An Overlapping Routing Tree Transmission Model Based on Segment Identification

OTSI Model

Sushu Guo
School of Information Engineering, Capital Normal University, Beijing China
wwwwwuy@126.com

Wenlong Chen
School of Information Engineering, Capital Normal University, Beijing China
chenwenlong@cnu.edu.cn

Jiacheng Wang
School of Information Engineering, Capital Normal University, Beijing China
2191002062@cnu.edu.cn

ABSTRACT

In the Internet of Things (IOT) based on IPv6. For large-scale multi-gateway WSN, the sensor device has its own certain limitations, and the processing capability of the node is very limited. Due to the limitations of the traditional WSN routing transmission protocol, this paper proposes an overlapping routing tree transmission model (OTSI) based on segment identifiers and a method to generate the model. We design a segment identifier based on the model, specifying transmission gateways and service demands for nodes in different manifestations of segment identifiers. We also designed a data transmission model of the OTSI in different scenarios. Through the OMNeT simulation experiment, it's found that the model can effectively specify the transmission gateway for the node according to the service demand, and achieve the balance of traffic transmission.

CCS CONCEPTS

• **Networks**; • **Network protocols**; • **Transport protocols**;

KEYWORDS

IOT, Routing tree, IPv6, Routing transmission, Load balancing

ACM Reference Format:
Sushu Guo, Wenlong Chen, and Jiacheng Wang. 2021. An Overlapping Routing Tree Transmission Model Based on Segment Identification: OTSI Model. In *The 5th International Conference on Computer Science and Application Engineering (CSAE 2021), October 19–21, 2021, Sanya, China.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3487075.3487108

1 INTRODUCTION

WSN (WSN) is one of the core technologies of the IOT. WSN has important applications in military applications, environmental monitoring etc. The existing WSN routing protocols are mainly divided into five types: geographical location-based routing protocols, hierarchical routing protocols, energy-aware routing protocols, data-centric routing protocols, and reliable routing protocols.

CSAE 2021, October 19–21, 2021, Sanya, China

ACM ISBN 978-1-4503-8985-3/21/10…$15.00
https://doi.org/10.1145/3487075.3487108

Due to energy consumption and computational complexity, the traditional Internet routing protocols are not suitable for WSN. Because of the connection requirements between the IOT and the normal Internet, a better protocol is needed. WSN routing protocols faces the problems of single transmission path, unspecified transmission service, slow route recovery speed etc. RPL provides an unique routing through its DAG and DODAG topologies, this method better solves the problem of node failures, but it does not effectively solve the problem such as transmission path designation, link congestion, etc. Aiming at the IOT environment of IPv6, this paper proposes an Overlapping tree routing transmission model based on segment identification (OTSI). The main contributions of this paper are as follows:

First, the overlapping routing tree is designed and its generation process is specified. The IOT nodes can choose different gateways for transmission.

Second, the segment identifier is designed. The segment identifier is embedded in the last part of the IPv6 address of the node, including gateway bits and service quality bits. The node selects the gateway and the expected service request through the segment identifier.

Finally, analyzing the different transmission scenarios and the changes of segment addresses during transmission, designing a routing transmission method based on overlapping routing trees.

The rest of this article are organized as follows: SectionIIintroduces the related work; Section III introduces the architecture of overlapping routing trees and segment address; SectionIV introduces segment addresses based on overlapping routing trees; Section IV designs an transmission method through different scenarios; SectionVverifies the feasibility of the model; Section VI summarizes the article.

2 RELATED WORK

Sensor nodes are limited by factors such as energy, storage, computing [1] etc. Therefore, it is necessary to design a suitable routing protocol to overcome the problems caused by traditional routing protocols. Previous studies have improved the lifespan of WSN from the perspectives of balancing energy consumption, sleep scheduling, and adjusting topology, but there are some shortcomings. Nowadays, The combination of IPv6 technology and WSN routing protocol has become a main research area. Karim et al. [2] proposed a new reverse packet elimination (RPE) algorithm implemented on IPv6. RPE reduces unnecessary packet transmission by sending a

cancel packet from the receiving end to the sender, thereby improving reliability and saving energy. However, the network lifetime slightly increases under the modified mechanism.

Daniel [3] et al. proposed a scheme for embedding coordinates in the Ethernet MAC address to allow the usage of IPv6 header compression, and proposed an efficient method to exchange neighbor address information and support dynamic address changes to replace promiscuous Listen in model. However, continuous dynamic address changes will bring a huge burden.

