Chen *et al. EURASIP Journal on Wireless Communications and Networking* (2018) 2018:86
https://doi.org/10.1186/s13638-018-1080-y

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

RTGOR: Reliability and Timeliness Guaranteed Opportunistic Routing in wireless sensor networks

Aiguo Chen*†, Xuemei Li, Xueting Ni and Guangchun Luo†

Abstract

Cyber-physical systems (CPSs) connect physical equipment and the information system to realize real-time perception and intelligent control of the equipment. With the rapid development of wireless sensors, wireless sensor networks (WSNs) now play a major role in CPS and have become a focus of research. However, WSNs in CPS face great challenges in ensuring the high reliability and time critical performance of data transmission because of the characteristics of the complex structure and dynamic connectivity. In order to meet the performance requirement of CPS data transmission, a Reliability and Timeliness Guaranteed Opportunistic Routing (RTGOR) protocol is proposed that is based on opportunistic routing and combined with quantified transmission reliability and time guarantees. Our simulation results demonstrate that RTGOR performs better than the state-of-the-art protocol QMOR (QoS-assured Opportunistic Routing Mechanism), in terms of the packet delivery rate and end-to-end delay metrics.

Keywords: Cyber-physical systems, Wireless sensor networks, Opportunistic routing, QoS

1 Introduction

With the rapid technological development of sensors and networks, emerging paradigms such as cyber-physical systems (CPSs) are getting increased attention as a result of their wide application in various areas. CPS systems connect physical sub-systems with computing systems through a variety of hybrid network technologies to realize highly reliable control of distributed physical devices [1, 2]. In many CPS application scenarios, such as environmental monitoring [3], and smart power grid [4], CPS systems perceive the physical environment by a large number of distributed wireless sensors and then perform automatic controls in a timely manner. Obtaining accurate perception data of environment is one of the key challenges in CPS-WSN applications.

At present, the main research in this field could be divided into two parts. One is the scheduling of data, including aggregation and extraction of large scale sensing data [5–8] and time-continuous data generation [9]. These works also minimize the size of the data transmitted by the network and reduce the network and computing overhead. The other research hotspot is data transmission, including broadcast, multicast, and unicast [10, 11]. Typically, sensors communicate through wireless sensor networks (WSNs) so data must be transmitted by multi-hop routing [12]. In such cases, providing good quality of service (QoS) for data transmission is a significant issue, in particular for the QoS guarantee of reliability and timeliness.

Traditional routing protocols for WSNs adopt deterministic routing methods [13]. At the beginning of the data transmission process, an end-to-end node sequence is established, and then each packet is forwarded on this node sequence. If packet loss or error occurs during transmission, a retransmission is initiated by the source. In an environment of poor link quality and poor stability, traditional methods consume a large amount of bandwidth and energy resources. Moreover, the transmission time is greatly prolonged, and reliability is difficult to guarantee.

To improve the performance of data transmission in multi-hop WSNs, opportunistic routing is widely studied [14]. It overcomes the shortcomings of traditional methods through its full broadcast characteristic. Neighbor nodes that receive the data packets broadcasted by source

---

*Correspondence: agchen@uestc.edu.cn
†Equal contributors
School of Computer Science and Engineering, University of Electronic Science and Technology of China, No.2006 Xiyuan Ave, Chengdu 611731, China

node can become the next-hop node, that is, as long as one neighbor node receives the packet, the transmission will not be interrupted. Typically, there is a set of one-hop neighbor nodes that could receive packets. In this set of alternate forwarding nodes, each node will be given priority according to the specific routing metrics—the better the metric, the higher the priority. If the data packet has been successfully delivered by a higher priority node, the lower priority nodes will no longer forward it. Obviously, opportunistic routing protocols greatly improve the reliability of wireless network transmission. Moreover, by adjusting the priority rules, a different quality of service can be provided. For example, the load balancing of each node or link can be achieved by determining the priority according to the load. So, bandwidth constraints and energy consumption performances could also be considered by the protocol. But in CPS systems, both reliability and timeliness are the key factors in data transmission. Existing routing protocols lack the ability to formally guarantee quantitative properties of reliability and timeliness at the same time.

