An Architecture of a Network Controller for QoS Management in Home Networks with Lots of IoT Devices and Services

Daisuke Kotani
Academic Center for Computing and Media Studies
Kyoto University
Kyoto, Japan
kotani@media.kyoto-u.ac.jp

***Abstract*—More and more IoT services are introduced in home, and they will consume many network resources in home networks including their uplink to the Internet, but sometimes the resources are insufficient to host all services. Traditionally, QoS control is applied to handle such situation by prioritizing important traffic. However, in the context of IoT, it is hard to find important traffic because it depends on the context that is greatly different among homes, such as services and the life of the people living at the home. In addition, usually there is no administrator who can oversee and configure the whole system including IoT devices and services in the home networks and the context of the homes. This paper proposes an architecture of the network controller that automatically estimate and prioritize important traffic under such situation. The controller under the proposed architecture provides three types of interfaces to ask each party, IoT devices, service providers, and users, for the input about its information. Then, the controller automatically estimates the important traffic based on the inputs and applies the estimated policy to the network in a centralized way. This paper also shows points of view of designing each interface according to the information that each party knows.**

***Index Terms*—IoT, Controller, QoS, QoE, Home Network**

I. Introduction

There are great expectations of IoT (Internet of Things) enabled services to enhance people's life in various fields, such as smart city, manufacturing, transportation, and many other fields [1]. Smart home [2] is one of fields that gather attention as an application of IoT. The applications of the smart home range from monitoring and visualization of various data captured by embedded sensors in home such as energy management [3] and human behavior monitoring for safety [4], to control various home appliances for optimizing energy consumption and improving human life [5], [6]. As the population of elderly grows, robots in home have also much attention for healthcare and assistance to elderly in home [7].

Nowadays various types of IoT devices in home needs to communicate with cloud services to achieve their roles. Examples include robots that work with functions provided as cloud services so called cloud robotics [8], wearable devices to monitor health of each person [9], activity recognition using data sensed by many devices [10].

As a result, more traffic will be transmitted between home and various cloud services when more IoT devices and services are introduced in home. However, quality of Internet connection from home is sometimes not enough to support various services provided at home simultaneously. Although it is reported that average download throughput is tens of Mbps [11], which may be enough for some applications used in home, upload throughput is also important for IoT applications because sensing data must be uploaded to the clouds. In addition, the throughput to the Internet and within the network becomes sometimes low due to temporal congestion and bad wireless conditions.

To keep quality of life of people living with lots of IoT devices and services under such insufficient network resources, it will be important to manage traffic in home networks so that services that have huge impact on people's life are less affected by such insufficient resources. Traditionally, QoS mechanisms are introduced to prioritize important traffic in such situation, like IntServ [12], DiffServ [13], traffic engineering, and more recently, Software Defined Networking [14]. We may be able to use these technologies for home networks.

What is problematic to apply QoS mechanisms to home networks with many IoT devices and services is to find important traffic for maintaining quality of life of people living at the home. It is readily understood that important traffic depends on the context, like people who are in home and activities of the people. If no one is in home, traffic to deliver pictures taken by surveillance cameras to the cloud will have high priority because of home security, and traffic from robots that interacts with people has less priority than those from surveillance cameras because no one uses it. On the other hand, when a person directly interacts with robots, such as talking with robots, traffic from robots usually have higher priority than those from surveillance cameras, because response delay to the person have negative impact on the quality of life of the person using the robot.

In addition, no one has enough knowledge to find and configure important traffic for people living in each home because of diversity of IoT devices and services and lack of skilled administrators in each home. IoT devices and device manufactures know the details of the devices like the amount of traffic and intervals of sending data, but the importance for the services is unknown to them. IoT service providers know the importance of data sent or received by devices, but they usually have no knowledge whether how much importance their services currently have from the viewpoint of the people's life. The people living at home may know the importance of services for their life, but the details of services and devices are often hidden from the people using them.

This paper proposes an architecture of a controller that manages a home network with lots of IoT services in a centralized way, for increasing quality of life of the people who are in the home. It is assumed that the network can be dynamically configured in a centralized way, e.g. the network is controlled by SDN using OpenFlow and the controller behaves as an SDN controller. The controller provides three types of interfaces to accept input from each party involved, one for IoT devices, another for service provides, and the other for users (people in home). The controller automatically estimates the global priority of each flow from the inputs, and configures networking devices like wireless access points, switches and CPE (Customer Premises Equipment) according to the global priority and the network state.

The contributions of this paper are summarized as follows:

- We have proposed an architecture of the controller of a home network with many IoT devices and services without administrator who knows the whole system and the context, which will be a common limitation in many home networks.
- We have provided points of view of designing interfaces for IoT devices, service providers, and people who are in the home, with consideration of capabilities that they can provide data.

