Computers, Materials & Continua
DOI:10.32604/cmc.2021.012365
Article

Tech Science Press

Design, Implementation and Verification of Topology Network Architecture of Smart Home Tree

Youbang Guan[1,2] and Bong Jun Choi[3,*]

[1]Department of Advanced Research and Development, Qingdao, China
[2]Department of Engineering, University of Leicester, Leicester, England
[3]School of Computer Science and Engineering, Soongsil University, Seoul, Korea
[*]Corresponding Author: Bong Jun Choi. Email: davidchoi@soongsil.ac.kr
Received: 30 June 2020; Accepted: 30 August 2020

Abstract: Smart home technology provides consumers with network connectivity, automation or enhanced services for home devices. With the Internet of Things era, a vast data flow makes business platforms have to own the same computing power to match their business services. It achieves computing power through implementing big data algorithms deployed in the cloud data center. However, because of the far long geographical distance between the client and the data center or the massive data capacity gap, potentially high latency and high packet loss will reduce the usability of smart home systems if service providers deploy all services in the cloud data center. Edge computing and fog computing can significantly improve the utilization of network resources and reconstruct the network architecture for the user's home. This article enables a fog resource-based resource allocation management technology. It provides a method that can more reasonably allocate network resources through a virtualized middle-tier method to ensure low response time and configure Quality of Service to ensure the use of delay-sensitive critical applications to improve the reliability of smart home communication system. Besides, the proposed method has is tested and verified by adjusting the variables of the network environment. We realize the optimization of resource allocation of client network without changing the hardware of client.

Keywords: Topology network; smart home tree; resource allocation; internet of things

1 Introduction

Smart home technology originated at the end of the 19th century. People want to use home appliances to build houses with higher automation and more in line with user needs. In the 2020s, more and more users had higher expectations for household appliances. Voice interaction, image recognition and other functions give home appliance provides more selling points. This situation has caused the cost of smart appliances to surge [1]. At present, the number of smart home users has spread to 7.5% of households worldwide and in 2018 generated $44.2 billion in revenue [2]. According to 2017 data, Europe already has 22.5 million smart homes accounting for 9.9% of

European households. After 2022, the global smart home market will proliferate at a rate of 30% per year. Britain, France, Germany, the three most developed countries in Europe will become the leader of the European market. By the end of 2020, 35% of North American households and 20% of European households can be classified as smart homes [3]. Smart home technology has not only driven the home appliance industry but also led to the development of concepts such as smart cities and smart grids. The market potential of smart homes has not fully explored and one day smart homes will eventually affect the way of consumer housing. In the current smart home industry, Haier uses "Carsarte" to emphasize "art of home" to represent the desire to enhance user comfort, safety and high-end user experience.

The significant increase in the number of Internet of Things devices has made networking devices more diverse. More devices that interact with the Internet through 3G, 4G, NB-IoT, WIFI, etc. [4]. The next-generation home appliance network should process and analyze the data of home appliances more complicatedly. However, because of the severe cost problem faced by the home appliance industry, how to improve the use of smart home appliances without increasing the cost of hardware experience has become a top priority for the industry. The fog node extends the cloud system services to the network edge close to the physical location of the smart home, allowing faster data processing and service applications which require network service providers or providing additional necessary equipment. However, most users think as long as there is a home router in the home, when users find that smart homes are no longer "smart" because of network problems, they rarely consider the problem of IoT gateways but think the network configuration of smart devices is not enough. The enthusiasm for home furnishing will test. Besides, the current cloud systems of smart home companies need to process an enormous amount of data from intelligent home appliances in users' homes such as clothes recognition of washing machines, voice interaction of intelligent speakers and linkage of multiple household appliances scenes. A specific Internet of Things protocol performs data collection. Sensors in home appliances gain first-hand data and then through the machine-to-machine (M2M) protocol that communicates with smart home devices and Internet of Things gateways, the output will be by the home station network into the core network.

The IoT gateway also provides functions such as local data storage and processing. But, with the rapid development of the entertainment industry, most users often have a highly integrated network router at home that has met the hardware requirements of the Internet of Things gateway. IoT gateways can serve multiple homes while ensuring trusted connectivity and security by implementing policy-based access mechanisms. IoT gateways can store in any routers or switches in hardware style or software style. Home appliance suppliers only need to do some software development to make home routers or smart speakers to replace traditional IoT gateways [5].

This article expresses the IoT gateway in software and it can attach the portal to a home router or foggy Core's network edge. The QoS of the gateway determines according to the various data processing capabilities and different data storage capabilities of the attached hardware equipment. Smart home data has an enormous amount of data and diverse characteristics. Each operation of parsing the communication instruction, including filtering and cleaning the information set, takes a lot of time. How long it takes depends on the data, whether it is a picture, a voice or a simple status instruction.

The rest of the article is organized as follows. In Section 2, we describe the literature review and research background. In Section 3, we discuss the proposed research method in detail. Section 4 analyzes the experimental data and some findings while Section 5 provides the conclusion of this paper and some future work in the smart home IoT area.