For the purpose of solving the problem mentioned above, a reliability and timeliness guaranteed opportunistic routing (RTGOR) is proposed. RTGOR considers the transmission time and the link delay as the QoS parameters to improve the transmission performance. Both reliability and timeliness requirements could be provided quantitatively for mission-critical applications in the RTGOR algorithm, and the complexity has not been increased. Our major contributions are listed as follows:

1. The expected transmission delay (ETD) based on the bidirectional transmission success rate is defined as the routing metric, and the lower delay node is selected as the next hop of transmission to provide the best delay guarantee.
2. Two-level lists selection method is defined. On the premise of ensuring reliability and timeliness, the scale of the forwarder list is minimized, the network load is reduced, and the communication ability of the network is improved.
3. A complete design and implementation of RTGOR on the Opportunistic Network Environment (ONE) simulator platform. Through performance comparisons, we demonstrate a substantial reliability and timeliness improvement of RTGOR under different scales of network nodes.

The remainder of this paper is organized as follows: Section 2 discusses the related work. Section 3 presents the reliability and timeliness guaranteed opportunistic routing algorithm. Section 4 describes the experiments and performance comparison. Section 5 concludes this paper with future work proposals.

2 Related work

Opportunistic routing protocols with QoS guarantees are hotspots in the field of WSNs, and a series of protocols has been proposed. To meet the demands of various scenarios and applications, different opportunistic routing protocols provide different QoS guarantees, including energy consumption, reliability, delay, and throughput.

The limited battery supply of a sensor node is one of the most important factors that limit the lifetime of the WSNs. As a consequence, increasing the lifetime of WSNs through energy-efficient mechanisms has become a challenging research area. So, energy consumption and end-to-end delay have long been the focus of QoS-awared opportunistic routing concerns [15]. For example, the work in [16] targeted the applications with low duty cycles and tried to reduce delay and energy consumption. In [17], with a given transmission rate requirement between source node and destination node, an adaptive power control scheme was implemented in relay nodes to minimize total average energy consumption. Yang et al. [18] proposed an energy-aware opportunistic routing protocol EARTOR with QoS constraints, which schedules the power level at each relay node for message relay to meet its end-to-end latency constraint, thereby achieving better energy efficiency. In the aspect of reducing network latency, some real-time routing protocols have been proposed [19, 20]; all these works realized soft QoS provisioning, without quantitative timeliness guarantee.

Moreover, for mission-critical CPS applications, both the end-to-end delay constraint and certain packet delivery reliability are expected to be guaranteed in an efficient way. Alwan et al. [21] proposed a cross-layer quality of service-aware scheduling to handle heterogeneous traffic with respect to delay and reliability in an energy-efficient way. The works in [15, 22] exploited the geographic opportunistic routing (GOR) for QoS provisioning in WSNs to guarantee both reliability and delay QoS constraints. Shen et al. [23] presented a QoS-aware multi-sink opportunistic routing (QMOR) to efficiently deliver multimedia information under QoS constraints. In QMOR, the multi-sink-aware operations are integrated into an optimization opportunistic routing framework, w ith the objective to minimize energy consumption subject to both delay and reliability constraints. However, the routings in these works just meet the timely requirement with probability; it is not possible to guarantee a quantifiable level of service.

In the later works [15, 21–23], energy consumption has not been paid special attention, because there are many application scenarios in which the quality of data transmission is more considered. In our work, we also aim to improve transmission reliability and reduce end-to-end delay.

3 Reliability and timeliness guaranteed opportunistic routing

3.1 General framework

In this section, we explain the RTGOR protocol in detail. The overall processing flow of RTGOR is shown in Fig. 1.

First, we define the reliability requirement and timeliness requirement from the business view. Thus, these two metrics come from the business layer's needs and are the requirement for the whole transmission process. Each step of the transmission process is scheduled to meet these metrics. The following are the definitions in detail:

- The global reliability requirement GR means that the statistical delivery rate should be greater than this quantitative requirement with respect to the delivery of packets to the intended recipient.
- The global timeliness requirement GD is expressed with the global maximum allowable delay. And during the transmission process, the remaining maximum allowable delay is constantly updated on each relay node according to GD and elapsed time.

