

A Reliable Data Collection Scheme with Efficiency Consideration for ZigBee Wireless Sensor Network Applications

Shih-Sung Lin*, Chien-Wu Lan, Ping-Nan Chen¹ and Ya-Hui Wu

Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology,
National Defense University, No. 75, Shiyuan Rd., Daxi Dist., Taoyuan, 335, Taiwan, R.O.C.

¹Department of Biomedical Engineering, National Defense Medical Center,
No. 161, Sec. 6, Minquan E. Rd., Neihu Dist., Taipei, 114, Taiwan, R.O.C.

(Received December 25, 2014; accepted May 11, 2015)

Key words: ZigBee, wireless sensor network, tree topology, transmission reliability, data collection efficiency

ZigBee devices and ZigBee wireless sensor networks (ZWSNs) are popularly utilized in developing monitoring and control (MC) applications. In this paper, a reliable data collection scheme with efficiency consideration for ZWSN-based MC systems is proposed. An empirical approach is adopted to tackle the issues of transmission reliability and data collection efficiency. Several experiments are performed to facilitate the analysis of factors that may result in packet losses and the measurement of data transmission times between ZigBee nodes. Therefore, a reliable data transmission method that contains mechanisms of receiving confirmation, retransmission for overdue, and retransmission for busy delay is developed to successfully solve the packet loss phenomenon. In addition, a new data collection scheme that utilizes the last-stage ZigBee router to perform polling to ZigBee end devices is proposed to effectively enhance the total data collection efficiency. In particular, the experimental results show that the total data collection time of our method can be 4.45 times lower than that of the traditional approach if there are 8 ZigBee routers and 8 ZigBee end devices in the MC system.

1. Introduction

ZigBee devices possess characteristics of small size, light weight, and low power consumption. A ZigBee wireless sensor network (ZWSN) can have up to 65535 nodes theoretically. Therefore, ZWSN is very suitable for various monitoring and control (MC) applications, such as remote healthcare,⁽¹⁾ remote control of home appliances,^(2,3) industrial control,⁽⁴⁾ and environmental monitoring.^(5,6) A ZWSN has three typical

*Corresponding author: e-mail: shihunglin@gmail.com

types of topology: star, tree, and mesh.⁽⁷⁾ In a ZWSN with star topology, the distance between the coordinator and the sensor nodes is less than 100 m. This fact limits the operating extent of a MC system based on the ZWSN with star topology. The mesh-topology ZWSN is more complex than the ZWSN with star or tree topology. Thus, the MC system based on the mesh-topology ZWSN is more complicated than those based on the ZWSN with the other two topologies in terms of the control and management mechanisms of sensor nodes. By contrast, in a tree-topology ZWSN, the coordinator is the root of the tree, and the router nodes can relay data to other ZigBee nodes. Thus, by adding extra routers between the coordinator and the ZigBee sensor nodes, the operating extent of a MC system based on the tree-topology ZWSN can extend through multi-hop transmission. In addition, the tree topology is less complex than the mesh topology. Therefore, the tree-topology ZWSN is popularly utilized in various remote MC systems. We also focus on the tree-topology ZWSN in this study.

The ZigBee protocol stack consists of several layers. The bottom two layers are the physical layer (PHY) and the media access control layer (MAC), which are specified by the IEEE 802.15.4 standard, whereas the ZigBee Alliance defines other layers, such as the network layer (NWK) and the application layer (APL).^(8,9) Most studies that focused on the data transmission reliability and efficiency issues of WSN worked on the MAC layer. The communication on the MAC layer contains two modes: beacon and nonbeacon. In the beacon mode, the sensor nodes can utilize guaranteed time slots (GTSs) to achieve reliable communication.^(10–12) However, the MAC beacon mode can provide only 7 GTSs.⁽¹³⁾ Once the number of sensor nodes is excessive (greater than 7), the contentionless media access may be broken, thereby adversely affecting the transmission reliability. On the other hand, the coordinator can wirelessly collect data from the sensor nodes using the nonbeacon mode. However, the rate of packet losses will increase as the number of sensor nodes increases while using the nonbeacon mode for wireless data transmission.^(14,15) To improve the data transmission reliability in the nonbeacon mode, some studies, such as those described in refs. 16 and 17, adjust the values of the back-off parameters in the carrier sense multiple access with collision avoidance (CSMA/CA) algorithm. However, this approach cannot achieve 100% reliable data transmission. Besides, enlarging the back-off parameters will increase the latency of data transmission. Some other studies, such as those proposed in refs. 18–20, utilize the coordinator to perform polling on sensor nodes to reduce the rate of packet losses. Nonetheless, this approach may cause delay in data transmission of the whole WSN, which will reduce the total data transmission efficiency.