The RPL protocol is the most widely accepted routing protocol in LLN. RPL provides unique routing through its DAG and DODAG topologies. However, when using different network topologies and media access control (MAC) protocols, RPL has some problems [4]. Agung et al. [5] analyzed the mobility and transmission range of the RPL routing protocol based on IPv6 of WSN. The results show that through the experiment of the RPL protocol, when the node moves randomly, the mobility of node is the best. However, RPL may take a while to complete the routing convergence.

Yang et al. proposed a dual-adaptive clustering hierarchy (DACH) [6] algorithm. After using LEACH for cluster initialization, DACH will perform adaptive clustering based on RSS, hop count etc. Therefore, the node based on DACH can access the Internet through IPv6, and its life span is significantly extended,but the flexibility of the algorithm has not been verified. In addition, the packet loss rate should be further reduced.

Redundant links are also called backup links. Both MMSPEED [7] and MCMP are source data packet transmission methods on redundant links. The MMSPEED protocol provides service differentiation and probabilistic service quality assurance in terms of timeliness and reliability. Providing multiple network speed options for various types of traffic, so as to select the correct speed option for time domain data packets. MMSPEED has certain applications in 6loWPAN.

Di Tang et al. proposed a new security and energy-aware routing protocol SEAR [8]. SEAR strengthens energy balance and prolongs life cycle by setting two configurable parameters, energy balance control and safety level. SEAR algorithm can prevent routing backtracking attacks and strike a balance between routing efficiency and energy consumption. The disadvantage is that the calculation scale is too large.

Zhao et al. proposed an optimal DAG construction method based on data-centric WSN [9] ,DAG allows each node having multiple parent nodes and multiple child nodes, and each intermediate node can Choose any parent node to send the data packets generated locally or forward the data packets received from the child nodes, therefore distribute the load in the network more evenly.

Zhe Zheng et al. proposed a high-reliability forwarding model HRVN based on virtual nodes in node-intensive WSN networks [10]. The virtual nodes are set up to achieve load balancing and rapid recovery of failures, but the address allocation of HRVN will cause the Waste of address resources.

Xingyu He et al. proposed a tree address-based coding-aware routing CARTA [11], which uses the inter-stream exclusive OR coding technology to improve the network performance of WSN. The disadvantage is that it is not suitable for complex networks. RENJIE LIU proposed a new model of an IPv6-based addressless IOT server [12], which allows people to use a larger IPv6 address space to hide addresses in use. The disadvantage is that the encryption algorithm used consumes computing resources.

Table 1: Symbol Identification Table

Notation	Meaning
O_Node	Overlapping nodes
G_Node	Gateway node
N_Tree	Normal Tree
O_Tree	Overlapping routing tree
S_Tree	Sub Tree
SGA	Segment Address
SI	Segment Identification
SNB	Subnet Bit
HB	Host Bit
GTB	Gateway Tree Bit
SQB	Service Quality Bit
RB	Reserved Bit
reach_node_list	List of reachable nodes
Child_list	Child node list
M_child	Maximum number of children

3 OVERLAPPING ROUTING TREE ARCHITECTURE

In this section, we will give a detailed description of OTSI, the symbols are listed in Table 1

3.1 Proposed Method

The typical data transmission structure of sensor network is tree topology. The root of the tree is a G_Node connecting the subnet of the IOT and the external Internet. The sensor nodes are added to the routing tree in order to go up. The data transmission of the traditional tree structure network adopts single-path routing, and each sensor node corresponds to an unique gateway, the path of node to sensor node is fixed, once the intermediate node fails or congested, data transmission problems will occur. Therefore, the flexibility and reliability of routing transmission in this scenario are slightly insufficient.

Definination1. OTSI. In a sensor network, if a sensor node belongs to multiple routing trees at the same time, then this node is called an overlapping node (O_Node), and the routing tree with O_Node is called an overlapping routing tree (O_Tree).

As shown in Figure 1, nodes A~I form an O_Tree. Figure 2(a) is an example of OTSI. A and F are G_Node. Figure 1(b) and Figure 1(c) are two routing trees N_Tree 1 and N_Tree 2 rooted at A and F respectively. The nodes C,D,E,H are O_Node, because they are both in N_Tree 1 and N_Tree 2. At the same time, O_Node H will transmit part of the traffic to node G through the path H-G-F, and part of the traffic of node H still maintains the original transmission direction and is transmitted along the path H-C-A. The O_Tree prevents more congestion caused by the centralized transmission of traffic to a certain extent, and uses the multi-gateway architecture to reduce the heavy burden of the gateway during the transmission of the single-gateway architecture.