When a sending node attempts to forward a packet, a timeliness guaranteed candidate list should be selected out based on the timeliness requirement. If a one-hop node does not meet the timeliness requirement, it will be discarded. Then, for the purpose of satisfying the reliability metric, a QoS guaranteed forwarder list is selected from the timeliness guaranteed candidate list. At the same time, the forwarding strategy of each node in the guaranteed forwarder list is also calculated according to both the timeliness and reliability requirements. Finally, the sending node sends packets to the forwarder in broadcast mode. The nodes in the forwarder list cooperate to determine the relay node, and the data is forwarded by the relay node.

3.2 Network model and metrics

The key to QoS-aware opportunistic routing is the method of selecting and prioritizing the forwarding candidate set in an efficient manner. This begins with the measurements of network and link using parameters such as actual delay and reception ratio. The classic network metric ETX (Expected Transmission Count) [24] calculates the expected number of data transmissions, including retransmissions. According to ETX, routing protocols meet the delivery rate through the retransmission approach. However, in order to ensure the timeliness requirement, retransmission until success is not efficient. Therefore, the delivery reliability and timeliness metric approaches are proposed to offer a quantitative QoS guarantee.

3.2.1 Expected delivery reliability

Delivery reliability is evaluated by the delivery rate of the packet, which refers to the ratio of the number of delivered packets and the number of packets sent per statistical cycle. This metric reflects the ability of the routing algorithm to deliver packets successfully, and it is the most important metric to mission-critical CPS applications.

Let the packet delivery rate of ith link on the routing path be P_i. To calculate end-to-end reliability, we define the expected delivery rate of a routing path as ETR, which is estimated as Eq. 1.

$$\mathrm{ETR} = 1 - \prod_{i=1}^{n} \bar{P}_i \tag{1}$$

where n is the total number of links. Because routers use hop-by-hop forwarding, the longer path of the nodes makes it more difficult to guarantee the whole reliability.

3.2.2 Transmission timeliness

In the mission-critical CPS application scenes, control of physical devices is more time sensitive and has a strict requirement for transmission timeliness. We use the delay constraint to indicate the correspondence transmission timeliness metric, which means the maximum allowable transmission delay of a data packet from source to destination. For quantitative evaluation, a new routing metric ETD (expected transmission delay) is defined in the process of data packet forwarding, which is calculated based on the bidirectional delivery rate and the transmission delay. The relevant definition and calculation method are as follows:

(1) The expected transmission delay of a path between the source node and destination node is the sum of delay that incurs over all links of this path.

Fig. 1 The overall processing flow

$$\mathrm{ETD} = \sum\nolimits_{i=1}^{n} \mathrm{ETD}_i \tag{2}$$

where ETD_i is the ith link's expected transmission delay, and n is the total number of links. In this routing mechanism, if the relay node fails to forward the packet at one time, it directly initiates a retransmission instead of restarting from the source node. So, ETD could be evaluated by means of summation.

(2) The time consumption on the ith link ETD_i $(0 \le i \le n)$ is defined as the total delay in the successful delivery of a packet over this link.

$$\mathrm{ETD}_i = (M_i + 1)E[T_i] \tag{3}$$

where M_i is the number of packets before the current packet in the queue on the sending node of this link. Let $E[T_i]$ be the time consumption of a successful packet transmission over the ith link. We only consider the transmission to the one-hop neighbors here. This is the product of the expected transmission count and the once ideal transmission time.

$$E[T_i] = d_{\mathrm{p}i}^{-1} T_i \tag{4}$$

$$d_{\mathrm{p}} = d_{\mathrm{f}} \times d_{\mathrm{r}} \tag{5}$$

where d_{p} is the bidirectional delivery rate of the current link. d_{f} is the forward delivery rate. d_{r} is the reverse.

(3) The total delay of one data packet transmission T_i is defined as the sum of required processing latency and transmission delay.

$$\begin{aligned} \mathrm{T} \;=\; T_{\mathrm{proc}} + T_{\mathrm{trans}} &= (\mathrm{DIFS} + T_{\mathrm{backoff}} + \mathrm{SIFS}) \\ &+ \frac{L_{\mathrm{PKT}}}{B} + T_{\mathrm{ACK}} \end{aligned} \tag{6}$$

where DIFS is a distributed inter-frame space. The sending node needs to wait for a DIFS to determine whether this transmission channel is occupied. T_{backoff} is the random backoff time for the sending node to acquire the channel. If the length of the packet is L_{PKT} and available bandwith is B, the transmission time should be L_{PKT}/B. SIFS is the amount of time spent by the receiver to process a received packet and to respond with an acknowledgement message. T_{ACK} is the transmission time for sending the ACK message. According to the formulas above, the expected transmission delay of each node to the destination is estimated as

