An IoT Framework for SDN Based City Mobility

Anas Al-Rahamneh[1,2], José Javier Astrain[1,2], Jesús Villadangos[3], Hicham Klaina[4], Imanol Picallo[3], Peio Lopez-Iturri[2,3], and Francisco Falcone[3]

[1] Statistics, Computer Science and Mathematics Department, Public University of Navarra, 31006 Pamplona, Spain
[2] Institute of Smart Cities, Public University of Navarre, 31006 Pamplona, Spain
[3]Electric, Electronic and Communication Engineering Department, Public University of Navarre, 31006 Pamplona, Spain
[4]Department of Signal Theory and Communication, University of Vigo, 36310 Vigo, Pontevedra, Spain

Abstract. The Internet of Things (IoT) is becoming more widespread, with global application in a wide range of commercial sectors, utilizing a variety of technologies for customized use in specific environments. The combination of applications and protocols and the unique requirements of each environment present a significant challenge for IoT applications, necessitating communication and message exchange support. This paper presents a proposed SDN-based edge smart bypass/ multiprotocol switching for bicycle networks that supports functionalities of coordination of various wireless transmission protocols. A performance assessment will be presented, addressing a comparison between the different protocols (LoRaWAN vs. Sigfox) in terms radio coverage.

Keywords: Internet of Things, Smart Mobility, SDN, Wi-Fi, LoRaWAN, Sigfox.

1 Introduction

The Internet of Things (IoT) has gotten a lot of press lately because of the features it offers that could help humanity advance in terms of intelligence, automation, and convenience, among other things. The IoT has transformed objects that are entirely unrecognizable into distinct, recognized, interconnected intelligent things that are supported by high-quality communication protocols, which are referred to as sensible objects. The new devices collect environmental data and send messages over the Internet while being monitored and controlled remotely by a central network server. The IoT entails extending communication to a new range of physical devices and everyday objects beyond popular devices such as laptops and smartphones.

The IoT services utilize various network protocols depending on the IoT service's specific purpose [1]. Current popular wireless protocols include ZigBee [2] and Z-Wave [3], which are mesh network protocols and utilize the IEEE 802.15.4 [4] personal area network standard. Alternatives to both standards include 6LowPAN [5], Thread [6], and Bluetooth Mesh [7], which also support IPv6 over mesh networks.

The IoT world is full of heterogeneous, often proprietary protocols, each tailored to a specific use case. This poses a challenge to the IoT's widespread adoption and evolution. The integration of multiple wireless communication protocols into a wireless sensor node provides flexible and expanded connectivity from the same device, also devices to be able to communicate seamlessly in ad-hoc environments.

Software-Defined Networking (SDN) is another new intelligent technology within the networking domain that increases network performance and provides better security, reliability, and privacy using dynamic software programs [8]. The SDN allows the control logic to be separated from the sensor nodes/actuators, which makes it a promising solution for inflexible management WSNs. The benefit of using SDN for WSN management is that it allows for centralized control of the entire network, making it easier to deploy network-wide management protocols and applications on demand.

Several works of literature have discussed how to deal with wireless communication multiprotocol in the heterogeneous network. Uddin et al. have proposed in [9] an SDN-based multiprotocol edge switching for largescale, heterogeneous IoT environments. The proposed system is based on the P4 programming language that lets end users dictate how networking gear operates to achieve this non-IP multiprotocol programmable forwarding capability. The proposed approach based on using a customized network switch to deal with different protocols requires availability throughout the city, which is a challenge in terms of cost and infrastructure.

Gao and Chang have presented in [10] a scalable and flexible communication protocol which is designed to work as a gateway between the Internet and various heterogeneous wireless networks. Froiz-Míguez et al. have presented in [11] a ZiWi gateway, a low-cost IoT fog computing home automation system that allows for carrying out seamless communications among ZigBee and WiFi nodes. Amiriyan and Nguyen have investigated in [12] the multiprotocol flow assignment in a smart home IoT network to the appropriate gateway interfaces. Kang et al. have proposed in [13] a self-configurable gateway featuring real-time detection and configuration of smart things over wireless networks. Chaudhary et al. have presented in [14] a smart home multiprotocol automation System using smart gateways. Kim et al. have proposed in [15] an Internet of Vehicles (IoV) access gateway to controls the incoming data traffic to the In-vehicle network (IVN) backbone and the outgoing data traffic to the IoV in the network environment. The challenges that face the gateways are that they are preconfigured, use vendor-specific APIs, and are limited to authorized devices and policies only.

This paper presents a proposed SDN-based edge smart bypass/ multiprotocol switching for bicycle networks that supports functionalities of coordination of various wireless transmission protocols, whether they be legacy, mainstream, or emerging solutions.