2 Literature Review

The research on the deployment of fog computing in IoT systems is ongoing [6–12]. Deng proposed a balance between energy consumption and delay by allocating work tasks in cloud computing and fog computing systems in 2015. Deng's research proves the rational use of fog computing in smart home architecture can reduce the consumption of network resources in the core network [13]. However, the network capacity and energy consumption of the entire system is not considered. Gu proposed the use of virtual machines for service type allocation, base station association and resource management experiments in medical network physical systems [14]. Facts have proved that Gu's plan is very useful in saving energy. Poghosyan analyzed the frequent usage patterns of household appliances in smart homes in 2017. In 2019, Kang edits the gateway system which can auto-configure intelligent home appliances and provide data for the Internet service provider (ISP) to the cloud for real-time monitoring of network service quality.

Lee uses a virtual gateway to form a master node and a slave node in the customer premises access network and performs data processing in the access network [15]. According to the experimental results, after using the fog computing algorithm, the communication delay is effectively reduced, and the reliability is much improved. However, neither Yu et al. [16] nor Lee et al. [15] considered the compatibility with the existing communication system when deploying the gateway. In 2017, Lohokare proposed an Internet of Things protocol that supports multiple data collection and analysis simultaneously [17] and according to the agreement, a highly integrated automated home system is built. This system can process data from all IoT devices deployed in a particular area. Compared to Kang's study, the system compatibility of Lohokare is significantly higher, but Lohokare's research still needs system deployment cost and stability. Yu uses fog computing combined with geographical distribution to reduce energy consumption in smart home energy consumption, consistent with the research direction of R8. However, they did not consider the cost of deploying the system.

In 2016, Rathore proposed a smart city paradigm based on the Internet of Things' big data analysis system. The system uses the Hadoop ecosystem to simulate the real environment of smart homes, smart cities and other scenes [18]. Although this system is very effective, the system does not take into account the technical reserve capabilities of smart home companies and smart city service providers. As seen from the previously mentioned literature, the existing fog computing and Internet-of-Things resource management technologies mainly aiming at network resources and energy allocation in a specific city and a specific area [16]. Although the fog device has additional computing and storage capabilities, this device cannot provide the same resource capacity as the cloud data center. Therefore, if an ISP wants to achieve the effective allocation of smart home network resources, ISP needs to monitor the user's network resources besides the hardware devices popular in the market. Therefore, IoT device status can better allocate network resources. A platform that combines fog computing nodes and cloud computing after successfully allocating network resources on the client-side can perform resource-efficient processing of IoT big data on an almost real-time basis while providing the cloud with insight and processed data.

3 Research Method

3.1 Existing Smart Home IoT Structure

In the smart home, because the overall complexity of the endpoint elements is relatively low, they usually use the gateway of the Internet of Things in many environments that support the Internet of Things. Although the IoT gateway and Wi-Fi access point are packaged in a physical

device in this article, they realize the IoT function of the networked gateway through software. Before conducting the experimenting, first analyze the current smart home protocol stack, as shown in Fig. 1.

