distances between the active gateway i and the malfunctioned gateway j increased. When d_{ij} was above 10 m, $A(\cdot)$ significantly declined. After that, the higher d_{ij}, the more decrease in $A(\cdot)$.

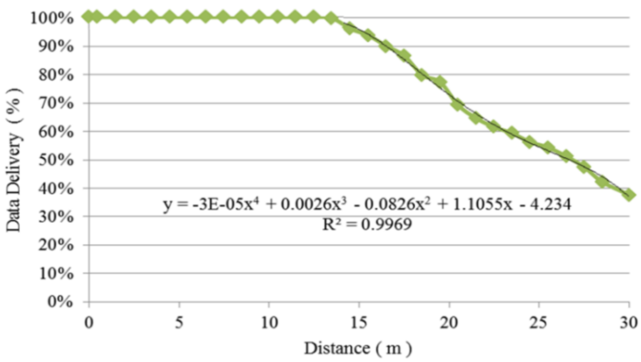


Fig.5 The regression of the successful rate of data delivery and distance between the active and failed gateway

Furthermore, a number of simulations were conducted to examine the performance of the proposed gateway with the automatic data backup mechanism. The simulation used six gateways and 120 sensor nodes. Each of the gateways controlled 20 nodes. All the gateways were placed within the communication range, and the nodes were placed surrounding the gateway. The proposed mechanism was designed to avoid data loss when a gateway malfunctioned and the sensor nodes in the sub-network would be taken over by a candidate gateway, and when the Internet of a gateway was not available to transmit data to a backend server and the gateway that was closest to the gateway with failed Internet connection would be selected as the data transfer helper to transmit data to the server. In the simulations, five of six gateways, one at a time, would stop their operation every 10 rounds. The simulation results, as presented by the successful rate of data delivery, are shown in Table 2. The results showed that the proposed system could maintain the data delivery above seventy present while others gateways failed. However, the data delivery would decrease by the number of failed gateways increased.

Table 2 The data delivery of the whole system when different numbers of gateways failed

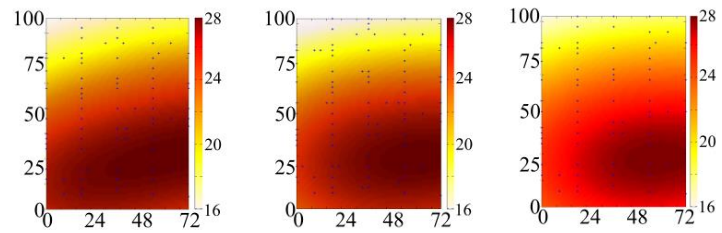
# of Gateways Malfunctioned	1	2	3	4	5	6
Data Dilvery Rate With ADBM*	0.733	0.767	0.85	0.883	0.933	1
Data Divery Rate Without ADBM*	0.167	0.333	0.5	0.667	0.833	1

Note: *the automatic data backup mechanism

4.2 Real deployment in a large-scale greenhouse

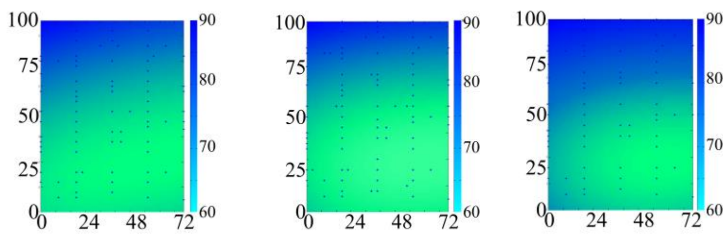
Furthermore, in order to evaluate the efficiency of the proposed gateway in actual deployment, we deployed a wireless sensing network in a large-scale greenhouse to examine whether the proposed method could offer reliable data transmission for practical monitoring networks. The deployment site was a large-scale cymbidiumorchid greenhouse that occupied an area of 7200 (m^2). Cymbidiumorchid was a remunerative crop. Some environmental factors, included uneven temperature distribution, plant bed transportation, non-ventilated room, would affect the growth of the plats.[12] The monitoring area was divided into five sub-areas, and a total of five gateways and over 120 nodes were deployed to five sub-areas to form five sub-networks. The figure 6 shows the real deployment in the greenhouse. Figure 7 and figure 8 show the variations of temperature and humidity in the greenhouse based on the data collected on May 21. Due to the result of watering, the temperature was lower and the humidity was higher in the upper right corner. Figure 7(a) and figure 8(a) show the variations of temperature and humidity when all gateways operated properly. With the proposed data backup mechanism, the monitoring information could be recovered, and the completeness of temperature and humidity data could be maintained, when two gateways were malfunctioned. Thus, the variations in figure 7(b) and 8(b) are more similar to those in figure 7(a) and 8(a), compared to figure 7(c) and 8(c). Based on these results, the proposed system could offer reliable data transmission for practically deployed monitoring networks, even if some of the gateways failed. .