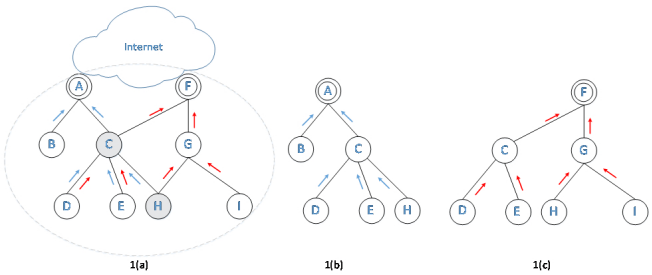

Figure 1: Schematic Diagram of an O_Tree.

For a multi-gateway WSN, each G_Node will build a routing tree with it, and each tree corresponds to a gateway tree bit. Since the O_Node exists in multiple routing trees, the node can mark the routing tree to which it belongs by the gateway tree bit, 0 means that the node does not exist in the routing tree with this gateway as the root node, while 1 means that the node exists in the routing tree with the gateway as the root node. Even if a node exists in multiple routing trees (such as gateway 1, gateway 2), there is only one S_Tree with it as the root (all members in the S_Tree belong to at least 2 G_Node).

3.2 OTSI Generation

The generation of O_Tree refers to the routing tree construction process of the traditional RPL model, however it has some differences. All nodes of the O_Tree are in a network segment and are constructed layer by layer. The nodes of each layer have its own RANK, which represents the level of the node in the network. The RANK of the G_Node of O_Tree is 0, and the sensor nodes directly connected to the G_Node are in the second layer, the RANK of these nodes is 1. Using the RANK can effectively solve the problem of data loops in an O_Tree, each node has a batch of addresses according to the SGA. Assuming that the network segment of the address allocated for the current routing tree in this article is 2001:DA80::0000:0000/64, taking node A as an example, node A will have a batch of addresses between 2001:DA80::0001:0000/64 and 2001:DA80::0001:ffff/64. That means each node occupies 65536 addresses. As shown in Figure 2, the address marked in red is the SI. The node can select the gateway for transmission according to the gateway bit marked by the SI, or select the transmission mode according to the quality of service bit. The specific explanation of the SI will be explained in Chapter 4.

3.2.1 Neighbor Node Discovery Phase. In the process of constructing a routing tree, nodes periodically send 'NR' (Node Reachable) packets to collect information of neighbor node. All nodes within the reachable range send 'NBI' packet after receiving the 'NR' packet. The 'NBI' packet contains the basic information of the current node, such as the RANK. The node that receives the 'NBI' packet will update its reach_node_list. Only nodes that become neighbors are eligible to have a parent-child relationship.

3.2.2 Parent Node Discovery Phase. While sending the 'NBI' packet, the node will also send the 'NDA' packet to the selected parent node, telling it is a child node. After the parent node has updated its own routing table, it sends the 'NDA' packet to the parent node of the parent node, and finally the two-way link is formed after reaching the G_Node. The 'NBI' data packet of the neighbor node contains the objective function, such as DAG characteristics and other important information. According to this information, it decides whether to establish a parent-child relationship with the root node, calculates its own RANK value in the graph, and then sends an 'NDA' message to its parent node. Secondly, a node that newly joins the routing tree can use the 'NR' message to actively request O_Tree information from neighboring nodes. All neighbor nodes repeat this process until an OTSI with multiple gateways as the root node is constructed in the network. At the same time, the value of M_child specifies the number of child nodes that the current node can accommodate. The values of all child nodes that become the current node will be stored in the list named child_list. If the number of child nodes is equal to M_child, the node is not allowed to join the routing Tree. When the node successfully joins the routing tree, its parent node will send 'Connection reply' message to confirm, then remove the added node from the neighbor node list reach_node_list.

According to the above rules, starting from the G_node of O_Tree, nodes that are not added to the routing tree in the Reach_node_list list will be added to the routing tree. Starting from the root node, when a node with a RANK of 1 is added to the routing tree and the number of child nodes is equal to the M_child, The first layer is built completed , and the second layer is built after the first layer is built with the same process.

3.2.3 G_Node Monitoring Phase. When constructing an O_Tree, all G_Nodes send 'NR' information at the same time. If node A is in the neighbor list of two nodes at the same time, and the GTB of node A includes the gateways of node B and node C at the same time, it means that node A can be establish a parent-child relationship with two nodes at the same time.

