INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS
Received: 03-03-2023
Accepted: 13-04-2023
Published: 26-05-2023

Citation: Devipriya K, Hemalatha R (2023) Improving Quality of Service using Multipath Routing Protocol for Delay Sensitive Applications of Internet of Things in Wireless Sensor Networks. Indian Journal of Science and Technology 16(21): 1538-1545. https://doi.org/10.17485/IJST/v16i21.441

* **Corresponding author**.
devipriyacs@tkcfw.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Improving Quality of Service using Multipath Routing Protocol for Delay Sensitive Applications of Internet of Things in Wireless Sensor Networks

K Devipriya[1]*, R Hemalatha[2]

1 Research Scholar, PG & Research Department of Computer Science, Tiruppur Kumaran College for Women, Tamil Nadu, India
2 Head & Associate Professor, PG & Research Department of Computer Science, Tiruppur Kumaran College for Women, Tamil Nadu, India

Abstract

Objectives: To increase the data transmission between the nodes and decrease the latency in data transmission between the nodes than the traditional routing methods. **Methods:** A novel methodology is being proposed to increase the success rate of real-time transmission by competitively utilizing high-quality links included in different paths in real-time multi-path routing. That is, if a packet that arrives first in one path is copied and delivered to another path immediately, each path competitively delivers the packet in real-time, which has the effect of delivering the packet through a virtual real-time optimal path composed only of high-quality links can be obtained through this, the proposed method can provide a higher success rate for real-time transmission than the existing methods in an environment where link quality is variable. To achieve this goal, the proposed method consists of 1) multi-path configuration method, 2) bridge node selection method, and 3) contention real-time transmission method. **Findings**: Performance evaluation is performed by comparing and analyzing the experimental results of Equal-Cost Multi-Path Routing (ECMP) and PMMR (Partitioning Multi-constrained Multipath Routing) among the existing multi-path methods and various conditions of the proposed method. The proposed method obtains three results according to the latency (0, 0.05, and 0.1) of the bridge node, and independent multi-path transmission allows each path to follow a single-path routing method. **Novelty :** The performance of data transmission between nodes is increased and reduced the latency time by the Proposed Contention Transmission Routing Algorithm (PCTRA) when compared to ECMP and PMMR.

Keywords: Wireless Sensor Networks; Internet of Things; Multipath Routing Protocol; Real Time Routing; High Speed Data Transmission

1 Introduction

A wireless sensor network is a network composed of a large number of small sensor nodes with sensing and communication functions. Wireless sensor networks applied to different application fields generate and collect data in various ways depending on the purpose of the application [1]. That is, in the wireless sensor network, the routing performance measured must be treated as important but it may be different depending on the type of information One of the main studies to improve this performance is real-time routing and another performance metric is the reliability of data delivery [2]. One of the major studies for this is called multipath routing.

However, [3] sensor nodes with limited processing power, energy and variable characteristics of the wireless transmission/reception environment make it very difficult to acquire such network status information in real time. In other words, [4] it is difficult to guarantee the reliability and accuracy of the collected information in a constantly changing wireless environment as well as extreme energy consumption to collect all state information of a network composed of numerous sensor nodes.