The proposed implementation benefits from the protocols' advantages, allowing it to perform better in various scenarios. When Wi-Fi connectivity is available, it will allow for more extensive data payloads and more frequent uplink transmissions. LoRaWAN, on the other hand, will take advantage of its low energy consumption and associated long-range coverage to cover a large area at once.

The rest of the paper is organized as follows. Section 2 presents the architecture of the proposed SDN-based edge. The system description is presented in Section 3. The measurement results are given in Section 4. Finally, Section 5 concludes the paper.

2 System Architecture of SDN-based Smart bypass for Bicycle Network

We proposed an SDN-based Smart edge bypass solution/ multiprotocol switching to forwarding data coming from wireless IoT devices and sensors over different wireless communication standards. This proposal aims to use public/open access points (AP) or gateways that are distributed throughout the city for various wireless communication protocols to transmit data to the cloud.

In our case, the mobility node (bicycle) is equipped with several wireless communication modules. So, when the node gets close to one of the APs or gateways, the SDN controller implements several pre-defined rules to match the AP's protocol with the wireless communication modules' protocols, then chooses the proper protocol to flow the data through it. In the case of a group of the different APs or gateways, the SDN controller determines the appropriate protocol to transmit data depending on the data type, size, etc. (see Fig. 1).

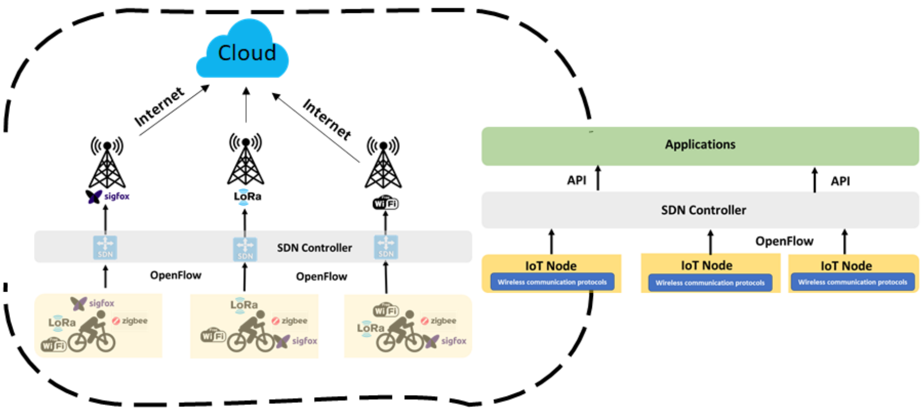

Fig. 1. Proposed System Architecture

3 System Implementation / Use-Case/ System Description

This section describes the proposed SDN's functionality and how we can implement it in our use case, Bicycle Network. Each of the bicycles will be equipped with several wireless communication modules and different sensors for sensing and gathering information about the environment. This data varies in size and formats, so selecting the appropriate protocol to send this data is essential to ensure that it reaches the destination. For instance**,** multimedia files such as video, pictures, and audio files require high-bandwidth wireless protocols due to these files' large size. In contrast, the small size of sense data like temperature measurements, humidity, or gas levels does not need this ability. Therefore, the functionalities of coordination of various wireless transmission protocols need to be handled well. For overcoming the problem of partial node death due to exhaustion of energy, energy harvesting was used through the use of a dynamo installed in a bicycle hub.

The proposed SDN will be provided by a set of pre-defined IF-This-Then-That (IFTTT) rules that regulate the protocols selection process and responsible for a set of tasks such as file transfer queuing, message queuing, and confirmation of receipt - acknowledgment packet (ACK) and negative acknowledgment (NAK).

In this respect, if the bicycle becomes close to a group of access points, the proposed SDN will first determine the protocol for each access point and the signal strength. Secondly, it will group the sense data based on its type and size. In case that there is multimedia data between that data, it is first ascertained that there is a Wi-Fi network within the networks. Secondly, it measured the Received Signal Strength Indicator (RSSI) and then attempted to connect to the strongest open network available. Once the connection is established, the proposed SDN dividing each file into one or more messages and transmitting the messages. The proposed SDN will wait until it receives an ACK from the recipient. If the ACK is not sent or the recipient returns a NAK, the proposed SDN will either try again from the same access point or send it from another access point. Fig. 2 shows a flow diagram that illustrates the different tasks performed based on pre-defined IFTTT rules.