In this work, we aim to improve the aforementioned shortcomings of the existing methods in terms of transmission reliability and data collection efficiency. First, we introduce the architecture of the ZWSN-based remote MC system used in this study. Then, we investigate the packet loss phenomenon of the ZWSN in the nonbeacon mode. Accordingly, we develop a reliable data transmission method to effectively solve the packet loss phenomenon between two ZigBee nodes. Next, on the application layer, instead of the MAC layer, we develop an efficient data collection scheme for the ZWSN. Finally, we construct a ZWSN-based MC paradigm system to validate the effectiveness of the proposed methods.

2. Architecture of the ZWSN-Based Remote MC System under Study

Figure 1 shows the architecture of the ZWSN-based remote MC system under study. The abbreviations used in Fig. 1 are explained as follows.

- (1) ZigBee coordinator (ZC): The ZC is responsible for creating the ZWSN, together with managing and controlling other ZigBee nodes in the ZWSN. The ZC connects with the remote MC server (RMCS) through a universal serial bus (USB) connection.
- (2) ZigBee end device (ZED): The ZED connects with various sensors and is deployed in the storeroom. It can acquire various environmental data, such as temperature, humidity, pressure, and luminosity, through sensors for the MC system. Thus, a ZED is referred to as a sensor node.
- (3) ZigBee controller router (ZCR): In each MC area, we install a ZCR to control and manage all of the sensor nodes in that area. The ZCR is also responsible for collecting data from the underlying sensor nodes and sending the collected data to the ZC.
- (4) ZigBee pure router (ZPR): The ZPR is utilized only for relaying messages for other ZigBee nodes. By using ZPRs, we can extend the operating extent of the ZWSN through multi-hop transmission.

The architecture of the ZWSN-based remote MC system consists of three parts: equipment side, server side, and client side. The equipment side contains a ZWSN with sensors. Each storeroom is equipped with a ZCR and many ZEDs. Several ZPRs may be deployed between the ZC and the ZCR for extending the communication distance. The ZC connects with the RMCS through a USB connection. The server side consists of a RMCS and the system database. The RMCS can send commands to and receive data from the ZC through a USB interface. The users on the client side can utilize PCs and notebooks to remotely operate the MC functions of the RMCS through the Internet.

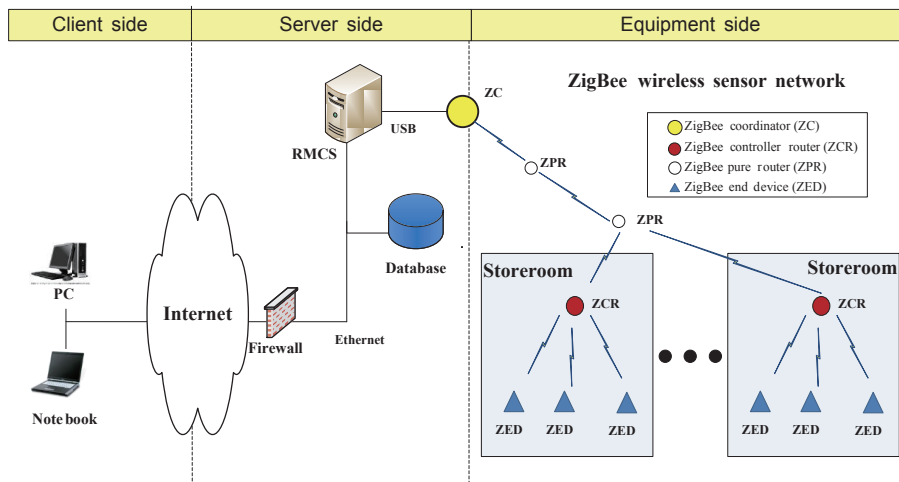


Fig. 1. (Color online) Architecture of the ZWSN-based remote MC system under study.

3. Reliable Transmission Method between ZigBee Nodes

3.1 Analysis of packet losses

In order to investigate the packet loss problem of ZigBee wireless data transmission, we built an experimental environment by constructing a ZWSN in an indoor space, as shown in Fig. 2. The indoor space is 61 m long and 23.7 m wide. In the figure, the ZC, ZCR, and ZEDs are indicated by a yellow circle, a red circle, and blue triangles, respectively. The ZC is installed in a room, located in the lower right corner, and connected with the RMCS. The room has side walls so that the ZC cannot directly communicate with ZEDs. The ZCR is deployed in the middle of the right-hand side to collect the sensed data from the ZEDs. N denotes the number of ZEDs, and L represents the communication distance between the ZCR and the ZEDs. In this experiment, we conduct three tests with L values of 10, 30, and 60 m. In each test, the N value varies from 1 to 8.

