DEMO: Mobile Relay Architecture for Low-Power IoT Devices

Ahsan Manzoor*, Pawani Porambage*, Madhsanka Liyanage*, Mika Ylianttila*, Andrei Gurtov†
*Centre for Wireless Communications, University of Oulu, Finland,
†Department of Computer and Information Science, Linköping University, Sweden
Email: *firstname.lastname@oulu.fi, †gurtov@acm.org

***Abstract*—Internet of Things (IoT) devices need pervasive and secure connections to transfer the aggregated data to the central servers located in remote clouds where the collected data further processed and stored. However, most low-power IoT devices cannot transmit the collected the data directly to such servers due the limited transmission power and range. Thus, third-party devices such as smart mobile phones are used as a relay to establish the communication link between IoT devices and the cloud server. This paper demonstrates a mobile-based relay assistance solution for secure end-to-end connectivity between low-power IoT sensors and cloud servers by using Bluetooth Low Energy (BLE) technology. The prototype implementation verifies the technical readiness of the proposed solution.**

***Index Terms*—Bluetooth Low Energy, Internet of Things, Relay, Security, Sensors, Ambient Assisted Living**

I. Introduction

Billions of smart devices are available in digital world due to the advancement of the Internet of Things (IoT). Thus, the proliferation of IoT technologies is closely coupled with day-to-day human activities[1]. Especially, IoT sensor devices are widely used in healthcare applications. The IoT integration into medical devices greatly improves the quality and effectiveness of health service, bringing especially high value for the elderly, patients with chronic conditions, and those requiring constant supervision. IoT integration has the potential to not only keep patients safe and healthy but to improve how physicians deliver care as well.

Many IoT devices in healthcare and AAL applications are equipped with unlicensed band short-range radio access technologies, including Bluetooth Low Energy (BLE), HaLow, ZigBee, and Smart Utility Networks (SUNs). [2]. Among them, BLE is the best-known and most used low-power communication technology that supports connectivity for Body Area Networks (BANs) and a large number of medical IoT devices which operate with coin cell batteries [3].

We define this particular objective of exploiting mobile-based relays for the back-end connectivity of BLE devices in terms of a specific AAL use case as illustrated in Figure 1. The elderly or people with chronic conditions may require continuous monitoring of their health records or localize with the help of different BLE sensor nodes. There are certain interested parties (e.g., family or caretakers) who need to track their behavior and examine the health conditions based on the data retrieved from the remote central cloud. Typically, the back-end connectivity between the BLE wearable sensor and the cloud data center is maintained by a dedicated mobile phone which possessed by the same individual [4], [5]. However, the elderly people may forget to bring the mobile phone when they are exceeding the comfort zone or the battery might be dead. Therefore, we proposed to use the help of some random mobile users who are performing as relays in our system. In order to keep the in-line with this mechanism, the unknown mobile user needs to be rewarded by the remote cloud for his relaying service. To the best of authors' knowledge, this will be the first attempt of exploiting third-party unknown mobile relays for the forwarding of medical data generated by BLE sensors.In this demo, we show the viability of realizing the proposed architecture through a prototype implementation with off-the-shelf IoT sensors and mobile devices [1].

Section II describes the system architecture and Section III presents a prototype implementation. Section IV gives an overview of the showcase we intend to present at the Demo Session, followed by Section V which specifies a set of technical requirements.

II. System Architecture

The network architecture is illustrated in Figure 1 with reference to the AAL use case. BLE sensor advertises its availability of data. There can be one or number of anonymous mobile phones who receive the advertisement and accept to cooperate with further communication as a relay node. The best relay node is selected based on the received signal strength indicator (RSSI). The link between the mobile and the central server (CS) in IoT cloud will be securely established over the Internet in a conventional manner (e.g., Hypertext Transfer Protocol Secured (HTTPS)). When the data is received from the BLE device, CS will update the database which is dedicated to that particular user.

The key attributes of this protocol should include the following:

1) Ubiquitous access and mobility support irrespective of the user's location.
2) Adaptability to arbitrary community or provider.
3) Real life compatibility.
4) Lightweight authentication between the BLE sensor and CS.

We consider few pre-requisites and key assumptions: The BLE devices will undergo an initial registration with CS in the IoT cloud. In order to maintain E2E secure communication, the BLE device and CS should share the cryptographic keys for data encryption and decryption, and the authentication credentials (e.g., User ID (UID), hash chain, etc.). The mobile should be able to handle multiple peripherals in one instance.