$$\begin{aligned} \mathrm{ETD}_i &= (M_i + 1)E[T_i] \\ &= (M_i + 1){d_{\mathrm{p_i}}}^{-1} \cdot \Big[(\mathrm{DIFS} + T_{\mathrm{backoff}}) \\ &+ \frac{L}{B} + j \cdot (\mathrm{SIFS} + T_{\mathrm{ACK}}) \Big] \end{aligned} \tag{7}$$

3.3 The timeliness guaranteed candidate list selection

In Section 3.1, the global timeliness requirement GD is defined, which is the time constraint for the complete delivery process. For example, for packet PKT, its global timeliness requirement is $\mathrm{GD}^{\mathrm{PKT}}$. At each intermediate node, we should dynamically update the remaining allowable delay $\mathrm{RAD}^{\mathrm{PKT}}$. Then, the timeliness guaranteed candidate list for PKT could be selected according to $\mathrm{RAD}^{\mathrm{PKT}}$.

First, when node N_{S} receives (or generates) a packet PKT, which needs to be forwarded to the destination, it probes to obtain the status of all one-hop neighbor nodes. Then, an initial timeliness guaranteed candidate list $\mathrm{CL}^{'} = \{N_1, N_2, \ldots, N_n\}$ is formed and sorted according to their corresponding routing paths' ETD from small to large, where n is the number of next-hop nodes, and the path is the best path from one-hop neighbor node N_i to the destination. In each node's expected transmission delay, ETD is equal to or less than $\mathrm{RAD}^{\mathrm{PKT}}$.

Then, let T_i and $E[T_i]$ be the ideal one-time transmission time and the expected successful transmission time over the link from the source node to a one-hop neighbor node N_i, respectively. We also could calculate the remaining allowable delay of this link RAD_i. According to their multiple relationships, the allowed retransmission times ART_i of each next-hop node in $\mathrm{CL}^{'}$ could be calculated. Then, the formal timeliness guaranteed candidate list is obtained, including the allowed retransmission times of each node.

$$\mathrm{RAD}_i = \mathrm{ETD}_i * \mathrm{ART}_i \tag{8}$$

$$\mathrm{CL} = \{(N_1, \mathrm{ART}_1), (N_2, \mathrm{ART}_2), \ldots, (N_{\mathrm{n}}, \mathrm{ART}_{\mathrm{n}})\} \tag{9}$$

CL routing metric calculation, taking into account queue delay, transmission delay, and fine-grained partition transmission time, is to join the data scheduling mechanism in each node under the premise of time consumption and transmission time considerations. It is the key to ensuring the quantification of time constraints.

3.4 The QoS guaranteed forwarder list selection

The most important issue in the design of opportunistic routing protocols is the forwarder list selection problem. In RTGOR, a dynamic calculation algorithm of QoS guaranteed forwarder list selection is proposed. The forwarder list will be selected from the timeliness guaranteed candidate list CL according to the global reliability requirement GR and the delivery reliability of each node's corresponding path. First, calculate the expected forwarding reliability MPST_i of a one-hop neighbor node in the timeliness guaranteed candidate list CL. This can be expressed as follows:

$$\mathrm{MPST}_i = 1 - \left(1 - d_{\mathrm{p}}\right)_i^{\mathrm{ART}}, i \in (1, n) \tag{10}$$

After obtaining the $\mathrm{MPST_i}$ of each neighbor node in CL, we select the minimum nodes $n_{\min}$ from CL to meet both the timeliness and reliability requirements. Select $n_{\min}$ nodes from priority highest to lowest as the candidate nodes for the current sending node. The application of the policy in the routing process is as follows: set a forwarder list FL and initialize to empty. From the candidate node priority list CL, select a node to join FL in the order of each priority until the transmission reliability of the node in FL satisfies the condition. The basic element of FL is two-tuple (N_i, ART_i). Let the length of the list FL be L_{FL}, and then there are:

(1) When $L_{\mathrm{FL}} = 0$, no forwardable node, transmission is end;
(2) When $L_{\mathrm{FL}} = 1$, the node with the priority q_1 (highest) is selected to join FL;
(3) When $L = 2$, select the two nodes with priority q_1 and q_2 into FL, and the node forwarding reliability is $\mathrm{PST} = 1 - (1 - \mathrm{MSPT}_1) * (1 - \mathrm{MSPT}_2)$; calculate the result of $\mathrm{PST} \geq \mathrm{GR}$; if it is true, the candidate node set is $\{N_1, N_2\}$; if false, $L_{\mathrm{FL}} = L_{\mathrm{FL}} + 1$;
(4) Repeat the above steps until the $\mathrm{PST} \geq \mathrm{GR}$; then, the relay forwarding node set length is L_{FL}.

3.5 The relay forwarding node selection

Then, the source node broadcasts the packets to all nodes in the forwarder list, or repeat multiple times. The highest priority node in the current valid list will send an ACK packet to the source node and other candidate forwarding nodes after it receives the packets. The other candidate nodes that received the ACK no longer forward this packet and discard it. If the ACK is not received, the candidate node of the secondary priority forwards this packet and sends an ACK to the source node and other alternate nodes. Repeat this process until the packet is forwarded successfully. The specific process is as follows:

(1) After determining the number of forwarder nodes L_{FL}, the sending node N_S sends current packet M to the set of forwarder nodes that have been determined.
(2) The node that successfully receives a packet in FL first looks at its priority in the candidate forwarding priority list. If it is not in the list, the node does not participate in the relay node selection. If it is in the list, the node caches the received packet and sets the waiting time for the packet to be forwarded. $\mathrm{wait\_time} = P \cdot \theta + t$, where P is the priority of candidate node, θ is the basic waiting time, and t is the random backoff time corresponding to one priority.
(3) The node with the highest priority forwards the packets in the cache and sends ACK to the source node and the remaining candidate nodes after successful receipt of the packet. The remaining candidate nodes receive the ACK returned by the node within the waiting time wait_time and then discard the data packet that has been received in the cache. If the ACK returned by the high-priority node is not received, the forwarding process of the high-priority node is repeated by the secondary priority node to forward the packet.
(4) If all the nodes in the current round did not receive the packet successfully, then all elements (N_i, ART_i) in FL reduce ART_i to 1. If the final result turns to 0, we will move this node out of FL. Then, repeat the above steps.

The above relay node selection method can compensate for the shortcomings of priority forwarding and avoid the low-priority nodes to repeatedly transmit or hastily drop packets because they can not obtain the forwarding state of high-priority nodes. This method increased the reliability of transmission.

4 Experiment evaluation and result analysis

To validate the performance of our algorithm, we compare the simulation with QMOR (QoS-assured opportunistic routing mechanism) [23] in the ONE (Opportunistic Network Environment) network simulator [25]. We compare the delivery success rate and transmission delay performance under five different network scale conditions. To reduce the impact of accidental errors on the experimental results, we run the simulation results at least 50 times.

4.1 Simulation settings

In the implementation of our simulation, sensor nodes are placed in a rectangular area of 4500 × 3000 m, and six groups of nodes are distributed in the region. We tested five network scenarios, with the total number of nodes set to 60, 80, 120, 160, and 200. The mobile model of the node is SPMBM (Shortest Path Map-Based Movement). The moving speed of nodes is 0.5 1.5 m/s. The max transmission distance of neighbor nodes is 200 m, and the life cycle of the message is 300 min. To ensure the global reliability of the network, each node's transport layer is implemented based on the TCP protocol; the network layer is the RTGOR protocol; the data link layer is the classic IEEE802.11n as the underlying transport protocol; and the transmission bandwidth is 300 Mbps. An end-to-end transmission delay threshold of 400 s and a reliability threshold of 0.8 is given. The reliability and delay performance statistical data are output to log file MessageDeliveryReport.