The experimental procedure of each test is described as follows: Step 1: The RMCS sends the data collection command to the ZC through a USB connection. Step 2: The ZC transmits the command to all of the ZEDs through the ZCR using broadcast communication. Step 3: After receiving the command, each ZED sends data of S bytes to the ZCR using the CSMA/CA algorithm, where S is 10 or 80. Step 4: Once the data of S bytes is received, the ZCR sends the data to the RMCS through the ZC. Step 5: After receiving the data, the RMCS stores the data into the database for calculating the packet loss rate.

The testing results of packet loss rate are shown in Fig. 3. As Figs. 3(a)–3(c) show, if the number of nodes, N , equals one, there is no packet loss. By contrast, if N is more than one, the packet loss phenomenon may occur and tends to be severe as N increases regardless of the payload size S and the communication distance L . This means that the number of nodes is the dominant factor affecting the packet loss rate. Besides, at the same L and N values, the packet loss rate of sending 80 bytes of data is higher than that of sending 10 bytes of data. In addition, as shown in Fig. 3(d), the communication distance does not affect the packet loss rate much under the same payload ($S = 10$ bytes).

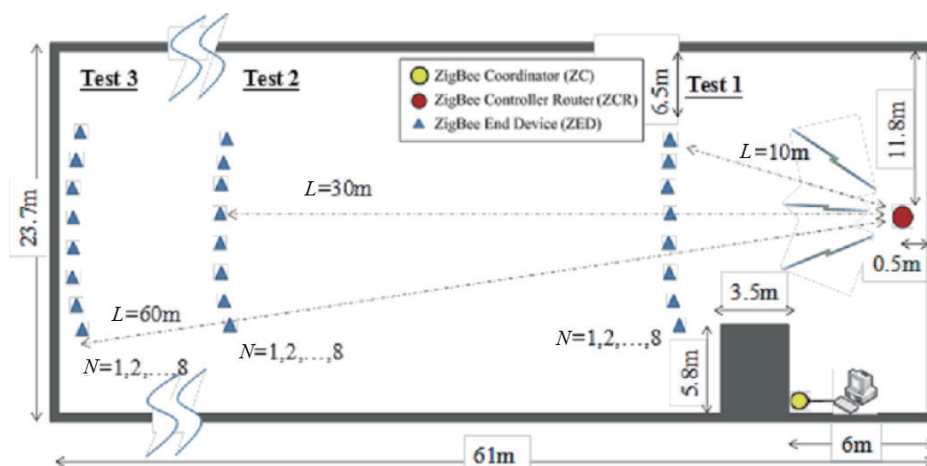


Fig. 2. (Color online) ZWSN deployment for analyzing and testing packet loss.