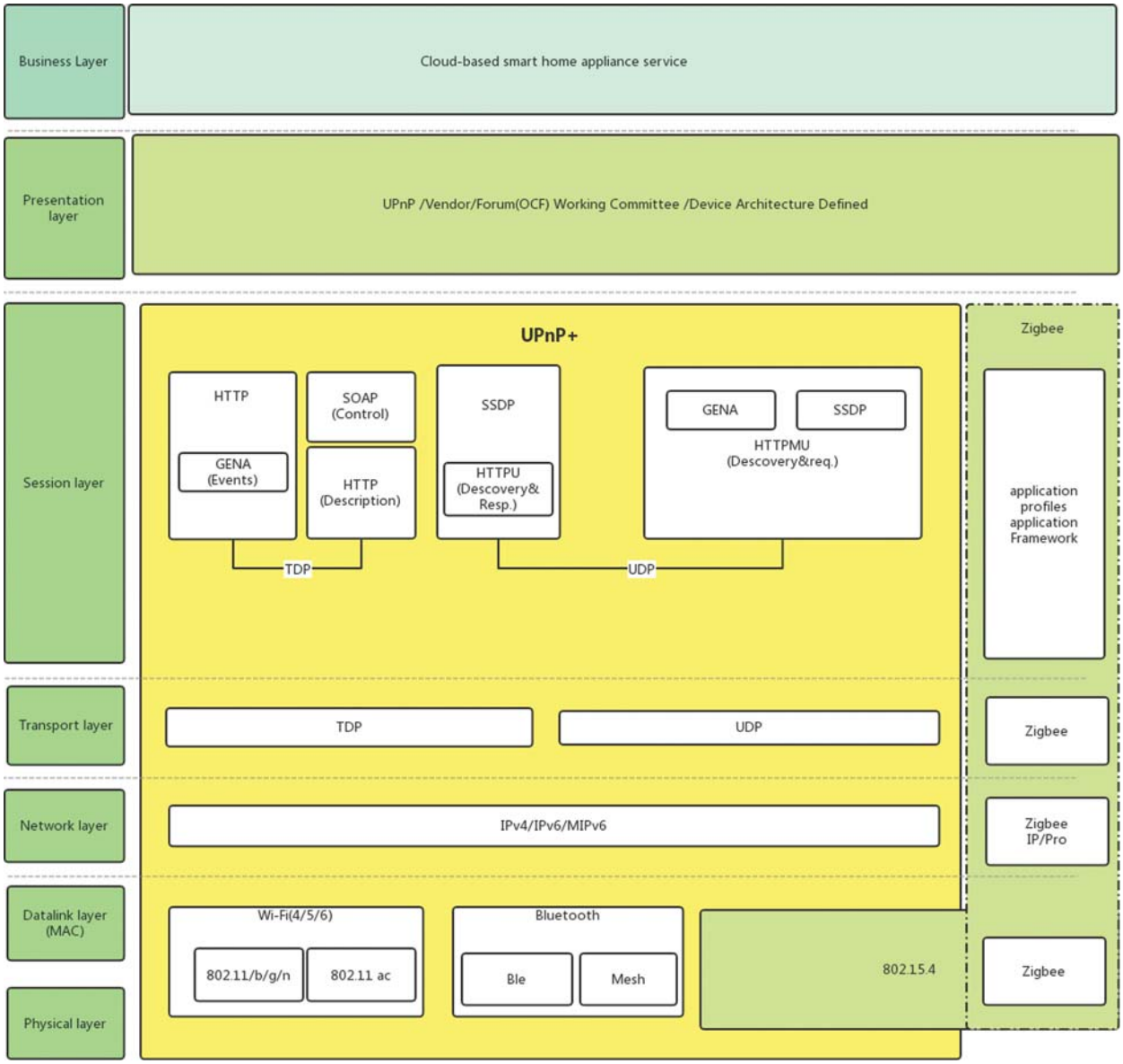

Figure 1: Existing smart home protocol stack

UPnP is one of the mainstream networking processes of smart home appliances. It can automatically detect intelligent home appliances in the home network of users and various services provided by smart home appliances. Any specification based on UPnP and OCF (Open Connectivity Foundation) can be combined with web applications to implement IoT services for other UPnP devices.

After 2015, UPnP extended the cloud function, which makes UPnP usually use WiFi connection in the lower layer. However, the cost of the WiFi module is high. At present, most smart home appliances still use the WiFi4.0 technology that originated in the early 21st century. Many sensors do not have sufficient computing power. Therefore, solutions such as Zigbee and Bluetooth have appeared [19].

Besides, with the improvement of smart home users, many smart appliances need to include image recognition, voice operation and other functions. For example, the refrigerator can judge the storage of ingredients in the box through image recognition. These technologies are difficult to meet by Zigbee's network conditions and Wi-Fi. The price of the module is very expensive. With the increase in connected devices under the trend of automation, connecting all edge devices to the core network will generate an extensive amount of instantaneous data at a specific time, saturating the communication resources of the access network. An enormous amount of initial data does not have an enough value for cloud decision-making or monitoring to make up for the high network costs. Therefore, as the edge device of the smart home IoT system, the IoT gateway at the user's home has many functions to be performed, for example, device connection, device authentication, network security, protocol conversion and device management.

3.2 Existing IoT Network Service Process

The current UPnP network service process refers to Fig. 2.

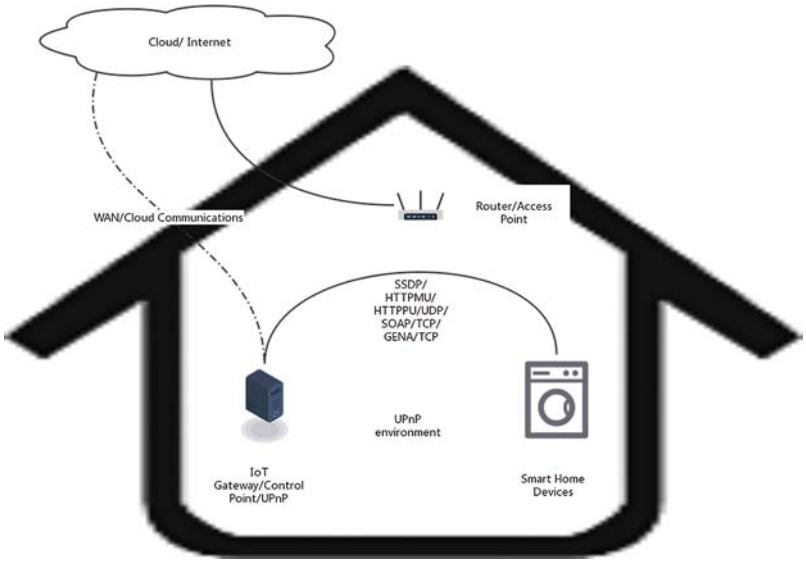

Figure 2: UPnP device control process

When the modern smart home appliances is set up for the first time, the IoT gateway serves as the access point in the user's home and the intelligent home appliances act as the clients assigned IP addresses. When smart appliances join the LAN, the device will search for a dedicated DHCP server or assign a unique address to a group of reserved dedicated addresses [20].