Fig.6 Real deployment in the large-scale cymbidiumorchid greenhouse



(a) (b) (c)

Fig.7 The temperature variation of the cymbidiumorchid greenhouse
(a) without introducing any failed gateways; (b) employing ADBM when two gateways failed; and (c) without employing ADBM when two gateways failed



(a) (b) (c)

Fig.9 The humidity variations of the cymbidiumorchid greenhouse
(a) without introducing any failed gateways; (b) employing ADBM when two gateways failed; and (c) without employing ADBM when two gateways failed

C0160
Yu-Chi Chang, Jie-Jyun Wan, Chia-Pang Chen, Cheng-Long Chuang, Hsun-Yi Chen, Chwan-Lu Tseng, and Joe-Air Jiang. “A Smart WSN Gateway with Automatic Data Backup Mechanism for Large-scale Monitoring in Greenhouse” . EFITA-WCCA-CIGR Conference “Sustainable Agriculture through ICT Innovation”, Turin, Italy, 24-27 June 2013.

5. CONCLUSIONS AND FUTURE WORKS

According to the experimental results, the proposed gateway with the automatic data backup mechanism can improve the reliability of data delivery. Using the automatic data backup mechanism is a good solution to ensure data continuity and completeness of the monitoring data, so the lost monitoring data caused by a failed gateway can automatically be recovered, and the data completeness can be effectively improved and eventually extending the lifetime of large-scale monitoring WSNs.

6. REFERENCES

Peng, Y., J. Song, and X. Y. Peng. 2011. A Self Detection Technique in Fault Management in WSN. In *2011 IEEE Instrumentation and Measurement Technology Conference, 10-12 May*. 1 – 4. Binjiang, China.

Lester, H. System architecture for wireless sensor networks. 2003. *Doctoral thesis*. University of California, Berkeley.

Dessart, N., P. Hunel, C. Rabat and H. Fouchal. 2010. Simulation of large scale WSN for medical care. In *2010 IEEE Computers and Communications (ISCC), 22-25 June.* 1115- 1120. Univ. Riccione, Italy.

Hussain, M., P. Khan and K. K. Sup. 2009. WSN research activities for military application. In *11th International Conference on Advanced Communication Technology, 15-18 Feb.* 271- 274. Phoenix Park, Ireland.

Pande, M. and S. Pathak and D. Mukhopadhyay. 2012. H2E2: A hybrid, hexagonal & energy efficient WSN green platform for precision agriculture. In *2012 12th International Conference on Hybrid Intelligent Systems (HIS), 4-7 Dec.* 155 – 160. Pune, India.

Harte, S., A. Rahman, and K.M. Razeeb. 2005. Fault tolerance in sensor networks sing selfdiagnosing Sensor Nodes. In *The IEE International Workshop on Intelligent environment, 29 June*. 7–12.

Paradis, L. and Q. Han. 2007. A Survey of Fault Management in Wireless Sensor, *Journal of Network and systems Management, Vol. 5, Issue 2*, June.

Ammari, H. M. and S. K. Das. 2009. Fault Tolerance Measures for Large-Scale Wireless Sensor Networks. *Journal of ACM Transactions on Autonomous and Adaptive Systems, Vol. 4, Issue 1*, January.

Sheu, J. P., C. J. Chang, C. Y. Sun and W. K. Hu. 2008. WSNTB: A testbed for heterogeneous wireless sensor networks. In *Proceedings of 1st IEEE International Conference on Ubi-Media Computing, 31 July-1 August*. 338–343. Lanzhou, China.

USA: Beagleboard.org. 2011. Beagleboard-xM Product Details. Available at: http://beagleboard.org/hardware-xM

Gent, M.P.N. and Y. Z. Ma. 1998. Diurnal Temperature Variation of the Root and Shoot Affects Yield of Greenhouse Tomato. In *HortScience : a publication of the American Society for Horticultural Science, V33 (1), May*. 45-51.