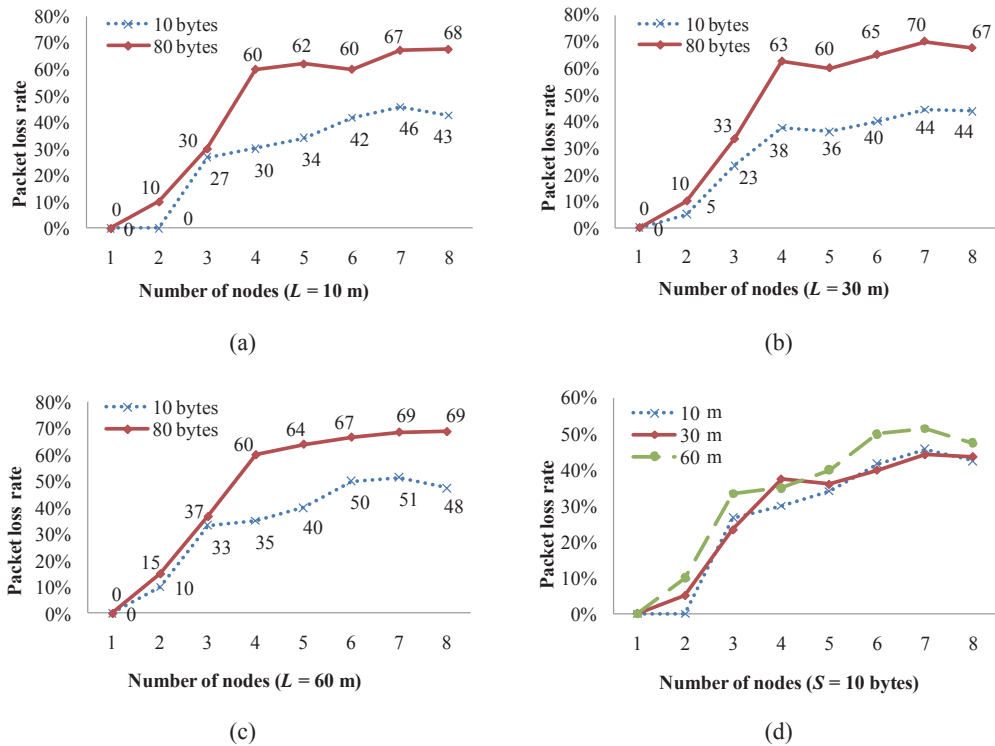


Fig. 3. (Color online) Test result of packet loss rate with different numbers of sensor nodes and different sizes of payload. (a) $L = 10$ m, (b) $L = 30$ m, (c) $L = 60$ m, and (d) $L = 10, 30$, and 60 m and $S = 10$ bytes.

3.2 Reliable data transmission method

In this section, we present a reliable data transmission method for the ZWSN. According to the above experimental results, if the number of ZEDs is greater than one, packet losses may occur. The main reason is that the ZEDs adopt the CSMA/CA algorithm for media access control. Before sending out a packet, each ZED evaluates the clearness of the communication channel (CC). If the CC is clear, the ZED sends the packet out. If the CC is busy, the ZED will wait for a random back-off time and then evaluate the CC again. The above process may repeat several times, which is a preset value, until the ZED abandons the transmission task. When there are more than one ZED needing to send packets out, some of the ZEDs may not be able to gain access to the CC through the CSMA/CA process, thereby giving up their transmission tasks and resulting in packet losses. In contrast, if we allow only one ZED to transmit data at any time, the above problem can be avoided, thereby resulting in no packet losses.

Hence, a possible way of achieving reliable wireless data transmission between two ZigBee nodes is by the one-to-one and receive-then-acknowledge mechanism. In other words, at any time, only one ZigBee device (sender node) sends data to another

ZigBee device (receiver node). Also, after receiving the data, the receiver node sends an acknowledgement (Ack) message to the sender node to confirm the successful data transmission. However, there are still some circumstances that may break the reliable data transmission. In the following, we discuss these circumstances and propose related solutions to make the transmission reliable.

(1) Retransmission-for-overdue mechanism

When the ZWSN encounters unstable linkage or wireless interference, the following two situations may take place. First, the receiver node does not receive the packet sent by the sender node, as shown in Fig. 4(a). Second, the sender node does not receive the Ack message sent by the receiver node, as shown in Fig. 4(b). To cope with this problem, we propose a retransmission-for-overdue mechanism, as shown in Fig. 4(c). After sending a packet out, the sender node will start a timer. If the sender node still does not receive the Ack message from the receiver node after a preset period of time, the sender node will retransmit the packet to the receiver node. The above retransmission-for-overdue process can repeat ten times at most. If the transmission still fails, meaning that the communication channel is heavily unstable or suffers severe interference, the sender node abandons the transmission task.

(2) Retransmission-for-busy-delay mechanism

When the receiver node is busy and receives the packet from the sender node, it will send a busy message to the sender node, causing the transmission failure. Hence, we proposed a retransmission-for-busy-delay mechanism to deal with this problem. If the sender node receives a busy message from the receiver node, it will retransmit the packet to the receiver node after waiting for a preset period of time, called busy delay. The above retransmission-for-busy-delay process can repeat ten times at most until the sender node receives the Ack message from the receiver node.

The proposed reliable data transmission method contains the one-to-one and receive-then-acknowledge mechanism, the retransmission-for-overdue mechanism, and the

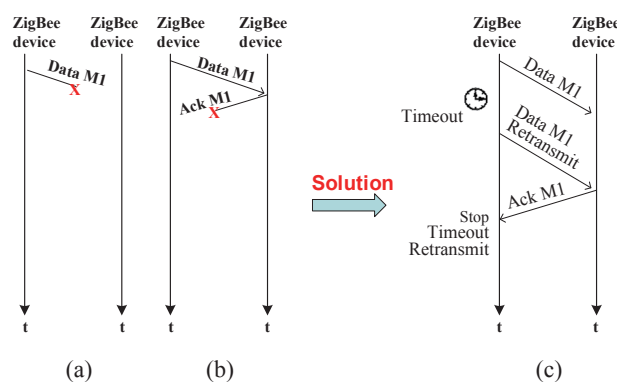


Fig. 4. (Color online) Design concept of the retransmission-for-overdue mechanism. (a) and (b) Packet loss. (c) Timeout retransmit.

retransmission-for-busy-delay mechanism. To verify the effectiveness of the proposed reliable data transmission method, the experiment described in § 3.1 is conducted again, but these three mechanisms are used for data transmission. The testing results are shown in Fig. 5. The packet loss rates of all the tests reduce to zero, thereby demonstrating that the proposed method can solve the packet-loss problem.