4.2 The packet delivery rate

The packet delivery rate is the ratio of the total number of packets arriving at the target node to the total number of

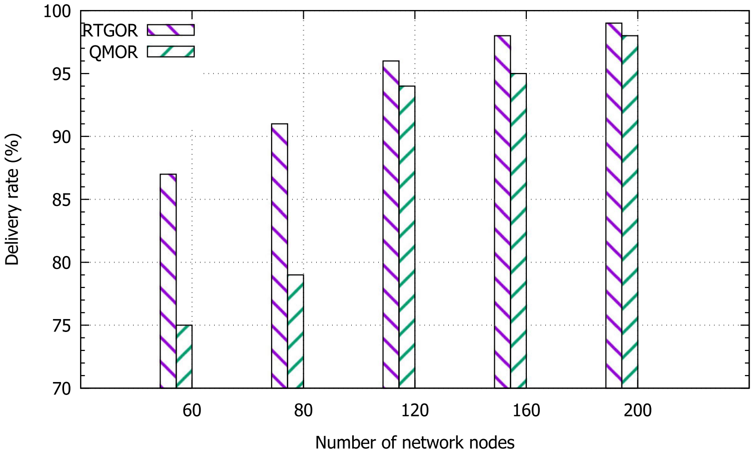

Fig. 2 Message delivery rate comparison

packets sent by the source node over a certain period of time. This metric characterizes the ability of the routing algorithm to forward packets correctly to the target node, namely, reliability.

Figure 2 shows the packet delivery rate under different background traffic scenarios, where the amount of nodes is set from 60 to 200.

RTGOR can always meet the reliability requirement ($> 80\%$) all the time. QMOR can only meet the reliability when the amounts of nodes are 120, 160, and 200. Moreover, in all scenarios, the delivery rate of RTGOR is higher than QMOR. In particular, in the case of sparse nodes, the performance of QMOR degrades very seriously. What needs special mention is that the delivery rate calculation of QMOR including the distribution exceeds the delay constraint. QMOR cannot quantify the delay characteristics, and the delay cannot be effectively controlled when the nodes are sparse.

4.3 The packet delivery delay

We compare packet delay characteristics in two aspects, the average packet delay and the delay distribution. The average packet delay is the average value of the transmission time of all packets from source node to destination node during the entire simulation period. And the delay distribution shows the number of packets that are accumulated at different latency times. Figure 3 shows the average packet delay under different traffic scenarios for both RTGOR and QMOR. This metric of RTGOR is always lower than QMOR; it always meets the demand of delay (< 400 s). When the node amount is reduced to 80 or 60, the delivery delay of most packets cannot meet the requirement for QMOR, and the average delay is 460.78 and 507.11 s, respectively. The average delay of RTGOR is 120.88 and 218.59 s, respectively, in the corresponding scenes. Lower average packet delay means that the routing algorithm has higher transmission efficiency but also that

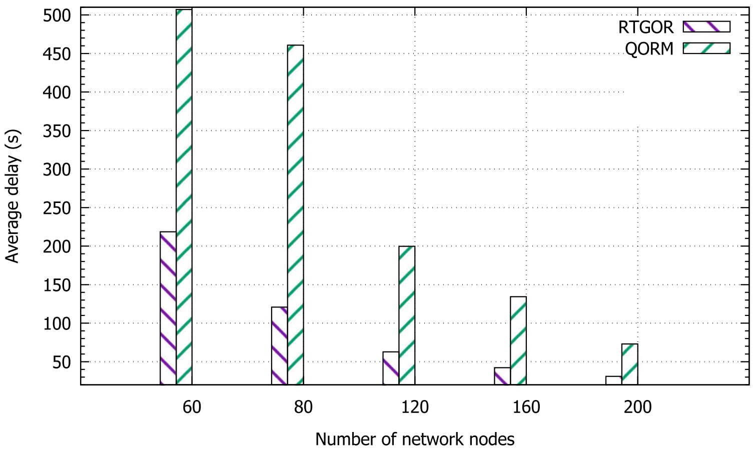

Fig. 3 Average packet delay comparison

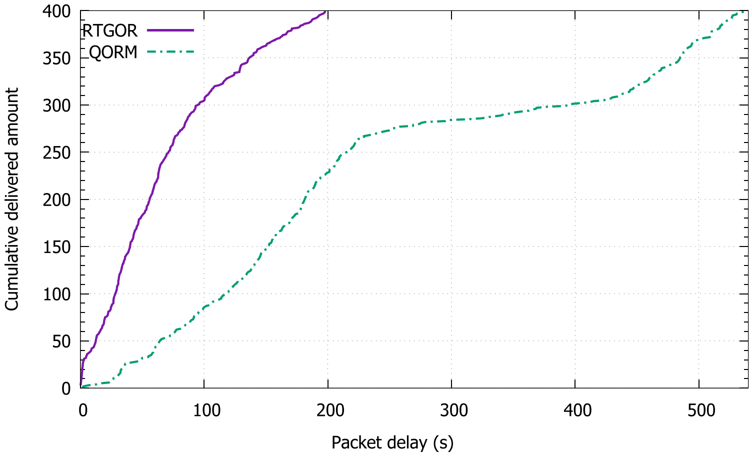

Fig. 4 Package delay distribution comparison

the packet transmission process will take up less network resources.