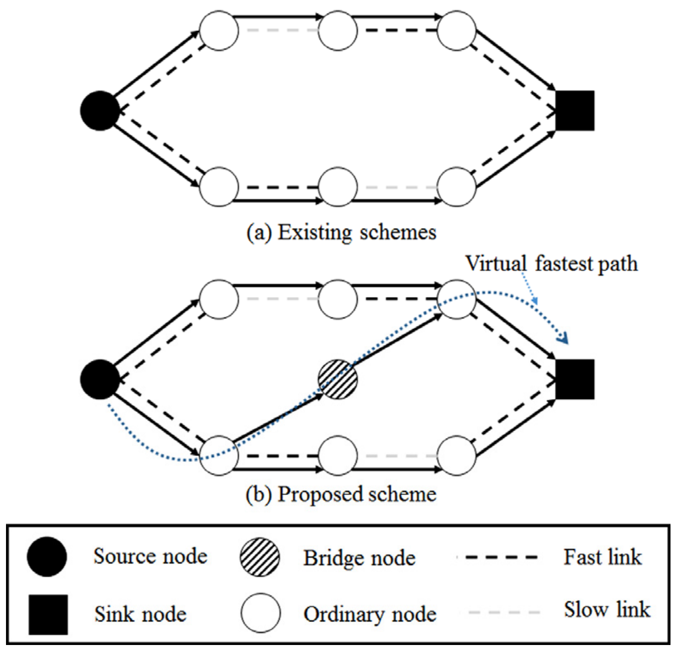

Fig 1. (a) Existing Routing Scheme, (b) Proposed Multipath Routing Scheme

Figure 1 (a) shows an example, the actual latency of each path can vary continuously due to the dynamic radio environment. In this paper, contention multiplicity is used to increase the probability of real-time data transmission in a wireless sensor network in a dynamic environment by utilizing broadcasting and over-hearing, one of the great features of wireless sensor networks. We propose a routing protocol, in that the proposed method selects a bridge node between two adjacent paths. The bridge node overhears the data transmission of two adjacent paths, stores the data that arrives first among the two paths, and transfers it to the other path if necessary. The forwarding node [5] that has received the data from the bridge node immediately resumes data transmission through the path it belongs to, and then ignores duplicate data transmitted from the previous forwarding node on the path. As a result, the contention data transmission algorithm of these bridge nodes makes it possible to obtain the effect of constructing a virtual optimal real-time path composed only of sections with a short delay time. Figure 1 (b) conceptually shows a virtual multipath constructed through a bridge node. Even if the link quality of each path changes due to the dynamic wireless environment, the proposed method can be adapted to and maintain the optimal virtual path composed of excellent links among multipath. Subsequent performance evaluation shows that the proposed method can increase the probability of satisfying real-time performance even when the real-time requirements are stricter or the network variability is high [6,7].

1.1 Background Study

Previous studies[1–3] , propose a two-factor authentication protocol for wireless sensor networks based on elliptic curve encryption, which realizes user, sensor and mutual network authentication among the gateways. The two-factor authentication scheme for wireless sensor networks proposed by Vaidya et al.[8] only uses a simple hash function and XOR function for encryption. In[9,10], proposed a smart card-based wireless sensor network authentication protocol, which realized the user and sensor authentication of nodes. In[5], proposes two-factor authentication protocols for wireless sensor networks applied in smart medical care, which couldguarantee the doctors to get reliable user data from the sensors.

Zhang[6] proposed a secure and efficient remote authentication protocol for wireless sensor networks. Compared with biometric features, Bio hash has obvious functional advantages and can greatly improve the accuracy of biometric identification. Chen et al.[7] proposed a lightweight verifiable group authentication scheme for the internet of things. Multi-factor-based authentication can provide high security. In this scheme, after the authentication is successful, the user can directly connect to the desired sensor node for communication. Das et al.[11] proposed a three-factor user authentication protocol for wireless sensor networks, the protocol uses a hash function and symmetric key encryption. Fang et al.[12] found a two-factor user authentication protocol for layered wireless sensor networks and proposed an improved authentication protocol. Guo et al.[13] proposed a review on privacy protection of medical and health big data, which utilizes hybrid cryptography, including symmetric encryption and certificate-less public key encryption algorithms. Nodes with limited resources are only included in the lightweight symmetric encryption algorithm, and their other devices perform certificate less public key encryption. This protocol is suitable for the interaction between remote users and resource-constrained sensor nodes in smart medical certification.