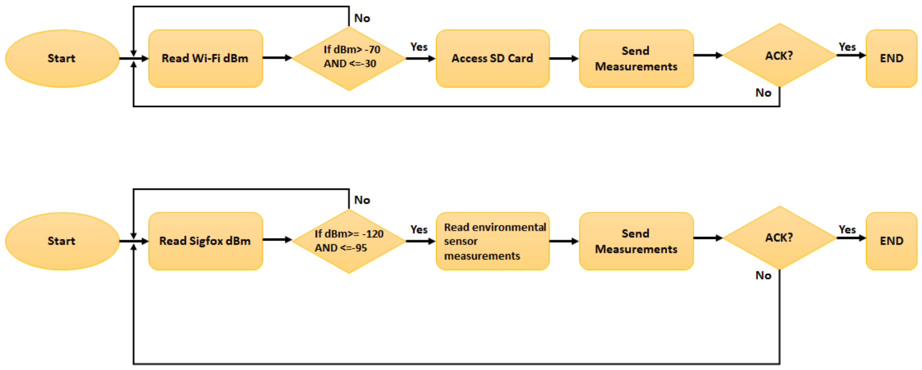

Fig. 2. Flow diagram of the simplified IFTTT rules to send for sensing information.

4 Experiments / Performance Assessment

This section presents the experimental setup and the experimental results of the RSSI and packet loss measurements that have been carried out within an urban test scenario in the city of Pamplona for the wireless protocols Sigfox, LoRaWAN, and Wi-Fi. The Sigfox and LoRaWAN are operating at 868 MHz, while the Wi-Fi operates within 2.4GHz/5.5GHz bands. Fig. 2 shows the employed hardware.

a b c

Fig. 3. Employed LoRaWAN and SigFox hardware for measurements; a) Dragino LoRa shield with GPS, b) The Things Networks LoRaWAN Gateway; and c) Arduino MKR FOX 1200.

The Dragino LoRa shield with GPS mounted on an Arduino UNO board has been employed to assess LoRaWAN technology. The TTN Gateway has been deployed within the Electric, Electronic, and Communications Engineering Department building of the Public University of Navarre (UPNA), and it is represented by a blue circle named "GW" in Fig. 3. The gateway has been located on the second floor, near a window, in order to increase link visibility. The Arduino MKR FOX 1200 device has been used for SigFox technology assessment. In this case, no gateway deployment is needed since the SigFox alliance provides the network infrastructure and coverage, so unlike

Fig. 3 shows a map where the measurement campaign has been carried out. The blue circle represents the LoRaWAN Gateway location, and the 26 measurement points where the mote based on Dragino LoRa shield has been deployed are shown with different colors. LoRaWAN, there is no need to establish and maintain the wireless communication network infrastructure. Values are in general above the sensitivity values (in the case of Dragino LoRa of -148 dBm and in the range of -126 dBm in the case of MKR FOX 1200).

Fig. 4. LoRaWAN measurements results. Green: No packet losses. Yellow: some packet losses. Red: All packets lost.

The blue circle represents the LoRaWAN Gateway location, and the 7 measurement points where the mote based on Dragino LoRa shield has been deployed are shown with different colors. The green color represents that no packet has been lost in the communication; the yellow color means that some packets have been lost, and the red color that all packets have been lost. For each measurement point, 4 packets have been transmitted from the mote to the TTN Gateway. The packets have been sent every 30s, which is the shortest interval between packets allowed by LoRaWAN. The equivalent measurement set for the case of SigFox setup is depicted in Fig. 4.

The high elevation zone (marked in DarkOrange in Fig. 3, which is higher than the tallest building of the University) causes significant losses in the communication with the nodes deployed across the hill, even for short distances from the Gateway (e.g. measurement points 2 and 3).

Fig. 5. SigFox measurements results. Green: No packet losses. Yellow: some packet losses. Red: All packets lost.

In order to gain insight in relation with quality of service metrics in relation with the operation of the proposed LPWAN systems, Signal to Noise ratio values have been measured within the area under analysis previously described. The measurement results for both SigFox SNR values as well as LoRaWAN are depicted in figure 5. As a function of node location, SNR values exhibit variations in the order of 10 dB, with higher values in the case of SigFox, owing in principle to larger values of transmit power employed.

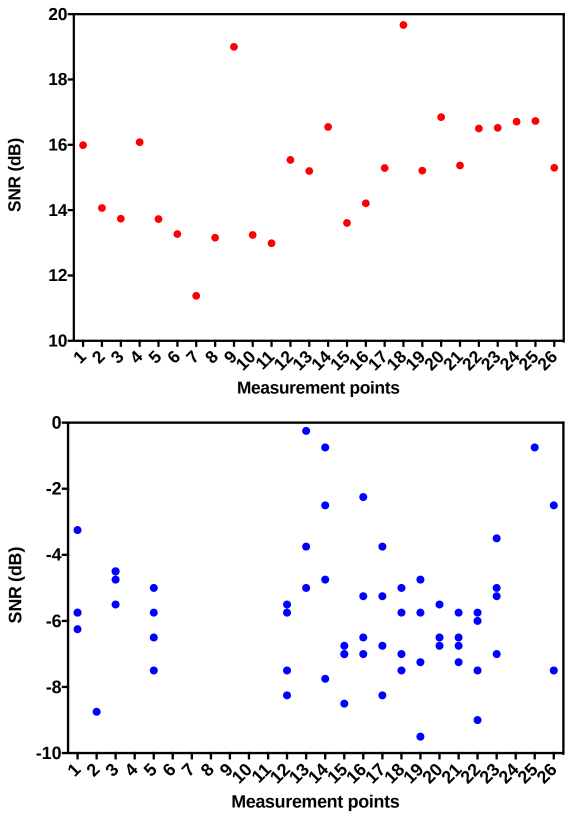

Fig. 5. Signal to Noise ratio measurement results within the area under test, for SigFox (upper image) and LoRaWAN (bottom image).