Figure 4 shows the other end-to-end delay performance, namely, the package delay distribution comparison. The Y coordinates of the points on the curve are the amount of packets that are successfully delivered in less than X-axis time. In each node size scene, the simulation transmitted 100 packets and finally counted the delay distribution of the first 400 packets.

From both Figs. 3 and 4, we can find that RTGOR obtains better delay performance at the same simulation scenario. And the above two groups of experimental results finally show that the RTGOR in the packet delivery rate and transmission delay show better performance.

In addition, RTGOR adopts a similar link and node state acquisition mode with QMOR, and it can select the optimal opportunistic routing with low overhead cost. The computational cost of RTGOR is slightly larger than QMOR, that is, because RTGOR uses a two-level lists selection mechanism in order to ensure transmission reliability and end-to-end delay. RTGOR aims to provide the quantitative guarantee of reliability and timeliness. Therefore, we think that the cost of a little calculation in exchange for a higher delivery rate and lower delay is reasonable.

5 Conclusions

In this paper, we put forward a Reliability and Timeliness Guaranteed Opportunistic Routing (RTGOR) protocol, which is realized based on opportunistic routing and combined with quantified transmission reliability and time guarantees. The algorithm is aimed at the high demand for timeliness and reliability of data transmission in CPS applications. Two QoS metrics of delay and reliability are employed. The reliability metric is set as the threshold value to select candidate nodes and then uses the delay as the other route metric to sort the neighbor nodes and calculate the number of retransmissions according to the delivery rate and delay of relay node; then, the relay nodes and forward polices could be determined. Experiments show that the algorithm is superior in performance with respect to the delay and reliability metric and can meet the needs of the CPS network.

The opportunity routing protocol proposed in this paper reduces the wastage of network resources brought by data broadcasting but also increases the computational cost of nodes. In CPS network routing, this requires not only the computational power of the nodes but also the energy provided by the nodes. Thus, avoiding the possibility of excessive computing overhead routing will be a topic of future work. In addition, the security of code distribution in WSNs is also a hot top [26], and our future protocol studies will consider the relevant issues.

Acknowledgements

This work is supported by the Science and Technology Supporting Project of Sichuan Provincial Science and Technology Department (Grant no. 2016GZ0075, 2016GZ0077) and the International Science and Technology Cooperation Project of Sichuan Provincial Science and Technology Department (Grant no. 2017HH0075).

Authors' contributions

AC, XL, and GL designed the algorithm and conceived the experiments. XN performed the experiments. AC analyzed the data and wrote this paper. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 31 October 2017 Accepted: 20 January 2018