4. Efficiency Analysis of the Reliable Transmission Method

4.1 Efficiency analysis of data collection

The data collection efficiency of the ZWSN using the proposed reliable data transmission method is analyzed in the following. Figure 6 shows the procedure of data collection by using multi-hop transmission in a ZWSN-based MC system. The proposed reliable data transmission method is used for wireless data transmission between two ZigBee nodes. N denotes the number of ZigBee routers. The data collection procedure is described as follows. (1) The RMCS sends the command of data collection to the ZC through a USB interface. (2) The ZC passes the command to Router 1 (the first-stage router) over the air, and Router 1 sends an Ack message to the ZC after receiving the command. (3) In a similar way, the command is sent to the ZED through multi-hop communication, i.e., the command passing through Router 2 to N , sequentially. (4) After receiving the command, the ZED sends the collected data to the RMCS through the reverse path.

In the experiment, the maximum number of hops is 4, and the data size is 10 or 80 bytes. The data collection times with different hops and different data sizes are shown in Table 1. The data collection paths are depicted in the first row. RMCS↔ZC indicates the round-trip path between the RMCS and the ZC, RMCS↔ZC↔ZR1↔ZED denotes the round-trip path between the RMCS and the ZED in Fig. 6 with only one hop, and so

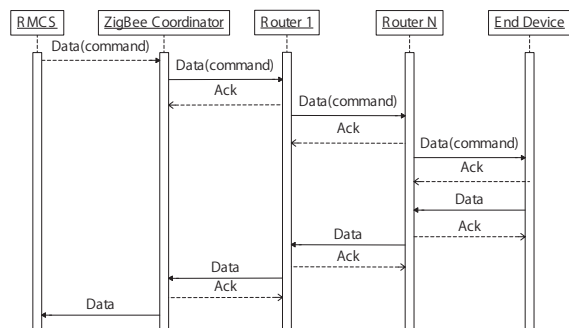
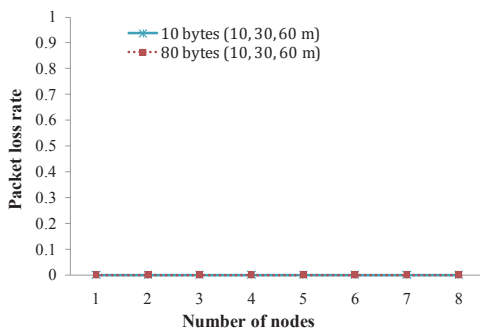


Fig. 5 (left). (Color online) Test result of packet loss rate by using reliable data transmission method.

Fig. 6 (right). Procedure of data collection by using multi-hop transmission.

Table 1
Data collection time with different hops and data sizes.

Size\path	RMCS ↔ZC	RMCS ↔ZC ↔ZED	RMCS ↔ZC ↔ZR1 ↔ZED	RMCS ↔ZC ↔ZR1 ↔ZR2 ↔ZED	RMCS ↔ZC ↔ZR1 ↔ZR2 ↔ZR3 ↔ZED	RMCS ↔ZC ↔ZR1 ↔ZR2 ↔ZR3 ↔ZR4 ↔ZED
Hops	0	0	1	2	3	4
Data collection time	T_{ZC}	T_{0ZE}	T_{1ZE}	T_{2ZE}	T_{3ZE}	T_{4ZE}
10 bytes	10.68 ms	39.68 ms	70.80 ms	102.86 ms	135.38 ms	166.94 ms
80 bytes	29.64 ms	60.70 ms	95.68 ms	132.18 ms	166.60 ms	200.54 ms

on. The number of hops is shown in the second row. T_{ZC} , T_{0ZE} , T_{1ZE} , T_{2ZE} , T_{3ZE} , and T_{4ZE} represent the data collection time through each round-trip path. The collection times for data of 10 and 80 bytes are listed in the 4th and 5th rows, respectively. On the basis of the figures in Table 1, the relationship between the data collection time and the number of hops is plotted in Fig. 7. The data collection time is almost linearly proportional to the number of hops.

The detailed time latency in each path is further analyzed as follows.

