A Mitigation Technique for Interference of Heterogeneous Networks for the IoT Device Domain

Seung-Jun Yu, Won-Seok Lee, Sung-Soon Park and Hyoung-Kyu Song*

uT Communication Research Institute, Sejong University, Seoul, Republic of Korea

*Corresponding Author: songhk@sejong.ac.kr

Extended Abstract/Poster Paper

Abstract – In Internet of Things (IoT) service systems, devices are connected to share data. The connections among the devices are implemented by short range, low power communication technologies such as Bluetooth, ZigBee, Z-Wave, Wi-Fi, etc. Since most of the technologies use unlicensed frequency band, interference between heterogeneous networks in the service systems can have a serious problem. IoT platforms like Open Connectivity Foundation (OCF) and oneM2M define common service layer to reduce cost for development of new IoT service applications. In architecture of oneM2M, the middle layer for gateways is defined to connect the IoT server to the networks of device domain. This position of middle layer gives the oneM2M gateways an opportunity to mitigate the interference. In this paper, an interference mitigation technique using the gateway position is presented.

Keywords: IoT, oneM2M, heterogeneous network, ZigBee, Bluetooth

2 IoT communication technologies

The communication technologies for the IoT devices have several common features [1]. The features are that the hardware modules supporting the technologies are small, the technologies consume low power, mobile devices are supported, and networks using the technologies are scalable. Wi-Fi, Bluetooth, and ZigBee belong to the technologies and these are used mostly than other technologies. Another common feature of the three technologies is that 2.4 GHz ISM frequency band is used for operation. This common operation band incurs an interference problem when device networks implemented by different technologies are in dense environment [2]. Since the increase of the IoT devices is expected, the interference between the heterogeneous networks is an important problem.

3 Architecture of oneM2M

The oneM2M standard defines two domains in architecture. Fig. 1 shows the architecture. The field domain is composed of IoT devices and a gateway. The Application Dedicated Nodes (ADN) and the Application Service Nodes (ASN) are nodes for the devices. The ASN is different from ADN in that the nodes have Common Service Entities (CSE) of IoT platform layer. The Middle Node (MN) is a node for the IoT gateway.

Field Domain

Infrastructure Domain

IoT devices

IoT gateway

IoT server

User

Fig. 1: Architecture of oneM2M

The infrastructure domain is composed of an IoT server and a user. The Infrastructure Node (IN) is a node for the server. In this figure, two device nodes are connected directly to the...
server node while others are connected through the gateway node. The device nodes connected through the gateway can be managed by the gateway and this paper presents the way to manage the heterogeneous device networks for interference mitigation.

4 Arbitration to mitigate interference

If the IoT gateway is used for all communications between the server and the devices, the gateway can keep information for the composition of the networks. Fig. 2 shows the process of the gateway for arbitration. When a new container is connected, the gateway registers the container in internal database according to the type of the network. Then the gateway enters into decision process for arbitration mode.

Fig. 2: Decision process for arbitration mode

In the interference analysis block, the gateway analyzes interference between different networks based on Quality of Service (QoS) values from the devices, number of nodes in each network, and the space which the networks are operated. The QoS values can be anything that indicates the state of the communications. After the analyzation is finished, the gateway decides the use of arbitration mode. If arbitration mode is selected, the gateway begins scheduling process using the information of networks.

Fig. 3: A scheduling packet for arbitration

In Fig. 3, the gateway broadcasts a packet. The broadcasted packet includes scheduling information in payload part of the network packet. The interval and window period fields are the scheduling information. To broadcast the scheduling packets, the gateway must prepare packets for every type network. Also the scheduling of the broadcasts for each network is necessary to avoid interference between the scheduling packets. If the interference effect between different networks is not severe, the arbitration process and the scheduling information are useless overhead. To inform whether the arbitration mode is used, a check bit is included in the scheduling packets.

Fig. 4: Allocation of transmission windows

Fig. 4 shows how the scheduling information is used. From the interval field, the nodes in the network know when the next window for transmission starts and from window period field, the nodes know the period that the nodes can transmit data. If a transmission window is allocated for Wi-Fi network, any nodes in the Wi-Fi network can transmit data. Therefore, the multiple access techniques for each network are necessary in the transmission widow. The period of the transmission window may need adjustment to optimize the allocation based on the number of nodes in the networks and IoT applications.

5 Conclusions

Since most communication technologies for IoT use ISM frequency band, interference between networks using different technologies can be a serious problem in dense environment. In this paper, an interference mitigation technique by arbitration is presented. In oneM2M architecture the gateway node has suitable position for performing the arbitration. Therefore, interference mitigation technique using the arbitration is implemented in the gateway.

6 Acknowledgement

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20161210200670). *Corresponding Author: songhk@sejong.ac.kr

7 References