After establishing the connection through the first step, the "discovery" process will start. After it adds the device to the network by user, UPnP allows the use of the Simple Service Discovery Protocol (SSDP) to include the device configuration information and functions and

publish it to other devices on the home LAN to discover the information. Then broadcast HTTP MU SSDP real-time messages to achieve device discovery. Smart home appliances monitor the SSDP messages of other devices on the network in real-time through the SSDP protocol. When the two devices find each other, they will make a master-slave determination. This is because the discovery messages are Unicast via HTTP Unicast (HTTPU) and UDP and SSDP exchange.

In the third step, after devices discover each other, they exchange information supported by each other to achieve a more elaborate device description. The household electrical appliances will transfer the configure information of their master-slave devices with the control terminal in XML format. This information usually includes the manufacturer's representation, device model name, device model, operating status, operating data, etc. Smart home appliances support simple information access protocol to support remote information in the client/server environment.

After the device completes the above three steps, the IoT gateway of the user's home will update the event of the corresponding smart home appliance. Event notification in XML format is compressed and transmitted by the TCP protocol. The control terminal, such as the user's mobile phone and tablet computer, can subscribe to the change of the device status. When the "state variable" of the smart home appliance on the control terminal changes, it sends the new condition to the control device that subscribes to the message.

To more accurately simulate the home network environment in the above two steps, this paper designs the existing smart home network architecture topology (Fig. 3) and builds a new intelligent home topology (Fig. 4) to simulate the intelligent home structure. The topological network is decomposed into three parts from top to bottom by this paper: access part (S1, C1), convergence part (e-level & a-level), edge part (h-level), each level of household appliances forms a node and convergence part of the devices all represent large appliances.