978-1-5386-4725-7/18/$31.00

[1] A teaser video about this demonstration is published here: https://www.youtube.com/watch?v=mIMh6Sfo84s&feature=youtu.be

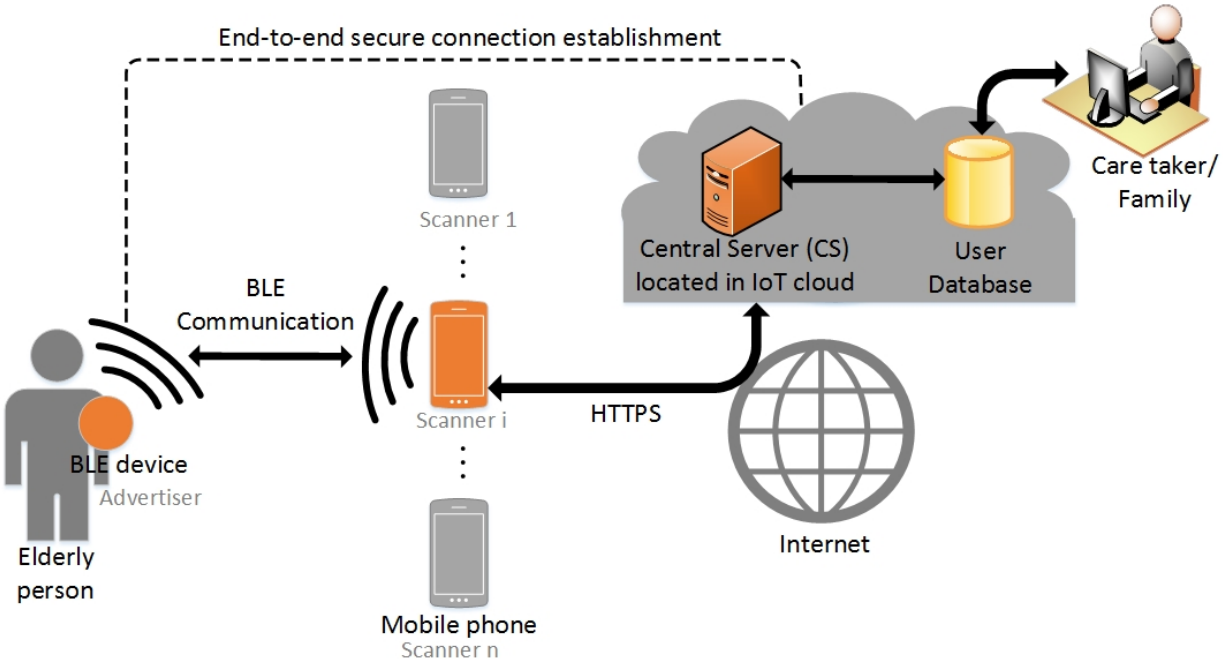

Fig. 1. The network architecture

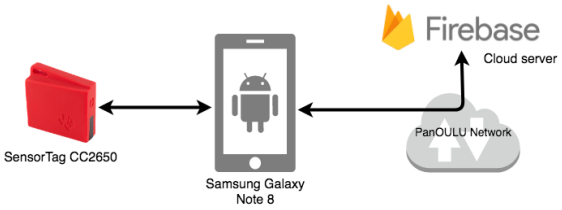

Fig. 2. Testbed setup

The link quality is guaranteed for all the communication channels over the period of communication. No mutual or transitive trusts are required between the relay device and sensor /CS. For the sake of rewarding mechanism, the mobile needs to be registered with CS in advance and the secure links (i.e. Transport Layer Security (TLS) protocol) should be established between the two entities. The functionality of CS is utterly trusted which will grant the incentives to the relay device at the end of successful service.

III. Prototype Setup

We have accomplished the prototype implementation on a testbed with a BLE sensor, mobile, and cloud platform (Figure 2). The Internet access was achieved by the general university WiFi network (i.e., PanOULU network[2]).

Texas Instrument SensorTag[3] CC2650 and Samsung Galaxy Note 8 were respectively used as the sensor and mobile hardware platforms. In accordance with the protocol, we slightly modified the BLE stack 2.2.1 on CC2650 using SmartRF Flash programmer 2. Table I shows the custom BLE stack configuration on the CC2650 sensor.

The mobile application (Figure 4) was developed on Android 7.1.1 operating system using Android Studio 3.0 libraries. This mobile application scans in the background to discover devices and connects to the BLE sensors. This BLE sensor is then paired with the mobile automatically, using the passcode 0000. After paring, sensor initiates data uploading directly to the Cloud platform. The last part of the implementation was to deploy the cloud server on Google Firebase where the user of the mobile application can authenticate himself and the sensor can upload the sensed data to a JSON database. The user needs to log in the application for authentication by CS and the collection of rewards.

The application monitors the amount of data transferred from the sensor to the cloud and after the confirmation from the CS, the application automatically credits the reward to the user account. In order to keep the reward mechanism simple and profitable, for transferring every 1 KB of data, the user

TABLE I
BLE Configuration Settings for CC2650

Attribute	Configured values
Transmission power	0 dB
Number of running services	6 services
Periodic event	1000 ms
Advertising interval	100 ms
Connection timeout	1000 ms
Broadcast delay	500 ms
Packet size	18 byte

[2]https://www.panoulu.net/open-wireless-internet-access
[3]http://www.ti.com/lit/ug/tidu862/tidu862.pdf