II. Related Work

There are lots of platform and standards for IoT devices, IoT data exchange, and interoperable platform of IoT devices and services. FIWARE [15] and W3C WoT (Web of Things) [16] are examples of them. FIWARE is originally designed for smart city to collect data from sensors in the city and distribute data to various applications. W3C Web of Things aims for more general IoT platform to make various IoT devices and services interoperable. Both FIWARE and W3C WoT has a standard specification to describe the capability of devices, such as data types that each device can sense and provide, as well as metadata of each device. The proposed architecture makes use of the same model as much as possible so that IoT device manufacturers do not have to learn various models to describe the device capabilities.

Some platform focused on specific use cases of IoT, such as smart homes [2].They aim to support complex tasks like message exchange between devices, interaction with cloud services, device discovery, etc. If network resources are insufficient to host these platforms, some support will be needed at the network layer to smoothly operate these platforms, preferably by coordinating these platforms and networks.

In the context of IoT, QoS can be regarded more broader than QoS in traditional networks like latency and jitter [17], [18]. Metrics of QoS in IoT include accuracy of data and timeliness of data delivery. Based on this insight, many algorithms are proposed to implement QoS for IoT environments [17]–[20]. Our focus is how to use these QoS mechanisms rather than improvement of implementation of the QoS mechanisms. In IoT, there will be lots of services and requirements to acquire and transmit data vary in each service. So, to make use of these QoS mechanisms efficiently, there is a need to control a network with enough knowledge of IoT devices and services.

One thing we need to care from the network viewpoint is that many IoT devices are sometimes tightly coupled with cloud services. Robots, an example of IoT devices that are expected to be everywhere in the near future, sometimes communicates with cloud services to provide their features, so called Cloud Robotics [8]. Rospeex [21] is an example of cloud robotics platform for human-robot spoken dialogue. Rospeex provides an API to retrieve text of speech and to output audio of text, and it uses cloud services for speech recognition and synthesis. We need to consider such characteristics, that is, to retrieve data from IoT devices, the devices communicate with services on the cloud by themselves to provide data.

III. Proposed Architecture

A. Target Environment and Assumption

Figure 1 shows the environment where we assume the proposed architecture is applied.

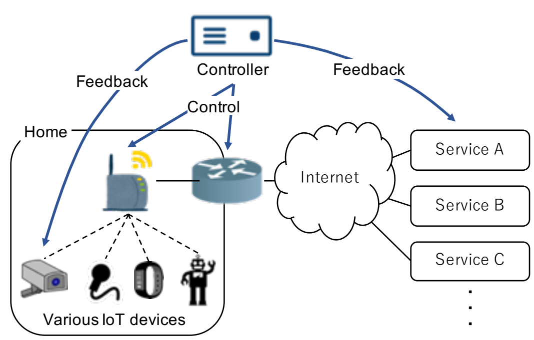

Fig. 1. Assumption of environment and use case of the proposed architecture.

There are various IoT devices in a home, and these devices are accessed from one or more cloud services over the Internet. The proposed architecture is implemented as a controller that configures QoS parameters on the networking devices in home networks. The controller optionally gives feedback to the devices and services so that they can change quality of data according to the network state to improve the quality of the IoT services.

In home networks, we assume that there is no entity like system administrators who know and optimize systems as a whole, and that there are three parties involved in the use of IoT services on home networks as follows.

IoT device (device manufactures) IoT device manufacturers provide IoT devices to the users who uses the devices with services provided by service providers. Some IoT devices implement their features in collaboration with cloud services provided by the manufacturers or third-party, like cloud robotics. Data and functions on the devices are accessed from the service providers that the users have selected. Examples include microphone, camera, wearable sensors, environmental sensors, robots, and home appliances.

Service Provider Service providers offer services to the users using data and functions on various IoT devices owned by the users. Services retrieve data from one or more devices, process the data, and control some of devices. Examples include surveillance services, remote control of home appliances, health monitoring and emergency calls and dialoges with robots. Importance of data differs among services. For example, a surveillance service may usually process pictures taken by camera to find suspicious person, but if network resources are insufficient to transmit the pictures, the service may use audio recorded by microphone instead of the pictures to find the abnormal status. A health monitoring service may use data sensed on different wearable devices at different frequency depending on the state of the users monitored.

Users Users are the people living at the home. They own IoT devices in their home and use services offered by various service providers. Importance of services depends on the state of the users and their home. For an example, a surveillance service is less important if one of legitimate people are in home because he or she can perceive the abnormal status by themselves. Instead, services that directly interact with him or her may be more important to improve the experience of the services.