(1) Time computation from RMCS to ZC

The baud rate of the serial port of the RMCS is set at 38400 bps in order to match the baud rate of the ZigBee device. Thus, the time consumption for sending B bytes from the RMCS to the ZC through the serial port can be computed as

$$T_s(B) = \frac{B \times 10}{38400} \times 1000 = 0.2604B \text{ (ms)}. \quad (1)$$

(2) Time computation over the air

The maximum transmission rate in the ZWSN is 250 kbps. Thus, the time consumption for sending one byte over the air can be computed as

$$T_z = \frac{1 \times 8}{250000} \times 1000 = 0.032 \text{ (ms)}. \quad (2)$$

However, in addition to the payload, each ZigBee packet contains the stack's headers and checksum whose size is about 34 bytes. Hence, the time consumption for sending a payload of B bytes over the air can be computed as

$$T_{\text{air}}(B) = B_{\text{total}} \times T_z = (34 + B) \times 0.032 \text{ (ms)}. \quad (3)$$

(3) Time consumption for processing CSMA/CA algorithm

According to the ZigBee specification, we set the parameter of back-off time to 3, the average value. Thus, the back-off time can be computed as

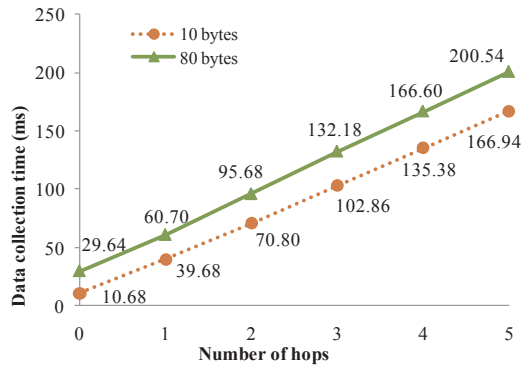


Fig. 7. (Color online) Relationship between data collection time and number of hops.

$$T_b = \frac{(2^3 - 1)}{2} \times 0.32 = 1.12 \text{ (ms)}. \quad (4)$$

After waiting for a back-off time, the ZigBee device will execute clear channel assessment (CCA) to check whether the channel is available for the transmission. CCA needs 8 symbol durations, and one symbol duration takes about 0.016 ms in 2.4 GHz. Therefore, the time consumption of CCA can be computed as

$$T_{\text{caa}} = 8 \times 0.016 = 0.128 \text{ (ms)}. \quad (5)$$

The time consumption for processing the CSMA/CA algorithm is the sum of T_b and T_{caa} .

$$T_{\text{CSMA/CA}} = T_b + T_{\text{caa}} = 1.12 + 0.128 = 1.248 \text{ (ms)} \quad (6)$$

According to the testing results in Fig. 7, we can compute the data processing time, called overhead, in the RMCS and the ZigBee devices in the data collection process as follows. The data processing time in the RMCS and the ZC is represented by T_1 and can be estimated as

$$T_1 = T_{\text{ZC}} - T_s. \quad (7)$$

The data processing time in the ZC and the ZED is denoted by T_2 and can be estimated as

$$T_2 = T_{\text{ZE}} - T_{\text{ZC}} - 4 \times T_{\text{CSMA/CA}} - 2 \times T_{\text{air}}(B_{\text{ACK}}) - T_{\text{air}}(B_{\text{CMD}}) - T_{\text{air}}(B_{\text{DATA}}). \quad (8)$$

The data processing time in the ZR1 and the ZED is denoted by T_3 and can be estimated as

$$T_3 = T_{\text{ZE}} - T_{\text{ZE}} - 4 \times T_{\text{CSMA/CA}} - 2 \times T_{\text{air}}(B_{\text{ACK}}) - T_{\text{air}}(B_{\text{CMD}}) - T_{\text{air}}(B_{\text{DATA}}). \quad (9)$$

By using the data in Table 1 and eqs. (1)–(9), the data processing times of different data sizes are estimated, as shown in Table 2. Note that the data processing time in the ZigBee devices is much greater than the time consumed in data transmission over the air and in processing the CSMA/CA algorithm. Hence, $T_{\text{CSMA/CA}}$ and T_{air} are ignored in the following analysis of the total data collection time.

4.2 Proposed method to enhance data collection efficiency

Traditionally, the data collection scheme uses the RMCS to perform polling on the ZEDs. To enhance the data collection efficiency, we propose a new data collection scheme that utilizes the last-stage ZigBee router to perform polling on the ZEDs.