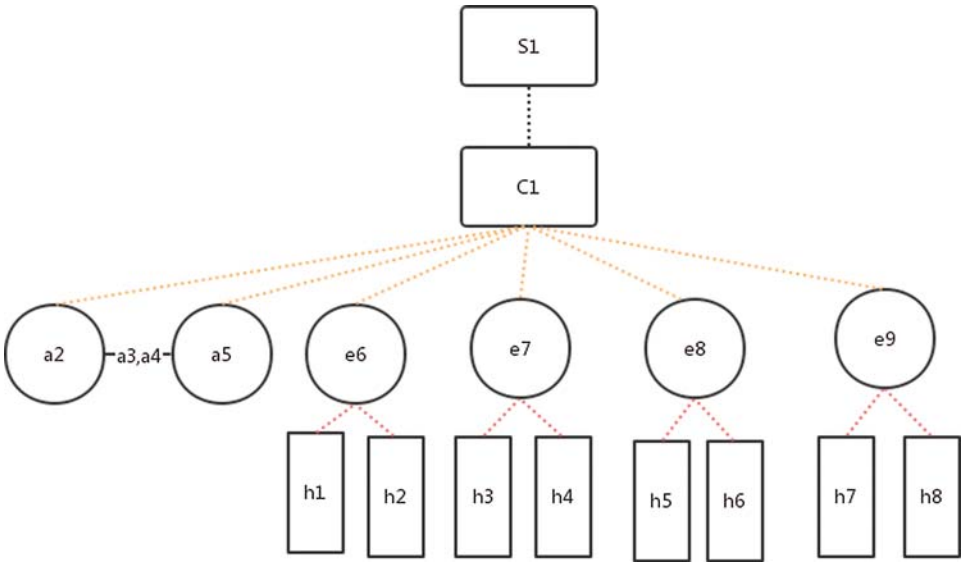

Figure 3: Existing smart home network topology

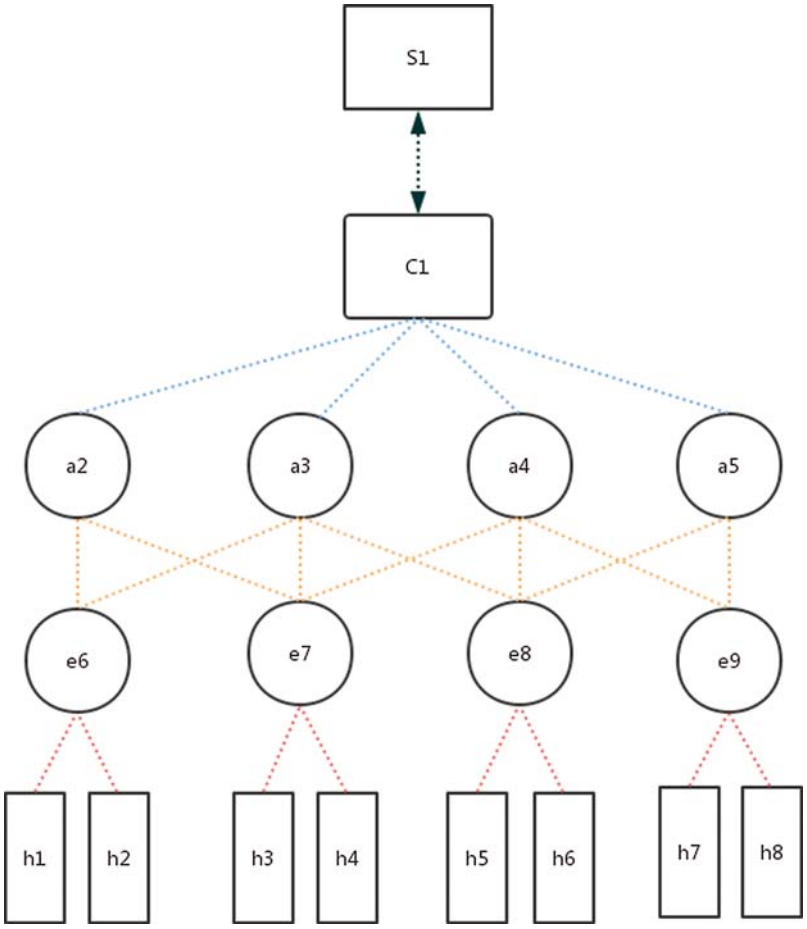

Figure 4: New smart home tree network topology

It limits the network path bandwidth to 3 levels which are represented by blue, yellow and red:

- Blue: 50 Mbps router capacity simulated home network
- Yellow: Link capacity of 20/40 Mbps analog smart home network device
- Red: 24 Mbps link capacity of small sensors simulating smart home

S1 represents the base station of the user's premises network. It is mainly used to upload the data traffic generated by the smart home and provide users with services such as voice, video and home appliance status transmission.

C1 is the router in the user's home, where it mainly plays the role of connecting home appliances to the core network and assumes the function of the IoT gateway through the design of software-defined network (SDN).

A2, a3, a4, a5, e6, e7, e8 and e9 represent smart home electronic devices that provide unique services. According to various intelligent home Wi-Fi designs, different smart homes provide quick services according to different bandwidths.

It will not link Class A devices with other appliances. Class H appliances are mainly composed of multiple sensors. To reduce the costs, home appliance provides rarely set too many

network settings on Class H appliances. It will link class E Home appliances with Class H appliances to provide users with more types of linkage.

When smart home appliances join the home LAN for the first time, the program in this article will start the topology detection thread to determine the adjacency relationship between the home network devices. After the controller device in the home LAN receives the packet in message, the message header will be parsed to get the corresponding address information and header fields of Layer 2 and Layer 3. Since the Ethernet table-based forwarding mechanism of the MAC table cannot support the loop topology, whenever a broadcast packet appears in the network, it will cause a broadcast storm, so pass the control the device S1 implements the proxy response of the Arp request. The controller records the mapping relationship between the IP address and the MAC address of the host in the network. After parsing the Arp request, it encapsulates the required MAC address into the Arp response and returned to the requesting end.

Therefore, in the smart home network constructed in this paper, the information in the data packet needs to be IP or Arp information judgment. If the information is Arp and broadcast messages, the controller needs to check the topology information and send the Arp request to each smart home device. Conversely, if the message does not belong to a broadcast message, we need to check the topology information and distribute the Arp response packet to the requesting end. After the message is inspected as IP by controller, the controller will record the host's IP address, the connected home electronic device and the service port number, check the host record, and find the home electronic device connected to the source host and the destination host. The Ryu controller provides a topology discovery mechanism that can get the link relationships of switches in the network, generating a topology graph data structure.

This article separately constructs the existing home IoT architecture, and the improved home IoT architecture and adjust the size of the packet sent by the host and simulate different services provided by different smart homes such as intelligent home status command upload, intelligent home voice service and intelligent home image recognition service. It simultaneously monitors the link capacity of devices in different architectures to achieve the performance comparison of different structures.

4 Data Analysis

After completing the architecture design through Ryu, this article uses multiple a-level and e-level appliances to send data packets to S1 and simultaneously to detect the average bandwidth of S1. The results are shown in Fig. 5.

In Fig. 5, the blue line represents the new tree topology and the orange line represents the existing smart home topology. When the number of hosts providing services is one and the services are the same, but as the number of hosts providing services increases, the average bandwidth of the tree topology decreases. The rate is lower than the existing smart home topology. However, the performance of the tree topology will gradually decrease as the bandwidth pressure increases, but it still improves the performance by 20% compared to the existing topology. When the bandwidth is the same, the bandwidth consumption of the tree topology is lower and the bandwidth resources saved are 1/5 times more than the existing topology.

In comparison, a tree topology smart home structure can provide better disaster tolerance and more reasonable bandwidth allocation. When a certain level of intelligent home equipment loses network connection, it is less susceptible.

