Future Generation Computer Systems 78 (2018) 626–640

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A reliable IoT system for Personal Healthcare Devices

Min Woo Woo, JongWhi Lee, KeeHyun Park *

Computer Engineering Department, Keimyung University, Republic of Korea

ARTICLE INFO

Article history:
Received 3 June 2016
Received in revised form
7 March 2017
Accepted 1 April 2017
Available online 12 April 2017

Keywords:
IoT
Personal Healthcare Device
OneM2M
u-healthcare
Fault-tolerant
Daisy chain

ABSTRACT

Healthcare applications in IoT systems have been receiving increasing attention because they help facilitate remote monitoring of patients. In this paper, we propose a reliable oneM2M-based IoT system for Personal Healthcare Devices. In order to use a Personal Healthcare Device as an Application Dedicated Node in the proposed system, a protocol conversion between ISO/IEEE 11073 protocol messages and oneM2M protocol messages is performed in gateways located between Personal Healthcare Devices and the PHD management server. The proposed oneM2M-based IoT system for Personal Healthcare Device is constructed, and evaluated in various experiments. The experiments show that the protocol conversion performs effectively, and that the conversion process does not cause the system to suffer serious performance degradation, even when the number of Application Dedicated Node is quite large.

Some Personal Healthcare Device data is too precious to lose due to system failures under u-healthcare environments. However, until now, few studies have focused on fault-tolerant health data services. Therefore, we also propose a fault-tolerant algorithm for the reliable IoT system in which gateways on the same layer in the system are linked to form a daisy chain for fault tolerance at the level, and a gateway stores the backup copy of the previous gateway positioned immediately ahead of the gateway in the daisy chain. The upper-layered gateway stores the parity data of the daisy chain as well. In this manner, as many as two gateway faults occurred at the same time can be recovered. For experiments, the resource trees of the oneM2M-based IoT system were expanded to store information on daisy chains, backup copies, and parity. Our experiments reveal that the proposed algorithm can recover from faults on gateways in the oneM2M-based IoT system.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Healthcare applications in IoT (Internet of Things) [1–6] systems have begun to draw attention recently, because IoT systems provide many useful features that facilitate remote monitoring of patients [7,8]. A Personal Healthcare Device (PHD) becomes an essential part of a remote monitoring system when healthcare applications in IoT systems are considered. PHDs are portable electronic healthcare devices that sense and measure users' biomedical signals. As people monitor their health more carefully than ever, PHDs will become increasingly popular, and must be able to seamlessly connect to main healthcare servers [9–12].

System failures [13–17] may occur because of hardware malfunctions, software bugs, power shortages, or environmental hazards. Most studies on IoT systems have been conducted assuming that few faults exist through which the operations of an IoT system are disrupted. However, because sensors or devices of IoT systems are geographically distributed and rarely maintained, these systems are increasingly vulnerable to failures such as power shortages or environmental hazards than are other systems. Moreover, as the number of nodes in a large-scale IoT system increases, the possibility of fault occurrence increases, causing the system to work improperly. Moreover, some PHD data is too precious to lose due to system failures under u-healthcare environments. However, until now, few studies have focused on fault-tolerant health data services in IoT environments.

The purpose of this study is twofold. The first purpose is to propose and construct an IoT system for PHDs based on the oneM2M communication protocol [5,6]. Whereas (programs installed on) sensors or meters can be Application Entities (AEs) in most oneM2M systems, (programs installed on) PHDs are the Application Entities (AEs) in the oneM2M system proposed in this paper. In order to use PHDs in a oneM2M system, a communication protocol conversion process is needed because PHDs and IoT systems use different communication protocols. In other words, the ISO/IEEE 11073 protocol [9,10] is an international standard

* Correspondence to: Computer Engineering Department, Keimyung University, 1000 Sindang-dong, Dalseo-gu, Daegu 704-701, Republic of Korea.
E-mail addresses: wmwpgm@gmail.com (M.W. Woo), dragon8829@naver.com (J. Lee), khp@kmu.ac.kr (K. Park).

http://dx.doi.org/10.1016/j.future.2017.04.004
0167-739X/© 2017 Elsevier B.V. All rights reserved.

for PHD communication, while the oneM2M protocol is an international standard for the IoT system considered in this paper.

There may be hundreds of IoT servers running in this world, and the number of such IoT servers will increase greatly every year. It would hardly be possible to use IoT systems if every IoT server supported its own proprietary communications protocol only. Therefore, standard communications protocols have been proposed in IoT environments for interoperability, and most the IoT servers have been made to support the standard communications protocols. On the other hand, most PHDs do support the ISO/IEEE 11073 communications protocol because the protocol is a standard communications protocol for PHDs. This is the reason why a protocol conversion process is needed in the paper. Until now, few studies have focused on protocol conversion process on health data services in IoT environments. In this study, on the basis of our previous protocol conversion study [18], the protocol conversion process is restructured and reprogrammed to allow its application to a wider variety of PHDs. Some experiments are performed on the prototype of the proposed system, to ensure that the system does not suffer serious performance degradation when the number of PHDs is quite large.