If an O_Node wants to join multiple independent routing trees, the node firstly choose to join the node with low RANK value (closer to the root node), and then joins the node with high RANK value. As shown in Figure 2, when node L wants to join the routing tree rooted at gateway B and the routing tree rooted at gateway C at the same time, node L will send a 'node priority' message to node H, because the rank of node H is lower than node j. While node L receiving the message, it will first establish a parent-child relationship with node H, and then establish a parent-child relationship with gateway J. If a node wants to establish a parent-child relationship with two nodes with the same RANK, then following the order in which the nodes send 'NBI' message. As shown in Figure 2, node J needs to establish a parent-child relationship with node E and node F at the same time, then node E sends 'NBI' first, at the same time, node F will receive a 'Node Waiting' message sent by node J. node J first establishes a parent-child relationship with node E, and then establishes a parent-child relationship with node F. All relevant bits are shown in Figure 3

3.3 Segment Address

Definination2.Segment identification. In OTSI model, several consecutive bits at the end of the IPv6 address constitute the segment ID (SI).

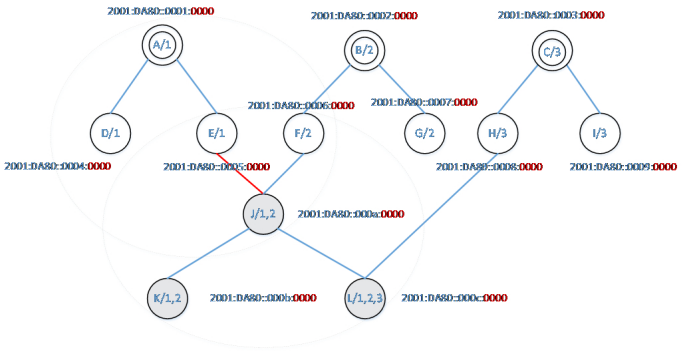

Figure 2: Schematic Diagram of the Middle Section of the O_Tree.

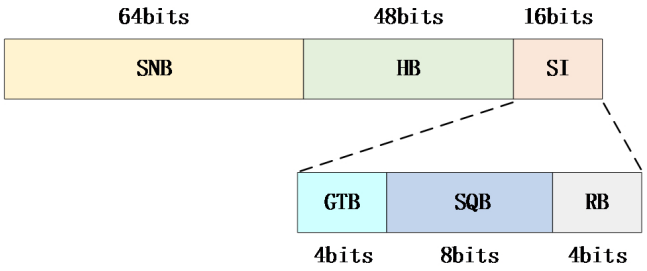

Figure 3: The IPv6 Address Format of the Sensor Node.

The SI of the same sensor network has bits of the same length. This article sets the length of SI up to 16, which can be customized according to different scenarios and needs, and the recommended value range is [8, 32]. The SI is embedded in the IPv6 address and is used to identify various routing information such as the routing tree and the quality of service, and the value of the SI does not affect the identity of the node.

In this article, each IOT node is assigned an IPv6 address segment, where the value of the first (128-16) =112 bits is determined and used to uniquely represent a node. The SI also has different values.

Because the SI length is 16, the IPv6 address space of each sensor node is 2^{16} (63326). The IPv6 subnet prefix length of the IOT subnet is 64. this subnet can represents 2^{48} network nodes. Let the segment address (SGA) of a node X be 2001: DA80::0001:0000, and its address range is between 2001:DA80::0001:0000 and 2001:DA80:0001:FFFF. In network transmission, any IPv6 address in this address range can represent a node X.

3.4 Related Bits

3.4.1 Sub Network Bits (SNB,64bits). The OTSI model follows the most typical IPv6 subnet address plan, and the IOT subnet has a uniform IPv6 network SGA with a 64-bit mask length. When the sensor node joins a certain routing tree for the first time, it learns the 64-bit SNB of the IOT subnet from the G_Node. The sensor node obtains an IPv6 SGA. according to the SNB and the host bit generated by itself.

3.4.2 Host Bits (HB,48 bits). In the OTSI, each node is uniquely represented mainly by the host bit. The sensor node is calculated based on the physical address of the wireless network card. The calculation method can refer to the 64-bit extended unique identifier (EUI-64 address).

3.4.3 Gateway Tree Bits (GTB).. The egress gateway can be selected by setting the "GTB", and multiple (up to 4) GTB can be set at the same time, indicating that it supports sending from any gateway that has been set. This article assumes that the GTB occupies 4 bits, each bit corresponds to a gateway, (corresponds to a routing tree). For example, "0101" means the second and fourth gateways.