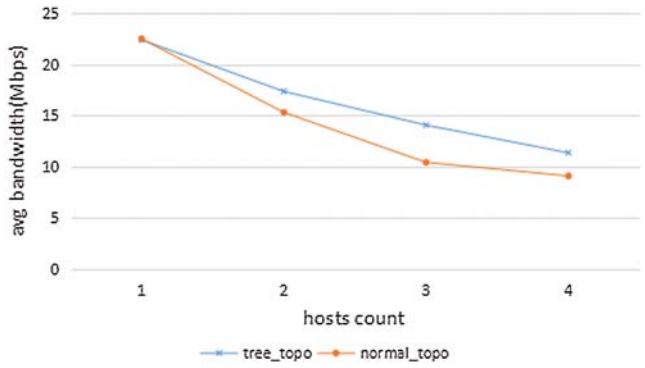

Figure 5: Comparison of bandwidth performance of different topologies

Therefore, we have transformed the tree topology and added a QoS guarantee mechanism. This measure is mainly for the growing voice and image demand of smart home appliances. When users use smart homes, they often generate a lot of voice information and image information. Although this information will be decomposed into smaller data grams and then sent to the core network one by one through C1. Besides, the transmission of other services also brings constraints [21]. In this article, first, different services such as voice/image are allocated to independent it earmarks ports 8080 and home appliance status and home environment services for ports 8899 and 12345.

To compare the performance of the tree topology under the QoS mechanism, this paper first uses the form of randomly sending data packets to test the performance of the smart home tree topology without the QoS mechanism.

Port 8080 in Fig. 6 is individually responsible for services with high traffic intensity such as voice and image whereas ports 8899 and 12345 are responsible for other services such as smart home status and home environment status.

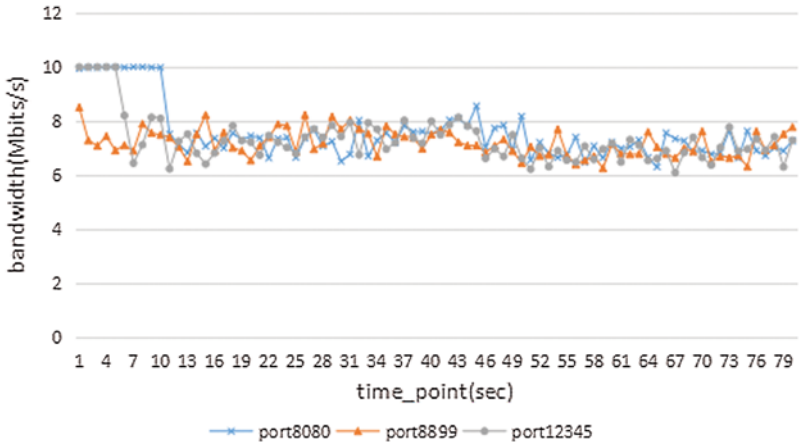

Figure 6: Topology network bandwidth of smart home tree without QoS guarantee

It can be seen from the data in Fig. 6 that although the network bandwidth consumption rate of the tree topology found in Fig. 5 is lower when facing the high traffic intensity brought by the

voice and image data in port 8080, the bandwidth is only 6–10 Mbits. This will significantly extend the transmission delay for voice and image information which cannot guarantee the transmission speed of information. If the home appliance supplier wants to improve the user's smart home experience, the home appliance supplier can only increase the network cost of smart home appliances or the network conditions of the user's home. If this comes true, it will significantly reduce the profit margins of the home appliance industry and the weak voice/image interaction experience due to the decline in network fees or network environment, resulting in low motivation for users to use smart home appliances. Therefore, this article is particularly crucial for the QoS limitation of the tree topology.

It can be seen in Fig. 7 that the bandwidth of port 8080 is increased from 6 to 10 Mbits in Fig. 6 to 10 to 30 Mbits and the bandwidth fluctuations in ports 8080, 8899 and 12345 are more obvious than those in Fig. 6 which is because existing smart home adopts the transmission method of TCP protocol. When the traffic intensity is too high, the TCP protocol will suppress the traffic sender and allow it to suspend sending data packets to avoid an enormous amount of link congestion which will cause a brief "network disconnection" case (Kurose, 2018).

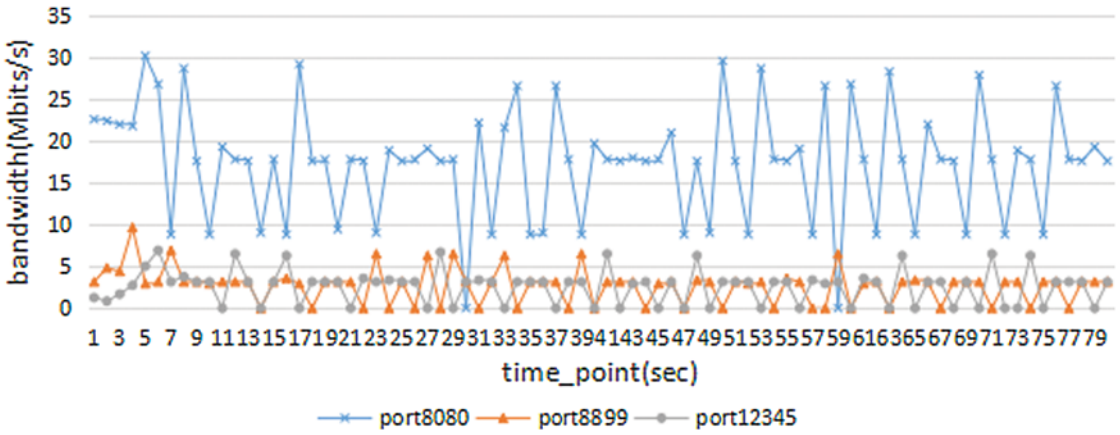

Figure 7: Topology bandwidth of smart home tree after QoS guarantee

This article finds that even if the QoS guarantee is set by configuring C1, the bandwidth of port 8080 will still drop to 0 at the 30 and 59 s. This situation is very likely to affect the user experience because the immediacy of the voice will cause the user and port 8899 services provided by 12345 need to upload an enormous amount of data to the cloud to perceive obvious problems. The user is not the first recipient, so the bandwidth of 0–10 Mbits is enough.