2 Methodology

The existing real-time data transmission methods in the wireless sensor network have made an effort (soft real-time) to increase the success probability of real-time data transmission through a probabilistic or heuristic approach. They transmit real-time data by selecting a path that satisfies the required peer to peer delay time from among several data transmission path candidates through path search. However,[9] as mentioned, if the corresponding route no longer satisfies the required delay time due to a change in the network state, another route must be searched again. Real-time multipath routing transmits data through multiple paths at the same time, and if any one of them succeeds in data transmission within the required delay time, real-time transmission succeeds[10]. Therefore, it is possible to increase the success probability of real-time data transmission compared to the method using a single path, which is an effective method in a wireless sensor network where it is very difficult to maintain a path that guarantees the required delay time. However, the existing real-time multi-path routing method has a limitation in that each path is used independently. In other words,[5] even if a path that can satisfy the currently required delay time exists in the network, real-time data transmission may fail if all links of the corresponding path do not satisfy it.

The purpose of the proposed method is to increase the success rate of real-time transmission by competitively utilizing high-quality links included in different paths in real-time multi-path routing. That is, if a packet that arrives first in one path is copied and delivered to another path immediately, each path competitively delivers the packet in real time, which has the effect of delivering the packet through a virtual real-time optimal path composed only of high-quality links can be obtained through this, the proposed method can provide a higher success rate for real-time transmission than the existing methods in an environment where link quality is variable.

To achieve this goal, the proposed method consists of 1) multi-path configuration method, 2) bridge node selection method, and 3) contention real-time transmission method. Each item will be described in detail in this chapter.

2.1 Multipath Configuration

Multipath routing transmits packets simultaneously through multiple paths, and since the source and sink are the same in packet delivery of each path, each path tends to be configured in a similar form. Therefore, collisions and congestion may occur due to interference between the paths. In the case of real-time transmission, such collisions and congestion can be fatal flaws due to packet delivery failures and delays for retransmission. Even if the link quality of each path changes due to the dynamic wireless environment, the proposed method can adapt immediately and maintain the optimal virtual path composed of excellent links among multipath.

2.2 Bridge Node Selection

The bridge node plays a role in restoring data transmission or supporting fast data transmission by utilizing the multi-path structure. To this end, it monitors neighboring paths and plays a role of relaying packets for contention communication between the paths. For smooth packet relay, the node with the best link quality with the forwarding nodes of each path should be selected as the bridge node.

The detailed explanation of the bridge node selection process is as follows. The bridge node selects the most efficient recovery transmission node among the candidate nodes located between the two paths. For this, a bridge node between the neighboring paths is first selected from among the multi-paths. And when the number of multipath is three or more, a bridge node is selected from the newly created additional paths. For example, if there are 3 paths, number 2 located in the middle in 1-2-3 selects both bridging nodes, and if the number of paths is 4, then 2 and 4, if there are 5, 2, Steps 4 and 5 select bridging nodes. The order of selection of bridging nodes is that among the forwarding nodes in the path that selects bridged nodes, the forwarding node immediately adjacent to the sink first selects its own bridged node, and all forwarding nodes on the same path located in the source direction are not selected. It sequentially selects its own bridging nodes from the non-candidate bridging nodes.

2.3 Contention Real-Time Delivery

As mentioned above, contention real-time transmission is achieved by transferring data packets received from one path to the other path by a bridge node that monitors two adjacent paths. Figure 2 shows the packet forwarding process of the bridge node. In Figure 2, Pi denotes the i^{th} path, PMi_j denotes the j^{th} member node of Pi, and the source is PS0 for all paths Pi.