As previously indicated, the system will make use of wireless connectivity as a function of network availability and bandwidth requirements. In the case WLAN is required, it will be employed as a function of coverage availability. Fig. 6 shows the map of public Wi-Fi hotspots locations within the city of Pamplona where people may obtain Internet access [16]. Work is currently underway in terms of traffic characterization, in order to aid in Quality of Services/Quality of Experience metrics, related with inter radio access technology traffic handling, achievable transmission rate and overall end to end delay, among others.

Fig. 6. Locations of public Wi-Fi hotspots within the city of Pamplona.

As it can be seen, the mobile node continues to search for APs while moving to transmit the information. Each wireless interface module on the mobile node keeps measuring the RSSI of its protocol. The node applies the pre-defined IFTTT rules over the received RSSI. Once any of the IFTTT rules are met, the mobile node performs that rule. The rule determines which kind of information is best suited to the capability of each wireless communication protocol to transmit the data over it.

5 Conclusions

This work presents a proposed SDN-based Smart bypass solution to switch between heterogeneous wireless communications protocols that are equipped to a mobile IoT node. The proposed system gives the node the flexibility and ability to choose the appropriate protocol between these protocols to transmit the data based on several factors such as packet loss, RSSI, file size, etc. Work is going in relation with traffic end to end characterization within the scenario under analysis.

References

1. A. Al-Fuqaha, M. Guizani and M. Mohammadi, "Internet of things: A survey on enabling technologies protocols and applications", *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
2. Zigbee Alliance, “ZigBee Specification,” ZigBee Document 05347r17, pp. 1-576, Jan. 2008.
3. Z-Wave Alliance, "Z-Wave Device Class Specification," Z-Wave Document SDS1042, pp. 1-195, Mar. 2018.
4. IEEE 802 Working Group, "IEEE Standard for Local and Metropolitan Area Network – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std 802.15.4TM-2011, pp. 1-314, Jun. 2011.
5. Kushalagarent, N. al. "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem, Statement and Goals", IETF RFC 4919, Aug. 2007.

6. Thread Group, https://www.threadgroup.org. last accessed April 16 2021.
7. Bluetooth SIG, "Bluetooth Mesh Networking", Bluetooth SIG Document, pp. 1-28, Jul. 2017.
8. Diego Kreutz, Fernando M.V. Ramos et al., Software-defined networking: A comprehensive survey, Proceedings of the IEEE, 103, 1, 1, pp.14-76, 2015.
9. M. Uddin, S. Mukherjee, H. Chang, and T. V. Lakshman, “SDN-Based multiprotocol edge switching for IoT service automation,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 12, pp. 2775–2786, Dec. 2018.
10. R. Gao and C. H. Chang, “A scalable and flexible communication protocol in a heterogeneous network,” in *2014 IEEE/ACIS 13th International Conference on Computer and Information Science, ICIS 2014 - Proceedings*, pp. 49–52, Sep. 2014.
11. I. Froiz-Míguez, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, “Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes,” *Sensors*, vol. 18, no. 8, p. 2660, Aug. 2018.
12. Milad Amiriyan Kim-Khoa Nguyen, Multiprotocol Flow Assignment in Smart Home IoT Network, 2020 IEEE International Conference on Communications (ICC), 2021.
13. B. Kang, D. Kim, and H. Choo, “Internet of Everything: A Large-Scale Autonomic IoT Gateway,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 3, no. 3, pp. 206–214, Jul. 2017.
14. S. K. Chaudhary, S. Yousuff, N. P. Meghana, T. S. Ashwin, and R. M. R. Guddeti, “A Multi-Protocol Home Automation System Using Smart Gateway,” *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2367–2390, Feb. 2021.
15. D.-Y. Kim, M. Jung, and S. Kim, “An Internet of Vehicles (IoV) Access Gateway Design Considering the Efficiency of the In-Vehicle Ethernet Backbone,” *Sensors*, vol. 21, no. 1, p. 98, Dec. 2020.
16. Buildings and Wi-Fi Areas in Pamplona, https://www.pamplona.es/ayuntamiento/varios/edificios-y-zonas-wifi-en-pamplona, last accessed April 16 2021.