To verify the impact of the brief "network disconnection" in Fig. 7 on the use of home appliances and to solve the actual use of smart homes, many home appliances are set far from the router where it will make the network environment worse such as smart bathroom and the smart balcony. Equipment in these two rooms have to face the problem of high dropout rate all the year-round and far from the stable network environment of home appliances in the living room. Therefore, this article conducted a performance verification of the dropout guarantee.

In Fig. 8, blue represents the bandwidth of the tree topology and orange represents the bandwidth of existing appliances. In this article, after the start of monitoring 8 seconds, the network of a-level, e-level and h-level devices in the topology is disconnected. In the period of

8–9 s, the bandwidth of the two topologies dropped rapidly, but the difference is that the bandwidth of the tree topology returned to the state of 7 s after two seconds. At the same time, this article conducted a network test on the disconnected home appliances and found the network services of all home appliances are regular. However, after the home appliance in the existing topology is disconnected from the core network, the network bandwidth suddenly drops to 0 Mbps. I do not connect the home appliance to the core network until the 35 s network is restored by Pr-set.

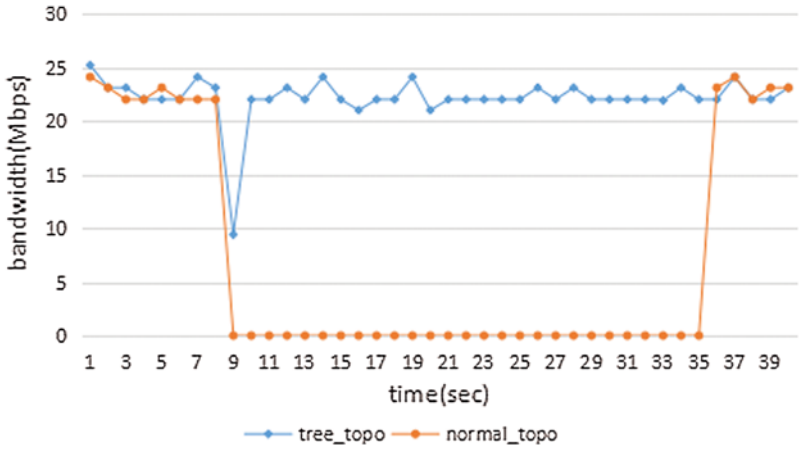

Figure 8: Comparison of offline disaster recovery

When users use smart home appliances, a-level and e-level home appliances are sold at high prices and home appliance suppliers will install better-performing bandwidth environments. However, for h-level home appliances, power consumption and profit margins lead to frequent disconnection. Besides, since h-level home appliances are usually composed of multiple sensors, the number of h-level home appliances in a user's home is often the largest. Still, the data uploaded by them can only be processed in the cloud before it can combine them with voice or images for intelligent services, so they are difficult to be perceived by users.

5 Conclusion

This article first analyzes the existing smart home network. The analysis includes network protocols and network logic, which also plays an excellent reference role in constructing the intelligent home tree topology in this paper. Secondly, this article compares the existing smart home network topology with the intelligent home tree topology through three Mininet simulation experiments: Bandwidth performance experiments, topology operation experiments and dropout guarantee experiments.

We find it that the proposed intelligent home tree has a slightly improved bandwidth utilization rate compared with the existing smart home structure. Still, the improvement effect is not apparent and with the access to home appliances, the improvement of equipment will further narrow the gap between the two topologies. In the state of high traffic intensity, the smart home tree topology will face the situation of reduced service quality, but this can be circumvented by adding software QoS settings on the router. When facing high traffic intensity or a poor network environment, the network performance of the smart home tree topology is significantly better.

Although individual devices are disconnected from the network, their suitable disconnection guarantee mechanism can restore the network device shortly. Compared with the existing smart home network topology, it is a significant improvement. After it disconnects the home appliance, they can restore the connection without being noticed by the user. The smart home tree topology does not bring any hardware changes in hardware equipment. It is only necessary to make software changes to the underlying logic of the home gateway and smart home appliance equipment. This network design makes the R&D cost of home appliances with no increase in cost. The corresponding change in logic of the software can refer to the R12 code.