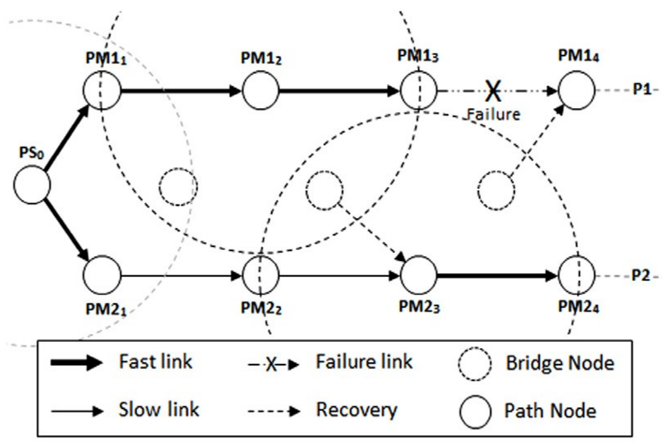

Fig 2. An example of data transmission using contention multipath

Since the bridge node has received both PREP and OPREP, it is adjacent to member nodes belonging to at least two different paths. For example, in Figure 2, if the bridge node forwards the data packet received from $PM1_2$, which is the forwarding node of route P1, to route P2, the bridge node passes through the neighboring route contention transmission can be performed by forwarding packets to $PM2_2$ and $PM2_3$, which are members of P2. In this case, since member $PM2_3$ is closer to the sink than $PM2_2$, it is more advantageous for $PM2_3$ to forward the packet for real-time transmission. As a result, the bridge node sends a packet to $PM2_3$. If $PM2_2$ detects data transmission of $PM2_3$, it discards the packet, and if not, it transmits data to the next forwarding node. This is because, basically, the selected bridge nodes recognize the forwarding nodes of neighboring multipath through the bridge node selection process and store their information. Therefore, it is possible to distinguish the source of the received (overhearing) packet in the data transmission process.

In the Proposed Contention Transmission Routing Algorithm (PCTRA), the transmission waiting time T is calculated in the following way. First, as in real-time transmission, the minimum value of the delivery waiting time to minimize the peer to peer delay time of a packet is set to 0 as T_min. On the other hand, T_max, the maximum value of the transfer waiting time is the maximum delay time that can satisfy the peer to peer delay time required by the application, and can be calculated through the same formula as Equation (1).

$$T_{-}\max = T_{-}\text{desired} - T_{-}\text{passed} - T_{-}\text{expected} \tag{1}$$

The three factors considered in Equation (1) above are as follows. - T_desired: packet request delay time, T_passed: The time spent transmitting the data packet received by each bridge node, T_expected: Expected delay for a packet to reach its destination via another path

By using the contention transmission method of the proposed method, the network operator can balance energy consumption and real-time improvement by appropriately selecting the required delay time of packets according to the type of data.

3 Results and Discussion

In this chapter, we conduct experiments in various environments to evaluate the performance of the proposed method and describe the analysis results. The basic settings of the experimental environment are shown in Table 1. Performance evaluation is performed by comparing and analyzing the experimental results of ECMP[6] and PMMR[7] among the existing multi-path methods and various conditions of the proposed method using the measures packet delivery ratio, energy consumption, and delay. The evaluation items are as follows.

Table 1. Simulation Environment and Default Settings

Parameters	Values
Network size	500m x 500m
Number of Sensors	1000
Node Placement	Random Rectangle
Number of Sources	1
Number of Destination	1
Distance from Source to Destination	250m
Radio range	30m (omnidirectional)
Number of Packets	100
Number of Paths	3
Average of Hop Delay	Random Propagation Delay Model
Node Failure Model	Random Propagation Loss Model
Number of Simulations	100

In all experiments, the proposed method obtains three results according to the latency (0, 0.05, 0.1) of the bridge node, and independent multi-path transmission allows each path to follow a single path routing method. Performance analysis is calculated by obtaining the results.

3.1 Packet Delivery Ratio (PDR) according to request timeout

In the basic experimental environment, the average one-hop transmission time is 1ms. Therefore, when the path length is 10 hops, the appropriate request timeout is 10ms. Based on this, Figure 3 shows the results obtained by performing the experiment on the environment in which the required time limit is changed from 7.3ms to 8.2ms. In Figure 3, the existing multi-path transmission method shows the lowest data transmission success rate. On the other hand, the proposed method shows that the shorter the waiting time, the better the data transfer success rate. Also, when the request timeout is less than 10ms, which is the average delay time between peer to peer, the data transfer success rate rapidly decreases as the request timeout decreases. You can check what you did. Through this, the proposed method can support routing that can effectively support delay-sensitive applications by setting an appropriate waiting time according to the reliability of the request in the application that requires a request timeout lower than the average delay time between the ends.