3.4.4 Service Quality Bits (SQB).. Used to describe data transmission service requirements (may be the source node settings, or the intermediate transmission node settings). Each bit represents different transmission service requirements, such as bandwidth, delay (transmission delay refers to the time when a data packet is sent out, and propagation delay refers to the time from when a data packet is sent out to when it is received), number of hops, energy Consuming etc.

3.4.5 Reserved Bit (RB).. Note that while the SNB is set to 64 bits. Other bits, such as the GTB and the SQB can be customized based on network deployment scenarios and transmission requirements. The remaining bits will be studied in the future.

3.5 Address Allocation

Definination3. Bit Setting. In addition to SNB and HB, other bits can be customized according to network deployment scenarios and transmission requirements. The definition is as follows.

Let the number of SI space bits be d, the m bits in the d bits of SI are set to GTB*{x1, x2, . . . , xm}*, and the n bits are set to service quality bits SQB*{y1, y2, . . , yn}* , The rest are reserved bits, where m+n<=d. x_i represents the i-th gateway, y_i represents the type of service requested by the node, and the remaining (d-m-n) bits are reserved bits to prepare for subsequent work.

Table 2 is an example of SI of node j. As shown in Table2, the address of node j is 2001: DA80::000a:3010/64, d=16, m=4, n=8, the part of SI is <0011 0000 0001 0000>, indicating that the data packet can be Transmit from G_Node A and B to the external network. The SQB is set to 1 and is Boolean type. The SQB is required to provide a transmission security service for node j. If it is set to 0, it means that no secure transmission service is required.

Table 2: Schematic Table of SGA

Address (Binary)	0011	0000 0001	0000
meaning	GTB	SQB	RB

3.6 Quality of Service Bits

As mentioned above, SQB is used to describe the data transmission service demands of the source node and the intermediate transmission node. The use of SQB includes the following three types.

3.6.1 Boolean Type. Only 1 bit is required, for example, 0 means no transmission energy consumption requirement, 1 means transmission energy consumption requirement. As shown in Figure 4(a), the first bit of the SQB of all nodes is set to 0, which means that there is no requirement for transmission energy consumption when the node transmits data.

3.6.2 Level Type. K bits represent 2^k level descriptions, for example, 2 bits represent 4 bandwidth levels. As shown in Figure 4(a), the requirement of node F for the link bandwidth is 50Mbps, so the node can only transmit to the gateway through the path F-D-B to root B. Taking the propagation delay as an example, as shown in Figure 4(b), the propagation rate of the data frame on the channel is 1^*10^5m/s, and the node F is required to reach the gateway A or the gateway B within the transmission time of 0. 6s. Therefore, node F can only transmit data packets to the external network through the path F-D-A.

3.6.3 Numerical Value Type. M bits represent a specific value with a maximum value of (2^m-1). If the value of 2^m is x, it means that it is required to reach the gateway within the range of x hops. Of course, the value range expressed by m bits can be scaled by multiplying and dividing in an equal proportion. As shown in Figure 4(c) the packet with node G as the source node is required to reach the gateway within 2 hops, so node G can only transmit the data packet to gateway A through the path G-F-A.

In the SI, whether to specify the quality of SQB has several reference factors: The network traffic NP_m is the most important factor that determines the SQB. Other network state parameters NP_i during node-to-gateway transmission include routing hops, physical distance, link bandwidth, link stability, etc. NP_i can be learned by the gateway in real time, or configured by the administrator. Both NP_m and NP_i have their own weights, and W corresponds to the weights of different parameters, as shown in the formula:

$$Wm + \sum_{i=1}^{n} Wi = 1$$

If it need to specify the SQB, the calculated result >1, if you not, the calculated result result<1.

$$\begin{cases} Wm * NP\_m + \sum_{i=1}^{n} (Wi * NP_i) & result > 1 \\ NP\_m & result < 1 \end{cases}$$

4 DATA TRANSMISSION

The data transimission processing of IOT nodes can be divided into uplink transmission and downlink transmission. In the OTSI, the O_Node selects a specific gateway for transmission according to GTB and SQB for uplink transmission, and the specific designation method has been described above. In the downlink transmission, the topology information of each routing tree is stored in an G_node. Due to the 1:N structure of the N_Tree, only specific paths can be transmitted, so the downlink transmission is very efficient.