This paper limits the number of hosts used in bandwidth performance testing. Although it reflects a particular trend, data reliability can still be achieved by optimizing algorithms to simplify manual operations to explode the number of hosts in the experiment. Besides, this article concerns the safety of home appliances. Without in-depth analysis, it connects the potential DDoS risk after home appliances in parallel is still a problem that the smart home industry needs to pay attention to and solve. The block-chain solution proposed by R10 is an excellent method. Still, there are many difficulties of application caused by factors such as insufficient electronic integration of home appliances, and small profit margins of home appliances is also a significant challenge that limits the continued iterative upgrade of smart home appliances.

Acknowledgement: The authors are grateful to the reviewers for their time and review.

Availability of Data and Materials: The data used for the findings of this study is available upon request from the corresponding authors.

Funding Statement: This work is supported by Soongsil University research funding.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Gram-Hanssen and S. J. Darby, "Home is where the smart is? Evaluating smart home research and approaches against the concept of home," *Energy Research & Social Science*, vol. 37, pp. 94–101, 2018.
[2] L. Kurkinen, "Smart homes and home automation," *Berg Insite M2M Research Series*, vol. 16, pp. 1–4, 2016.
[3] K. Adhinugraha, W. Rahayu, T. Hara and D. Taniar, "On internet-of-things gateway coverage expansion," *Future Generation Computer Systems*, vol. 107, pp. 578–587, 2020.
[4] B. K. Sovacool and D. D. F. Del Rio, "Smart home technologies in europe: A critical review of concepts, benefits, risks and policies," *Renewable and Sustainable Energy Reviews*, vol. 120, pp. 1–20, 2020.
[5] A. Yassine, S. Singh, M. S. Hossain and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems*, vol. 91, pp. 563–573, 2019.
[6] S. S. Gill, I. Chana, M. Singh and R. Buyya, "CHOPPER: An intelligent qos-aware autonomic resource management approach for cloud computing," *Cluster Computing*, vol. 21, no. 2, pp. 1203–1241, 2018.
[7] H. X. Li, W. J. Li, S. G. Zhang, H. D. Wang and Y. Pan, "Page-sharing-based virtual machine packing with multi-resource constraints to reduce network traffic in migration for clouds," *Future Generation Computer Systems*, vol. 96, pp. 462–471, 2019.
[8] W. Peng, G. H. Dong, K. Yang and J. S. Su, "A random road network model and its effects on topological characteristics of mobile delay-tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2706–2718, 2013.

[9] X. Su, X. C. Liu, J. C. Lin, S. M. He, Z. J. Fu *et al.,* "De-cloaking malicious activities in smartphones using http flow mining," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 6, pp. 3230–3253, 2017.

[10] R. X. Sun, J. W. Xi, C. Y. Yin, J. Wang and G. J. Kim, "Location privacy protection research based on querying anonymous region construction for smart campus," *Mobile Information Systems*, vol. 3682382, pp. 1–11, 2018.

[11] B. Yin and X. T. Wei, "Communication-efficient data aggregation tree construction for complex queries in IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.

[12] X. M. Huang, R. Yu, J. W. Kang, Z. Q. Xia and Y. Zhang, "Software defined networking for energy harvesting internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1389–1399, 2018.

[13] R. Deng, R. Lu, C. Lai and T. H. Luan, "Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing," in *IEEE Int. Conf. on Communications*, London, UK, pp. 3909–3914, 2015.

[14] L. Gu, D. Zeng, S. Guo, A. Barnawi and Y. Xiang, "Cost efficient resource management in fog computing supported medical cyber-physical system," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 1, pp. 108–119, 2015.

[15] W. Lee, K. Nam, H. G. Roh and S. H. Kim, "A gateway based fog computing architecture for wireless sensors and actuator networks," in *IEEE 18th Int. Conf. on Advanced Communication Technology*, PyeongChang, South Korea, pp. 210–213, 2016.

[16] L. Yu, T. Jiang and Y. Zou, "Fog-assisted operational cost reduction for cloud data centers," *IEEE Access*, vol. 5, pp. 13578–13586, 2017.

[17] J. Lohokare, R. Dani, A. Rajurkar and A. Apte, "An iot ecosystem for the implementation of scalable wireless home automation systems at smart city level," in *IEEE TENCON Conf.*, Penang, Malaysia, pp. 1503–1508, 2017.

[18] M. M. Rathore, A. Ahmad and A. Paul, "IoT-based smart city development using big data analytical approach," in *IEEE Int. Conf. on Automatica*, pp. 1–8, 2016.

[19] Y. Cui and H. Lee, "A novel digital device monitoring system using UPnP cloud architecture," in *Int. Conf. on Engineering Technologies and Big Data Analytics*, Bangkok, Thailand, pp. 69–71, 2016.

[20] M. K. Shafique, N. K. Baloch, M. I. Baig, F. Hussain, Y. B. Zikria *et al.,* "NoCGaurd: A reliable network-on-chip router architecture," *Electronics*, vol. 9, no. 2, pp. 1–22, 2020.

[21] F. B. Yahya, C. J. Lukas and B. H. Calhoun, "A top-down approach to building battery-less self-powered systems for the internet-of-things," *Journal of Low Power Electronics and Applications*, vol. 8, no. 2, pp. 1–13, 2018.