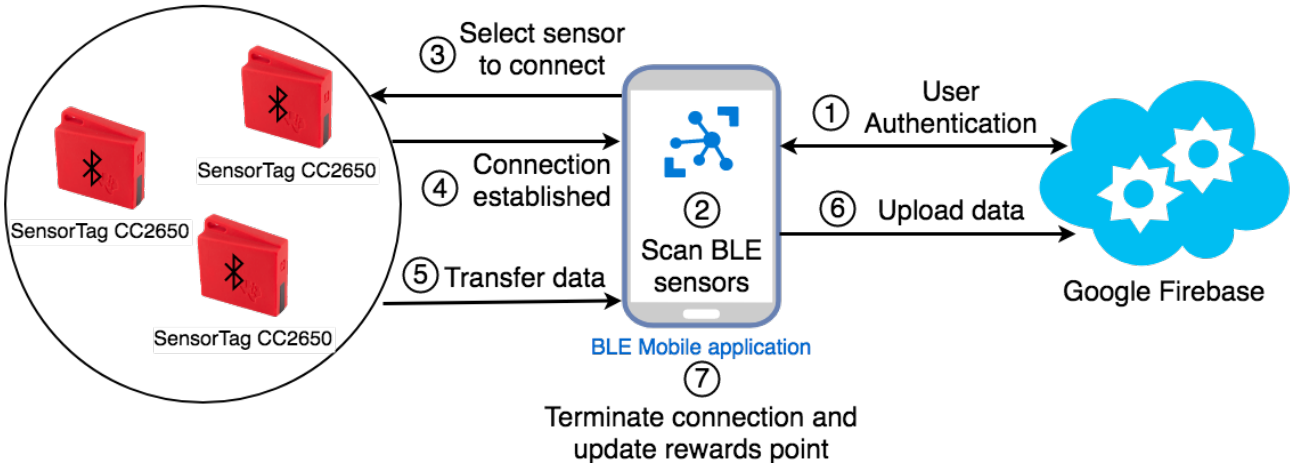

Fig. 3. Demonstration Flowchart

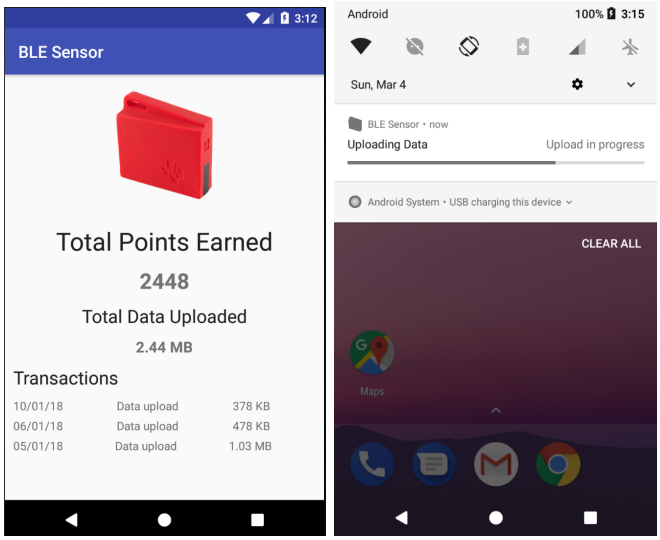

Fig. 4. BLE Mobile Application

gets one point which can later be used for different purposes. Moreover, Firebase uses HTTPS connection over TLS for secure communications between the mobile and cloud server along with real-time database security.

IV. Demonstration and Interaction

A. Demonstration Content

In this demonstration, we will visualize the whole process as shown in Figure 3. The demonstration is divided into three parts. The first part includes the user authentication from the cloud server and initialization of the scanning process from the mobile. After the scanning is complete, the application will select the sensor based on its signal strength and establish a connection. The last part includes the transfer of the data from the sensor to the Google firebase cloud. As the data is uploaded, the connection is terminated and the user account is rewarded according to the amount of data transferred.

B. Interaction Content

The attendees will be able to interact with this demo in two ways. In the first case, the attendee will be able to download the developed Android application on their mobile phone and register as a user. They will be able to visualize the whole demonstration process on their mobiles. In the second case, the attendee can use one of the authors mobile, with the pre-installed android application. The attendees can also look at the data uploaded using their account on the cloud server.

V. Technical Requirements

We require 3 Texas Instrument Sensor Tag CC2650 updated with custom BLE stack 2.2.1, one laptop and one mobile with Android version 7.1+. Authors will bring the required equipment for demonstration.

Acknowledgement

This work has been performed under the framework of the Infotech Doctoral Program of UniOGS and the three projects, 6Genesis Flagship (grant 318927), SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems) and Towards Digital Paradise. These projects are funded by Academy of Finland and TEKES, Finland. It is also supported by Center for Industrial Information Technology (CENIIT).

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] N. Xia, H.-H. Chen, and C.-S. Yang, "Radio resource management in machine-to-machine communications-a survey," *IEEE Communications Surveys & Tutorials*, 2017.

[3] J. Nieminen, C. Gomez, M. Isomaki, T. Savolainen, B. Patil, Z. Shelby, M. Xi, and J. Oller, "Networking solutions for connecting bluetooth low energy enabled machines to the internet of things," *IEEE network*, vol. 28, no. 6, pp. 83–90, 2014.

[4] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the internet of things with bluetooth smart," *Ad Hoc Networks*, vol. 57, pp. 19–31, 2017.

[5] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.