The second purpose is to propose a fault-tolerant algorithm for the reliable IoT system. We propose a fault-tolerant algorithm in which gateways on the same layer in the system are linked to form a daisy chain for fault tolerance at the level, and a gateway stores the backup copy of the previous gateway positioned immediately ahead of the gateway in the daisy chain. The backup copy of the last gateway in the daisy chain is stored by the upper-layered gateway in the system. The upper-layered gateway stores the parity data of the daisy chain as well. In this manner, as many as two gateway faults occurred at the same time can be recovered. The fault-tolerant algorithm that employs the daisy chain proposed in this study is evaluated based on experiments on the multilayered oneM2M-based IoT system. For experiments, the resource trees of gateways and the server are expanded to store fault-tolerant-related data such as daisy chain data, backup copies, and parity data. Our experiments reveal that the proposed algorithm can recover from faults on gateways in the oneM2M-based IoT system.

Healthcare applications in IoT systems have begun to draw attention recently because they provide many features that are useful for remote monitoring of patients, including scalability, flexibility, and interoperability [7,8,19]. When healthcare applications in IoT systems are considered, gateways located between sensors (or PHDs) and the IoT servers usually play very important roles [8]. Good (Poor) management of the gateways usually leads to good (poor) performance in the entire IoT system. Thus, most of the protocol conversion process and fault-tolerance process proposed in this study are performed at the gateways.

The remainder of this paper is organized as follows. Section 2 describes some related studies, and Section 3 explains the structure of the oneM2M-based IoT system and modules constructed in this study Section 4 discusses communication protocol conversion mechanisms between oneM2M protocol messages and ISO/IEEE 11073 protocol messages. Section 5 shows the results of some experiments using the system constructed in this study, along with a discussion based on the results. Section 6 discusses the proposed fault-tolerant algorithm for the reliable IoT system Finally, Section 7 draws some conclusions and discusses some possible directions for future research.

2. Related studies

The ISO/IEEE 11073 communication protocol [9,10] was proposed by an ISO/IEEE committee as an international standard to provide interoperability for health and medical services in ubiquitous environments (especially using PHDs). The oneM2M communication protocol is an international standard for IoT systems [5,6]. In such a system, a sensor or device (i.e., an installed program on either) represents an application dedicated node-application entity (ADN-AE) that gathers surrounding data and transmits them to the system's middle node-common service entity (MN-CSE). An MN-CSE controls or monitors ADN-AEs that belong to the MN-CSE. Moreover, it performs processing that is necessary to achieve efficient communication between ADN-AEs and the infrastructure node-common service entity (IN-CSE). A manager or user can access data stored in the IN-CSE through an ADN-AE.

In [11], a message processing scheme for an integrated PHD gateway in an integrated PHD management system is proposed. The ISO/IEEE 11073 communication protocol is used to transmit health messages measured by a PHD to the integrated PHD management server via the related integrated PHD gateway. The OMA DM communication protocol is used to transmit device management commands issued by the integrated PHD management server to a PHD via the related integrated PHD gateway. In [10], a multilayer secure biomedical data management system for managing a very large number of diverse personal health devices is proposed. The ISO/IEEE 11073 protocol and OMA DM protocol are extended and implemented in the system. The PHD gateway module receives separate ISO/IEEE 11073 or OMA DM messages from the PHD agents of the PHDs in order to integrate them to send the server a single integrated message.

An IoT application that has emerged is healthcare [7,8,19,20]. The importance of gateways located between sensors and the Internet has been recognized in IoT-based patient monitoring systems, because the gateways have beneficial knowledge and constructive control over both the sensor network and the data to be transmitted over the Internet [8]. The Smart e-Health Gateway proposed in [8] provides local storage to perform real-time local data processing and embedded data mining.

When a patient's biomedical data is processed, reliable IoT systems should be provided to facilitate fault-tolerant healthcare services. Until now, few studies have focused on fault-tolerant health data services. Studies on fault-tolerant IoT systems have mainly focused on routing problems [20–22]. In [20], a fault-tolerant and scalable IoT architecture for healthcare is proposed. Fault tolerance is achieved via backup routing between nodes and advanced service mechanisms, to maintain connectivity in the presence of faults on the paths between system nodes. A fault-tolerant routing protocol for IoT systems is proposed to assure successful delivery of packets, even in the presence of faults on the paths between a pair of source and destination nodes [21]. The proposed approach based on the learning automata and cross-layer concepts dynamically selects the optimum path. Dijkstra's algorithm can be used to select secure fault tolerant routing paths to enhance performance and minimize energy consumption [22].

3. Structure of a oneM2M-based IoT system for PHDs

3.1. System structure

Fig. 1 shows the structure of the proposed oneM2M-based IoT system for PHDs. In an IoT system, (a program installed on) a sensor or device represents an Application Dedicated Node-Application Entity (ADN-AE) that gathers surrounding data and transmits it to the system's Middle Node-Common Service Entity (MN-CSE). A (program installed on a) PHD acts as an ADN-AE in the proposed system. An MN-CSE controls or monitors ADN-AEs that belong to the MN-CSE; moreover, it performs processing that is necessary to achieve efficient communication between ADN-AEs and the Infrastructure Node-Common Service Entity (IN-CSE).

Download English Version:

https://daneshyari.com/en/article/4950217

Download Persian Version:

https://daneshyari.com/article/4950217

Daneshyari.com