Table 2. Comparison of PCTRA with ECMP and PMMR

Methods	Average Packet Delivery Ratio7.3 to 8.2	Average Power Consumed10 to 19	Average of Peer-to-Peer Delay0.15 to 0.6
PCTRA	96.4	1600	9.32
PCTRA with latency 0.1	70	1075	9.96
PCTRA with latency 0.05	78.8	975	10.01

Continued on next page

Table 2 continued

ECMP	76.3	885	10.27
PMMR	70.1	785	10.23

The Table 2 is plotted based on average packet delivery ratio ranging from 7.3 to 8.2, average power consumed from 10 to 19 and average peer to peer delay from 0.15 to 0.6 and the data is plotted in Figure 3.

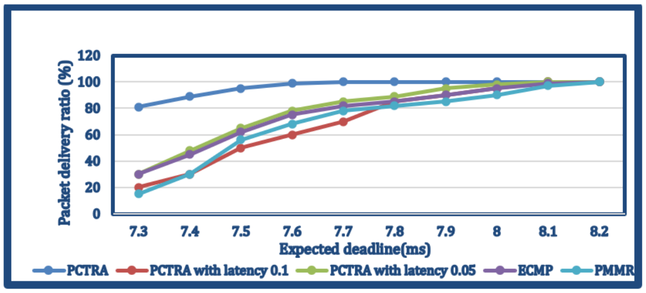

Fig 3. Packet delivery ratio by expected deadline

From the Figure 3 it is clear that the packet delivery ratio of PCTRA, PCTRA with latency 0.1, PCTRA with latency 0.05 performed better than ECMP and PMMR with the help of the virtual network even with latency PCTRA performed better, Because ECMP and PMMR are affected by external dynamic environment.

3.2 Power consumption according to peer to peer hop count change

In this experiment, in order to analyze the change in power consumption according to the distance between the ends, the experiment was performed in an environment where the number of hops in the path was changed from 5 to 15 hops. As a result of this, it can be seen in Figure 4 that power consumption increases in proportion to the distance because the number of data transmission increases as the distance between the ends increases in all routing methods. In particular, among the proposed schemes, the gradient of change in total energy consumption of the emergency transmission scheme is larger than that of other schemes. In the emergency transmission mode, as soon as the bridging nodes receive a data packet, it forwards the packet to another path, providing a high transmission success rate, while the bridging nodes increase their routing participation, resulting in increased power consumption. Also, analyzing the results of this experiment, it can be confirmed that the longer the waiting time of the bridge node in the proposed method, the gentler the slope of the power consumption. The reason for this result is that the longer the waiting time for the bridge node to determine the failure, the longer the transmission due to delayed transmission in multipath routing.

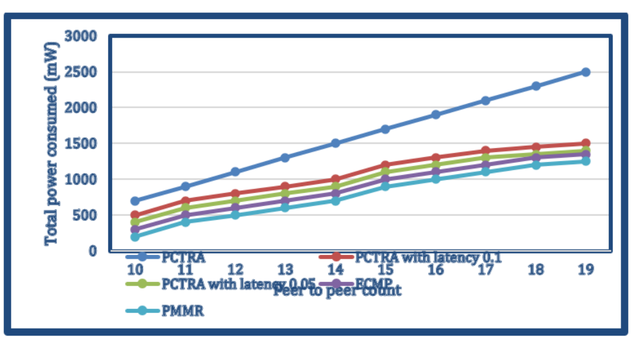

Fig 4. Total power consumed in peer to peer count

3.3 Peer to peer average delay time according to hop delay deviation

This experiment was conducted to compare the difference in the average propagation delay time between the ends of the multipath according to the change in the delay time deviation of single-hop transmission. In Figure 5, it can be seen that for all routing methods, the average peer to peer propagation delay time decreases as the hop delay deviation increases. This is a phenomenon that does not occur in single-path routing, and shows the characteristics of routing using multiple paths. The peer to peer average delay time of ECMP and PMMR has the smallest decrease due to the increase in the deviation of the hop delay time. This is because the greater the deviation of the hop delay time, the higher the probability of existence of links with significantly higher hop delay time than the average delay time.