B. Architecture Overview

Figure 2 shows an overview of the proposed architecture of the controller.

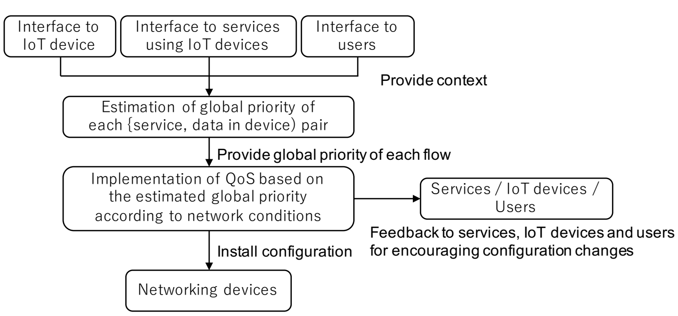

Fig. 2. An overview of the proposed architecture.

C. Interfaces to IoT Devices / Services / Users

The first step is that the controller obtains context information related to IoT devices, services and users. To receive inputs, the controller has three types of interfaces that are suitable for each party (IoT devices, services and users). Each interface is designed according to the following principle.

Interface to IoT Devices The interface to the devices is to obtain what kinds of data a device can send and receive. This aim is very similar to the abstraction of the devices in existing IoT platforms such as FIWARE [15] and WoT [16], which is expressed as a set of (property/attribute, type of its value) pairs, so we use the same model with them so that inputs to FIWARE or WoT can be reused as much as possible. This information does not depend on the services and the users, so the devices are assumed to automatically provide their information via this interface.

In addition to the list of properties/attributes and their types, for each property/attribute, the controller needs to know the cloud services that the devices communicate with to provide and process data (Coflow [22] in the context of IoT, so we call IoT Coflow hereafter), because the objective of applying QoS cannot be achieved without consideration of such IoT Coflow.

Interface to Services The interface to the services is to obtain what kind of data in a device a service access. The service registers a list of properties/attributes in devices the users have, along with the endpoint of the service (IP address, URL, etc.) that communicates with the devices.

As described in Section III-A, the importance of data may depend on the service, that is, some data may be less important than others to provide the service. So, the service also needs to provide such importance as a priority of each property/attribute.

Interface to Users The interface to the users is to obtain which services are important for the users' life. So, the users are expected to provide a list of (service, priority for their life) through this interface.

D. Estimation of Global Priority of Each (Service, Data in Device) Pair

The second step is to estimate the global priority of each (service, data in device) pair for users' life from three types of inputs from the interfaces. The global priority is the priority that is assigned from the viewpoint of integrating all IoT devices and services used by the people living in a home.

The basic policy of this estimation is to give more preference on services that the users think important, and on (service, data in device) pair that are important to provide services to the users in a good quality.

There is a tradeoff between two strategy of the estimation. One is to maximize the number of services that the users can be offered at the same time. To achieve this, (service, data in device) pairs that have high priorities provided by the services have high global priorities. The other is to maximize the quality of each service that the users can be offered at the same time. This may be achieved by assigning high priorities to (service, data in device) pairs of the important services.

E. Implementation of QoS Based on The Estimated Global Priority

The third step is to apply the global priority estimated at the previous step to the network traffic considering the network state. In this step, we assume that we reuse existing many sophisticated algorithms for QoS shown in Section II, as well as simple greedy algorithms that packs the traffic into the network in the highest priority order. After the configuration is decided, the controller configures networking devices to apply QoS to each traffic.

Another role of this step is to feedback the results of the estimation and the implementation to the devices and the services. Although this feedback and the use of this feedback at the devices and the services are optional, we expect them to use this feedback to change the quality and priority of data exchanged between them to improve the quality of each service provided to the users if possible. For example, a surveillance service stops using pictures taken by camera and uses audio captured by the microphone because of the feedback of insufficient network resources from the controller and trying to continue to provide the services as much as possible. After the services and the devices change their behavior, they provide a new information through the corresponding interface at the controller, and the controller updates the network configuration with new global priorities.

IV. Prototype Implementation

We have developed the first prototype controller based on the proposed architecture with limited capabilities that make an admission control of flows at one OpenFlow switch. The interfaces to IoT devices, services and users are designed as RESTful API, and the estimation component and the implementation component has its own RESTful API so that we can easily replace these components to better ones. The estimation algorithm is designed to maximize the number of services that users can use, because unavailability of services may greatly decrease the quality of life of users.

V. Concluding Remarks

This paper proposes an architecture of the controller that manages QoS in home network with lots of IoT devices and services so that users can get a good experience of using many services. One of important features is that the proposed architecture is designed under assumption that no administrator that have good knowledge of the whole network and systems, which will be realistic in many homes. The automatic estimation of global priority from inputs of three parties, IoT devices, services, and users, will contribute to derive the necessary policy for QoS in the home networks.