(1) Traditional data collection scheme

In the procedure of a traditional data collection scheme, the RMCS performs polling to the ZEDs. The RMCS collects data from each ZED by following the procedure in Fig. 6. Thus, the total data collection time from a ZED with one ZigBee router can be estimated as

$$T_{\text{RMCS}} = T_s + T_1 + T_2 + T_3. \quad (10)$$

If there are N ZEDs, the total data collection time through one ZigBee router can be estimated as

$$T_{\text{RMCS}} = N \times (T_s + T_1 + T_2 + T_3). \quad (11)$$

If there are N ZEDs and M ZigBee routers in the ZWSN, the total data collection time can be estimated as

$$T_{\text{RMCS}} = N \times (T_s + T_1 + M \times T_2 + T_3). \quad (12)$$

(2) Proposed data collection scheme

The proposed data collection scheme uses the last-stage ZigBee router, instead of the RMCS, to perform polling to the ZEDs. The procedure of the proposed data collection scheme is shown in Fig. 8. If there are N ZEDs and one ZigBee router in the ZWSN, the total data collection time can be estimated as

Table 2
Data processing times of different data sizes.

Time	Data size (10 bytes)	Data size (80 bytes)
T_s	2.86 ms	21.09 ms
T_{air}	1.41 ms	3.65 ms
$T_{\text{CSMA/CA}}$	1.25 ms	1.25 ms
T_1	7.82 ms	8.55 ms
T_2	22.60 ms	22.42 ms
T_3	25.26 ms	26.23 ms

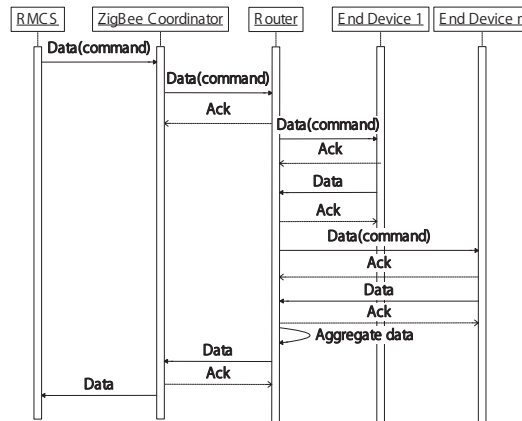


Fig. 8. Procedure of the proposed data collection scheme using the last-stage ZigBee router to perform polling to ZEDs.

$$T_{ZCR} = T_s + T_1 + T_2 + N \times T_3. \tag{13}$$

If there are N ZEDs and M ZigBee routers in the ZWSN, the total data collection time can be estimated as

$$T_{ZCR} = T_s + T_1 + M \times T_2 + N \times T_3. \tag{14}$$

4.3 Efficiency comparison of data collection schemes

The difference in the total data collection times of the above two data collection schemes can be computed using eq. (12) minus eq. (14):

$$T_D = (N - 1) \times (T_s + T_1 + M \times T_2). \tag{15}$$

From eq. (15), the proposed data collection scheme can have a shorter total data collection time than the traditional one. The more routers in the ZWSN, the more time can be saved by using the proposed scheme. A performance enhancement index (PEI) is defined as follows to indicate how efficient the proposed scheme can be:

$$PEI = \frac{T_{RMCS}}{T_{ZCR}} = \frac{N \times (T_s + T_1 + M \times T_2 + T_3)}{T_s + T_1 + M \times T_2 + N \times T_3}. \tag{16}$$

In the case that the payload size is 10 bytes, we can get $T_s = 2.86$ ms, $T_1 = 7.82$ ms, $T_2 = 22.60$ ms, and $T_3 = 25.26$ ms. By varying the values of N and L in eq. (16), we can evaluate the PEI under various conditions. For example, in the case of $N = 8$ and $M = 8$, the PEI is about 4.45, meaning that the proposed data collection scheme is much more efficient than the traditional one.

5. Experimental Evaluation of the Proposed Data Collection Scheme

Finally, we construct a ZWSN to conduct tests for evaluating the actual performances of the above two data collection schemes. In this experiment, the number of ZEDs is set to be one to eight ($N = 1, \dots, 8$), a ZigBee router is used, and the transmission distance between the ZCR and the ZEDs is set to be 10, 30, and 60 m ($L = 10, 30,$ and 60 m). The testing results are shown in Fig. 9. We can easily observe that the total data collection time is almost unaffected by the communication distance L . The actual data collection times and the associated PEIs of the two data collection schemes are shown in Table 3. The total time to collect data from 8 ZEDs by using the proposed scheme is about 314.2 ms, and the associated PEI is about 1.94. The PEIs approximated using eq. (16) are also shown in Table 3. As shown in the table, the actual PEIs are very close to the PEIs approximated using eq. (16). This means that the data collection time analyses and approximations presented in § 4 can be useful references for evaluating the data collection time in the ZWSN.