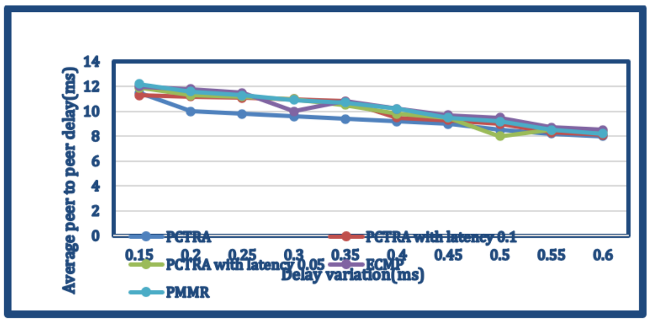

Fig 5. Average peer to peer delay by delay variation

4 Conclusion

This study has proposed a real-time multi-path routing protocol that guarantees real-time transmission of data using a multi-path contention transmission method and reflects application needs. The proposed method provides real-time routing through multipath cooperation by constructing a wireless separated multipath and selecting a bridge node to support contention transmission between the separated multipaths. In addition, the proposed method can provide performance which is suitable for various environments and applications by setting flexible delivery latency that can provide both timeliness of real-time routing and transmission reliability at the same time. Virtual network is established and the restrictions due to external dynamic environment is reduced to a large degree. This was verified through performance evaluation by comparing and analyzing three results according to different waiting times of the existing multi-path routing methods and the proposed method by performing experiments in various environments. In future research, we plan to improve the proposed method by conducting additional research to set flexible waiting time for contention transmission and to reduce unnecessary relaying.

References

1) Shaojie N, Yang, Yong, Wenxiang XL, Wei YE, Xiaozhou. The Status Quo and Prospect of Satellite Network Routing Technology. *Journal of Electronics & Information Technology*. 2023;2023(2):383–395.
2) Feng H, Zexiang L, Xu D. Research on path dynamic redundancy strategy in Time Sensitive Network. *Microelectronics & Computer*. 2022;2022(11):54–61.
3) Ting Y, Guanghua Z, Ling L, Yuqing Z. A Survey of Authentication Protocols in the Internet of Things. *Journal of Cryptologic Research*. 2020;7(1):87–101.
4) Chenyu W, Ding W, Feifei W, Guoai X. A multi-factor authentication protocol for multi-gateway-oriented wireless sensor networks. *Chinese Journal of Computers*. 2020;(4):43–43.
5) Xutong Z, Mowei W, Cui Y. Low Latency Network: Architecture, Key Scenarios and Research Prospects. *Journal on Communications*. 2019.
6) Hongjun Z. A secure and efficient remote authentication protocol for wireless sensor networks. *Journal of Terahertz Science and Electronic Information*. 2021;19(1):150–155.
7) Shuyi C, Yali L, Changlu L, Tao LI, & Dong Yongquan. A lightweight verifiable group authentication scheme for the Internet of Things. *Electronic Journal*. 2022;50(4).
8) Vaidya B, Makrakis D, Mouftah H. Two-factor mutual authentication with key agreement in wireless sensor networks. 2016. Available from: https://doi.org/10.1002/sec.517.
9) Mishra D, Vijayakumar P, Sureshkumar V, Amin R, Islam SH, Gope P. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimedia Tools and Applications*. 2018;77(14):18295–18325. Available from: https://doi.org/10.1007/s11042-017-5376-4.
10) Wu Z, Huang W, Dai Z, Dai B, Mo Y. On-demand intelligent routing technology for deterministic networks. *Telecommunications Science*. 2021;37(11):11–16. Available from: https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00048.

11) K DA. A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. *Wireless Personal Communications*. 2015;82:1377–1404. Available from: https://doi.org/10.1007/s11277-015-2288-3.
12) Weidong F, Wuxiong Z, Tao P, Zhiwei G, Yepeng N. An anonymous two-factor user authentication protocol for layered wireless sensor networks. 2020.
13) Zijing LG, Yuchuan C, & Zhiping, Tengfei Z. A Review on Privacy Protection of Medical and Health Big Data. *Computer Science and Exploration*. 2021;15(3).