5 EXPERIMENTAL EVALUATION

In our experiment, we used OMNeT network simulation simulator to build a specific topology, as shown in Figure 5. The sensor nodes of Node0 to node14 are built into an OTSI layer by layer, in which nodes 0, 1 and 2 are three G_Nodes. Node15 is an Internet node. Nodes inside the OTSI interact with internet node 15 through G_Nodes 0, 1 and 2.

5.1 Gateway Load Balancing

This paper tests the traffic sent to the gateway by all nodes in different time periods. At 0-1s, all ordinary nodes send packets to gateway 0, and O_Node can only send packet to G_Node 0 instead of the other two gateways. As shown in Figure 6, about 7 nodes send data at this time, The packet received is between 0. 5kb-0. 6kb. At 1s-2s, all ordinary nodes send data packets to gateway 1, and about 9 ordinary nodes send packets. The size of data packets received by gateway 1 in this time period is between 0. 5kb-0. 7kb. At 2s-3s, ordinary nodes only send packets to gateway 2, and about 6 nodes send packets. The packets received by gateway 2 range from 0. 3kb to 0. 4kb. The ratio of the number of sub nodes connected

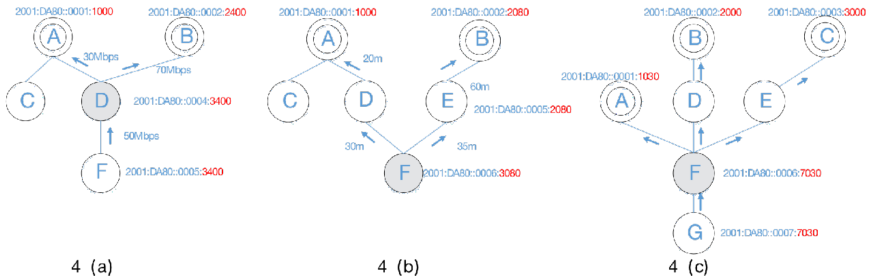

Figure 4: Schematic Diagram of SQB.

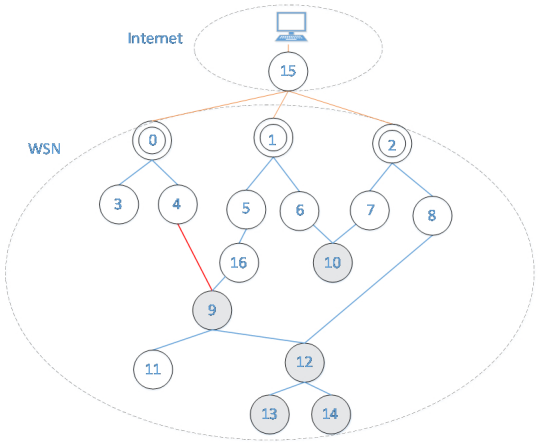

Figure 5: Schematic Diagram of OMNeT Simulation.

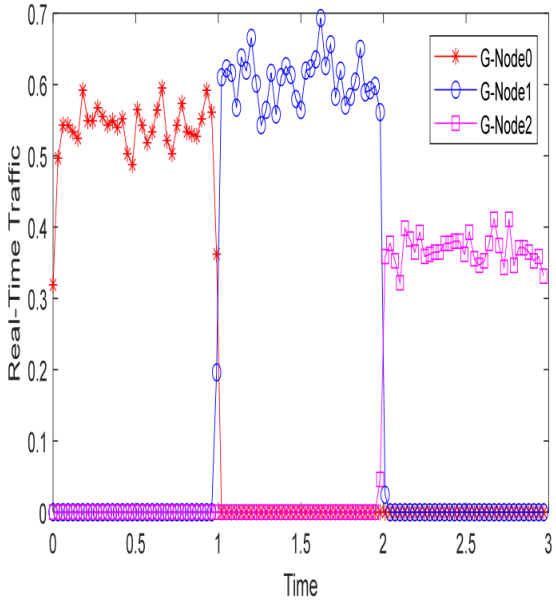

Figure 6: The Packets Received by Gateways.

to the G_Node is about 7:9:6, and the traffic ratio received by the corresponding gateway is about 11:12:7. It can be seen that the number of sub nodes connected to the G_Node is different, and the number and size of data packets received are also different. Obviously, the more child nodes connected, the more traffic will be received.