Future work includes extensive evaluation of interfaces from the perspective of real service developments in a realistic scenarios, as well as designing more sophisticated algorithms for the estimation of global priority and integration of sophisticated QoS implementation algorithms.

Acknowledgment

The author would like to thank Hitoshi Morioka of SRC Software, Satoru Momiki, and members of ACCRA (Agile CoCreation of Robots for Ageing) project for their valuable comments and assistance. This work is partly supported by the Commissioned Research of National Institute of Information and Communications Technology.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[2] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, and C.-H. Lung, “Smart home: Integrating internet of things with web services and cloud computing,” in *IEEE CloudCom 2013*. IEEE, 2013, pp. 317–320.

[3] D.-M. Han and J.-H. Lim, “Smart home energy management system using IEEE 802.15. 4 and zigbee,” *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1403–1410, 2010.

[4] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, and T. Porcheron, “Monitoring behavior in home using a smart fall sensor and position sensors,” in *1st Annual International IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology. Proceedings (Cat. No.00EX451)*, 2000, pp. 607–610.

[5] J. Choi, D. Shin, and D. Shin, “Research and implementation of the context-aware middleware for controlling home appliances,” *IEEE Transactions on Consumer Electronics*, vol. 51, no. 1, pp. 301–306, Feb 2005.

[6] K. C. Sou, J. Weimer, H. Sandberg, and K. H. Johansson, “Scheduling smart home appliances using mixed integer linear programming,” in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, Dec 2011, pp. 5144–5149.

[7] K. Yamazaki, R. Ueda, S. Nozawa, M. Kojima, K. Okada, K. Matsumoto, M. Ishikawa, I. Shimoyama, and M. Inaba, “Home-Assistant Robot for an Aging Society,” *Proceedings of the IEEE*, vol. 100, no. 8, pp. 2429–2441, Aug 2012.

[8] J. Kuffner, “Cloud-Enabled Robotics,” in *2010 IEEE-RAS International Conference on Humanoid Robotics*, Dec 2010.

[9] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci, and S. Andreescu, “Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing: Opportunities and challenges,” in *IEEE SCC 2015*, June 2015, pp. 285–292.

[10] F. Cicirelli, G. Fortino, A. Giordano, A. Guerrieri, G. Spezzano, and A. Vinci, “On the Design of Smart Homes: A Framework for Activity Recognition in Home Environment,” *Journal of Medical Systems*, vol. 40, no. 9, p. 200, Jul 2016.

[11] M. Isla, “The World’s Internet Speeds Increased More than 30You Keeping Up?” http://www.speedtest.net/insights/blog/global-speed-2017/, accessed: 2018-07-31.

[12] R. Braden, D. Clark, and S. Shenker, “Integrated Services in the Internet Architecture: an Overview,” June 1994, RFC1633. [Online]. Available: http://tools.ietf.org/rfc/rfc1633.txt

[13] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. . Weiss, “An Architecture for Differentiated Services,” December 1998, RFC2475. [Online]. Available: http://tools.ietf.org/rfc/rfc2475.txt

[14] M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, “PolicyCop: An Autonomic QoS Policy Enforcement Framework for Software Defined Networks,” in *IEEE SDN4FNS 2013*, Nov 2013, pp. 1–7.

[15] “FIWARE,” https://www.fiware.org/.

[16] W. W. W. Consortium, “Web of Things at W3C,” https://www.w3.org/WoT/.

[17] L. Li, S. Li, and S. Zhao, “QoS-Aware Scheduling of Services-Oriented Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1497–1505, May 2014.

[18] R. Duan, X. Chen, and T. Xing, “A QoS Architecture for IOT,” in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Oct 2011, pp. 717–720.

[19] S. Abdullah and K. Yang, “A QoS aware message scheduling algorithm in Internet of Things environment,” in *IEEE OnlineGreenComm 2013*, Oct 2013, pp. 175–180.

[20] T. Tachibana, T. Furuichi, and H. Mineno, “Implementing and Evaluating Priority Control Mechanism for Heterogeneous Remote Monitoring IoT System,” in *Adjunct Proceedings of MOBIQUITOUS 2016*. ACM, 2016, pp. 239–244.

[21] K. Sugiura and K. Zettsu, “Rospeex: A cloud robotics platform for human-robot spoken dialogues,” in *IEEE/RSJ IROS 2015*, Sept 2015, pp. 6155–6160.

[22] M. Chowdhury and I. Stoica, “Coflow: A Networking Abstraction for Cluster Applications,” in *ACM HotNets-XI*. ACM, 2012, pp. 31–36.