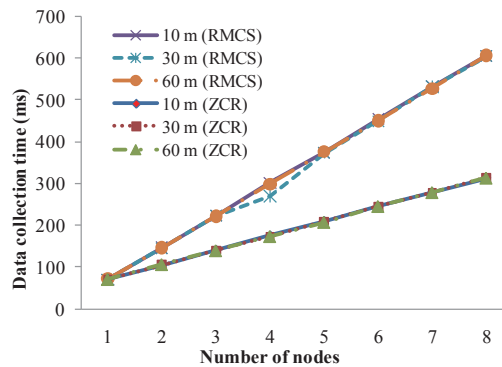


Fig. 9. (Color online) Data collection time comparisons of the two data collection schemes.

Table 3

Actual data collection times and associated PEIs of the two data collection schemes.

N	Time (ms) proposed scheme	Time (ms) traditional scheme	PEI	Approximated PEI
1	69.6	71.0	1.02	1.00
2	104.5	145.9	1.40	1.40
3	140.2	222.5	1.59	1.61
4	174.7	301.2	1.72	1.75
5	209.2	373.6	1.79	1.84
6	244.0	453.2	1.86	1.91
7	278.6	531.6	1.91	1.96
8	312.4	604.5	1.94	2.00

6. Conclusions

In this paper, an empirical approach is adopted to tackle the issues of transmission reliability and data collection efficiency in the tree-topology ZWSN. First, the packet loss phenomenon is investigated by experiments. On the basis of the testing results, we propose a reliable data transmission method to avoid the packet losses between two ZigBee nodes. Furthermore, we present thorough analyses of the time consumption in the data collection process by deriving various time estimation formulations. Accordingly, we propose a new data collection scheme for the ZWSN-based MC system. Finally, we use experimental results to validate the effectiveness of the proposed reliable data transmission method, the efficient data collection scheme, and the various time estimation formulations. In particular, the experimental results illustrate that the total data collection time of our method can be 4.45 times lower than that of the traditional approach if there are eight ZigBee routers and eight ZEDs. The results shown in this paper can be useful references for developing ZWSN-based MC systems.

References

- 1 M. R. Pallikonda, S. Radhakrishnan and P. Subbaraj: *Future Gener. Comput. Syst.* **26** (2010) 569.
- 2 Y. C. Lee, H. Y. Lai and P. J. Lee: *IJETI* **2** (2012) 283.
- 3 J. Han, C. S. Choi and H. Lee: *IEEE TCE* **57** (2011) 85.
- 4 W. T. Sung and Y. C. Hsu: *ESWA* **38** (2011) 4522.
- 5 L. Boquete, R. Cambralla, J. M. Rodríguez-Ascariz, J. M. Miguel-Jiménez, J. J. Cantos-Frontela and J. Dongil: *ISA Trans.* **49** (2010) 270.
- 6 Y. D. Kim, Y. M. Yang, W. S. Kang and D. K. Kim: *Comput. Stand. Interfaces* **36** (2014) 288.
- 7 S. Farahani: *ZigBee Wireless Networks and Transceivers* (Jordan Hill, Oxford, 2008) pp. 3–4.
- 8 ZigBee Alliance: <http://www.ZigBee.org> (accessed March 2014).
- 9 IEEE 802 LAN/MAN Standards Committee: <http://www.ieee802.org> (accessed March 2015).
- 10 C. Buratti: *IEEE TVT* **59** (2010) 2031.
- 11 B. Shrestha, E. Hossain and S. Camorlinga: *Proc. ICCS (IEEE, 2010)* pp. 56–61.
- 12 Y. C. Tseng and M. S. Pan: *Comput. Commun.* **31** (2008) 999.
- 13 P. Park, P. Di Marco, P. Soldati, C. Fischione and K. H. Johansson: *Proc. ICMAS (IEEE, 2009)* pp. 130–139.
- 14 O. Bazan and M. Jaseemuddin: *IET Commun.* **4** (2010) 2252.
- 15 C. Buratti and R. Verdona: *IEEE TVT* **58** (2009) 3480.
- 16 S. C. Ergen, C. Fischione and A. S. Vincentelli: *Proc. IGTC (IEEE, 2008)* pp. 388–393.
- 17 G. Anastasi, M. Conti and M. Di Francesco: *IEEE TII* **7** (2011) 52.
- 18 M. Bertocco, G. Gamba, A. Sona and S. Vitturi: *IEEE TIM* **57** (2008) 1.
- 19 C. Lee, H. S. Lee and S. Choi: *Proc. ICCIT (IEEE, 2010)* pp. 916–919.
- 20 M. López, J. M. Gómez, J. Sabater and A. Herms: *Proc. IEC (IEEE, 2010)* pp. 575–580.