References

1. R Rajkumar, I Lee, L Sha, J Stankovic, in *Proceedings of the 47th Design Automation Conference*. Cyber-physical systems: the next computing revolution (Design Automation Conference. IEEE, 2010), pp. 731–736. https://doi.org/10.1145/1837274.1837461
2. T Alhmiedat, *Wireless sensor networks toward cyber-physical systems. Cyber-Physical Systems: A Computational Perspective*, 1st edn. (Taylor & Francis Group, LLC, 2016), pp. 106–121
3. G Mois, T Sanislav, SC Folea, A cyber-physical system for environmental monitoring. IEEE Trans. Instrum. Meas. **65**(6), 1463–1471 (2016)
4. MA Shuang, XU Zhen, L Wang, Set theory based modeling method of cyber physical system for power grid. Autom. Electr. Power Syst. **41**(6), 1–5 (2017)
5. J Li, S Cheng, Y Li, Z Cai, Approximate holistic aggregation in wireless sensor networks. ACM Trans. Sens. Netw. **13**(2), 740–741 (2017)
6. S Cheng, Z Cai, J Li, H Gao, Extracting kernel dataset from big sensory data in wireless sensor networks. IEEE Trans. Knowl. Data Eng. **29**(4), 813–827 (2017)
7. S Cheng, Z Cai, J Li, X Fang, in *Computer Communications*. Drawing dominant dataset from big sensory data in wireless sensor networks, vol. 1, (2015), pp. 531–539
8. Z He, Z Cai, S Cheng, X Wang, Approximate aggregation for tracking quantiles and range countings in wireless sensor networks. Theor. Comput. Sci. **607**(P3), 381–390 (2015)
9. S Cheng, Z Cai, J Li, Curve query processing in wireless sensor networks. IEEE Trans. Veh. Technol. **64**(11), 5198–5209 (2015)
10. Z Cai, R Goebel, G Lin, *Size-constrained tree partitioning: approximating the multicast k-tree routing problem*, vol. 412, (2011), pp. 240–245
11. Z Cai, ZZ Chen, G Lin, A 3.4713-approximation algorithm for the capacitated multicast tree routing problem. Theor. Comput. Sci. **410**(52), 5415–5424 (2009)
12. FJ Wu, YF Kao, YC Tseng, From wireless sensor networks towards cyber physical systems. Pervasive Mob. Comput. **7**(4), 397–413 (2011)
13. C Intanagonwiwat, R Govindan, D Estrin, J Heidemann, F Silva, Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Netw. **11**(1), 2–16 (2003)
14. N Chakchouk, A survey on opportunistic routing in wireless communication networks. IEEE Commun. Surv. Tutor. **17**(4), 2214–2241 (2015)
15. JH Patel, BB Godbole, Intelligent opportunistic routing in wireless sensor network. Int. Res. J. Eng. Technol (IRJET). **2**(8), 344–348 (2015)
16. O Landsiedel, E Ghadimi, S Duquennoy, M Johansson, in *The 11th International Conference on Information Processing in Sensor Networks (IPSN'12)*. Low power, low delay: opportunistic routing meets duty cycling, (2012), pp. 185–196. https://doi.org/10.1145/2185677.2185731
17. CY Lee, GU Hwang, in *Wireless Telecommunications Symposium (WTS)*. Minimum energy consumption design of a two-hop relay for QOS guarantee, (2010), pp. 1–6. https://doi.org/10.1109/WTS.2010.5479670
18. W Yang, W Liang, W Dou, in *Global Communications Conference (GLOBECOM2010)*. Energy-aware real-time opportunistic routing for wireless ad hoc networks, (2010), pp. 1–6. https://doi.org/10.1109/GLOCOM.2010.5683491
19. AAA Abdullah, An enhanced real-time routing protocol with load distribution for mobile wireless sensor networks. Comput. Netw. **57**(6), 1459–1473 (2013)
20. M Chovanec, P Šarafín, in *Computer Science and Information Systems*. Real-time schedule for mobile robotics and WSN aplications, (2015), pp. 1199–1202
21. H Alwan, A Agarwal, in *International Conference on Computer Systems and Applications (AICCSA)*. A cross-layer-based routing with QoS-aware scheduling for wireless sensor networks, (2013), pp. 1–8. https://doi.org/10.1109/AICCSA.2013.6616449
22. L Cheng, J Niu, J Cao, SK Das, Y Gu, QoS aware geographic opportunistic routing in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **25**(7), 1864–1875 (2014)
23. H Shen, G Bai, Z Tang, L Zhao, Qmor: QoS-aware multi-sink opportunistic routing for wireless multimedia sensor networks. Wirel. Pers. Commun. **75**(2), 1307–1330 (2014)
24. N Javaid, A Javaid, IA Khan, K Djouani, in *the 2nd International Conference on, Computer, Control and Communication (IC4)*. Performance study of ETX based wireless routing metrics, (2010), pp. 1–7. https://doi.org/10.1109/IC4.2009.4909163
25. A Keränen, J Ott, T Kärkkäinen, in *Proceedings of the Second International ICST Conference on Simulation Tools and Techniques*. The ONE simulator for DTN protocol evaluation, (2009), pp. 1–7. https://doi.org/10.4108/ICST.SIMUTOOLS2009.5674
26. M Xie, U Bhanja, J Shao, G Zhang, G Wei. LDSCD: A loss and DoS resistant secure code dissemination algorithm supporting multiple authorized tenants, vol. 420, (2017), pp. 37–48