5.2 Link Failure

Figure 7 shows the change of traffic received by different gateways when the link is disconnected. As shown in Figure 7, At 0. 8-1. 7s, the link from node 9 to node 4 is disconnected. At this time, the traffic of nodes 11 to 14 could have been transmitted through gateway 1 can only be transmitted through gateway 2 and gateway 3. At

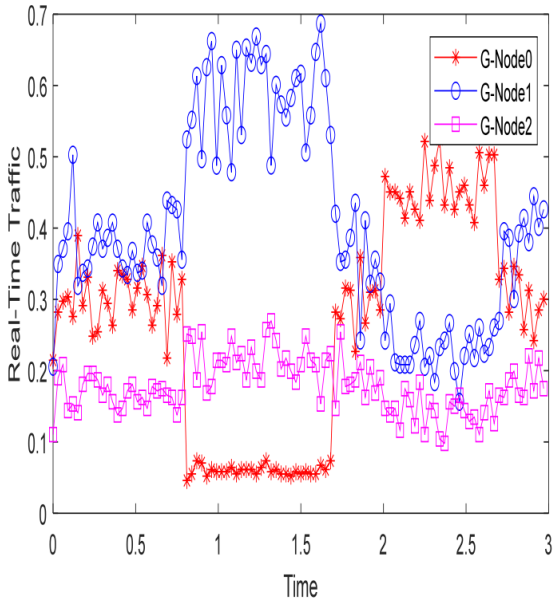

Figure 7: The Change of Load When Link Is Disconnected.

this time, the traffic received by G_Node 1 and G_Node 2 increases significantly, while the traffic received by node 0 decreases significantly. At 2s-2. 7s, the link from node 9 to node 16 is disconnected. At this time, the traffic that can be transmitted to G_Node 1 with nodes 11 to 14 can only be transmitted through gateway 0 and gateway 2. During this time period, it can be seen that the total data transmission traffic of gateway 1 decreases significantly and the total data transmission traffic of gateway 0 increases significantly. The traffic received by gateway 2 has not changed significantly overall.

5.3 Traffic of Different SQB

Figure 8 shows the traffic received by the three gateways when node 12 sets the SQB bit (propagation delay, hops). It can be seen that the propagation delay of node 12 gateway 0 is the shortest in the time interval of 0-1s, and the propagation delay of node 12 transmitting to gateway 1 is the shortest in the time interval of 1-2s. In the time interval of 2-3s, the propagation delay of node 12 transmitting data packets to gateway 2 is the shortest. It can be seen that the model designed in this paper can flexibly switch transmission paths when nodes have transmission service demands. Figure 9 shows the corresponding hop number change of node 12 transmitting data to the gateway when setting the experiment request. As shown in Figure 5, within 0-1s, node 12 transmits to the external network through gateway 0, and 4-hop transmission through node 12-9-4-0. Within 1-2s, node 12 transmits to the external network through gateway 1. Through node 12-9-16-5-1, it needs to go through 5-hop transmission. It can be concluded that when the node specifies the SQB, the path of data packet transmission from the current node to the node will change, and the corresponding hop number will also change.

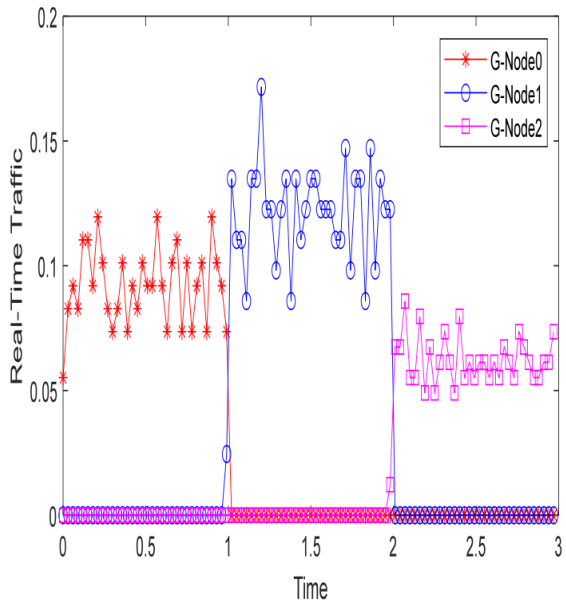

Figure 8: The Flow of the Gateway with SQB (Propagation Delay).

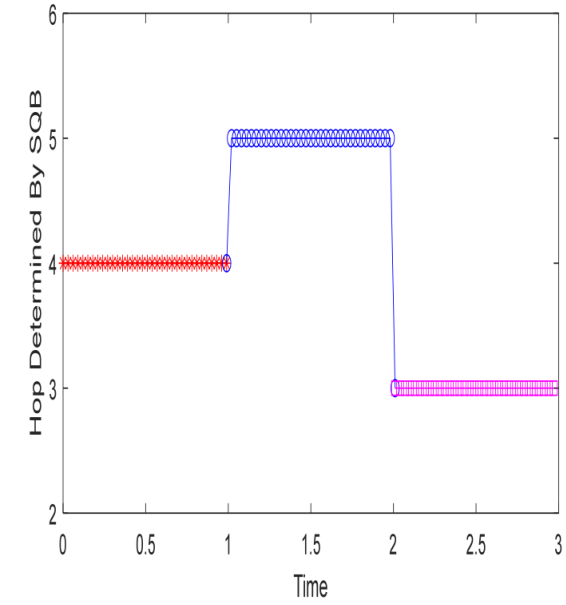

Figure 9: The Flow of the Gateway with SQB (Hops).

6 SUMMARY

In order to improve the robustness and load balancing of WSN, an overlapping tree routing transmission model based on SI is proposed in this paper. In OTSI, G_Nodes and ordinary nodes form a tree topology. O_Node only need to set the last segment of their IPv6 address as GTB and SQB. At this time, GTB can specify different gateways, and the SQB can specify different service demands for the node. OTSI provides a load balancing and path backup mechanism based on IPv6. The analysis shows that the storage consumption of forwarding items of G_Node in OTSI model is related to the number of O_Node. And it can realize rapid recovery when the link is disconnected.In WSN, the sensor node changes the routing and forwarding according to the different states of the O_Node, so when the link fails, other gateways can take over the forwarding work of some traffic of the node. The experimental results show that OTSI achieves good load balancing and fast link recovery with low forwarding capacity overhead. However, the design of IPv6 address space in OTSI model may lead to excessive use of IP address. We take the callback mechanism of IPv6 address as our future work.

ACKNOWLEDGMENTS

We gratefully acknowledge the support from The National Natural Science Foundation of China (61872252) and Beijing Natural Science Foundation (4202012)

REFERENCES

[1] He, A., Lin, Z., & Qu, Q. (2018). Gateway deployment algorithm based on 6lowpan multi-gateway system. Application of Electronic Technique. Rpl-based routing protocols in IOT applications: a review. IEEE Sensors Journal, PP(99), 1-1.
[2] Kvist, F., Urke, A. R., & Vsthus, K. (2020). Energy efficient determinism in wsn through reverse packet elimination. Sensors (Basel, Switzerland), 20(10).
[3] O' Daniel, T. (2020). Ipv6 wsn geolocation using the mac address. Journal of Physics Conference Series, 1529, 022017.
[4] Tran, H , Vo, M. T. , & Mai, L. (2018). A Comparative Performance Study of RPL with Different Topologies and MAC Protocols. 2018 International Conference on Advanced Technologies for Communications (ATC).
[5] Prawira, Agung Jati, M. Abdurohman and A. G. Putrada (2019). An Analysis on RPL Routing over IPv6 WSN Mobility and Transmission Range. 2019 International Symposium on Electronics and Smart Devices (ISESD).
[6] Yang, D., & Qiao, G. (2014). Dach: an efficient and reliable way to integrate wsn with ipv6. International Journal of Distributed Sensor Networks, 2012(1).
[7] Beniwal, R, Nikolova, K, & Iliev, G. (2019). Performance Analysis of MM-SPEED Routing Protocol Implemented in 6LoWPAN Environment. 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). IEEE.
[8] Di, T, Jiang, T, & Jian, R. (2011). Secure and Energy Aware Routing (SEAR) in WSNs. Global Telecommunications Conference. IEEE.
[9] Zhao Wenbo, Xu Luping, Dai Hao, & Wang Guangmin. (2018). Optimal DAG construction method for lifetime in data-centric wireless sensor network. CN107911834A.
[10] Chen, W, Zheng, Z, Rong, X, Li, F & Sun, Z. (2015). Hrvn: a highly reliable forwarding model based on virtual nodes in node-intensive wsns. International Journal of Distributed Sensor Networks, 2015, (2015-10-28), 2015, 235.
[11] Xingyu He, Guisong Yang (2020). CARTA: Coding-Aware Routing via Tree-Based Address. Wirel. Commun. Mob. Comput. 2020: 4730594:1-4730594:16 (2020)
[12] Liu, R, Weng, Z, Hao, S, Chang, D & Li, X. (2020). Addressless: enhancing IOT server security using ipv6. IEEE Access, 8(1), 90294-90315.