Physical Tracking of ESP32 IoT Devices with RSSI Based Indoor Position Calculation

Received 30 January 2023; Accepted: 5 March 2023 *Research Article*

Özlem Şeker
Department of Computer Engineering
Graduate School of Natural and Applied Sciences
Dokuz Eylul University
Izmir, Turkey
ozlem.yerlikaya@cs.deu.edu.tr
0000-0002-8686-340X

Batuhan Şahin
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
batuhan.sahin@ceng.deu.edu.tr

Tunahan Akdoğan
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
tunahan.akdogan@ceng.deu.edu.tr

Gökhan Dalkılıç
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
dalkilic@cs.deu.edu.tr
0000-0002-0130-1716

***Abstract*— In recent days, the increase in the number of devices that can access the Internet and the variety of areas where it is used have made it essential to ensure the security of the transmitted data. The unique values embedded in the hardware can be used as keys or secret values within cryptographic algorithms to provide the confidentiality and integrity of the data. In such a situation, maintaining the security of the Internet of things (IoT) device used is a prominent element as well as the privacy of the data. The security requirement of each IoT application may be different. While some applications contain sensitive personal or commercial information, for some applications only the presence of the device may be important. In addition, it is likely to have different devices capable of processing cryptographic algorithms. Within the scope of this study, the distance information was calculated with received signal strength indication (RSSI) data based on 4 reference points of the ESP32 IoT device located indoors. The error rate was observed with the positioning based on the RSSI information of the current position of the device. It has been tested whether it is possible to detect whether the device that transfers the data is legitimate or not via indoor position calculation using RSSI.**

Keywords— indoor localization, IoT, RSSI, ESP32, Wi-Fi.

I. INTRODUCTION

Internet of things (IoT) devices have less processing power, storage, and power consumption than computers or other complicated electronic devices. Therefore, the usage area of IoT devices is limited due to having these three features. For instance, a device with a low processing power means less computation and code execution. The disadvantage of resource constraints creates advantages such as cheapness and less power consumption of IoT devices. Using IoT devices in an application requires a well-done specification analysis. The advantages need to outnumber the disadvantages of the application. The comparison between sophisticated devices (computer, mobile phone) and IoT devices are generally compared based on price and power consumption in the system. However, the most important part is mostly ignored which is security. An application on a computer or a mobile phone will use more processing power and will be able to run cryptographic algorithms that require more computational power. IoT devices may lack to process huge computations of cryptographic algorithms. Therefore, it is more difficult to ensure security with IoT devices.

Most IoT devices do not have an operating system to execute programs dynamically. IoT devices can be used as stations or access points in a local network or mesh networks [1]. They can broadcast data in the local network. This behavior may protect them from threats that come over the Internet. However, it causes a critical security vulnerability in the local network. Any device within the range of the local network can access the network. It can spread inconsistent data by impersonating the devices found in the application, making the network unusable by constantly sending data, and collecting data such as important personal information in the application and misusing it. To solve this physical threat, we decided to use an indoor positioning system (IPS). In IoT applications, without human interaction, and without a user interface, determining the location of the devices in the communication network is of great importance in terms of secure device management. Furthermore, it should not be forgotten that a huge communication network that grows with devices is expected [2, 3]. Positioning can monitor IoT devices, with information related to multiple reference points within the located area. It is possible to diversify examples of outdoor localization such as global navigation satellite system (GNSS) including global positioning system (GPS), global navigation satellite system (GLONASS), Galileo, and BeiDou [2]. Among these, the most common one is the GPS. However, these outdoor positioning systems cannot meet the expected performance for detecting devices in indoor environments due to the density of objects and signal attenuation by various building materials. For this purpose, the IPS technique is examined to determine the location of objects where GPS cannot determine the position. In various IoT applications such as smart home applications, IoT devices can be mostly used indoors and in small buildings. Therefore, localization using Wi-Fi and Bluetooth is used instead of GPS.

Considering the physical tracking of the devices, the distance of the devices to each other or the distance to the wireless access point will allow us to have information about the device's location. In our implementation and benchmark tests, the location of the IoT devices that are ESP32-WROOM-32 version of ESP32, is determined by using IPS.

If the ESP32 gateway is aware of the location information of all devices in the IoT application, it can decide which device is legitimate and which device is an external threat. ESP32 [4] supports both Wi-Fi and Bluetooth low energy (BLE) wireless communication. Therefore, RSSI is used as an indicator of the strength of the signal. The strength of the signal is expressed in decibel milliwatts (dBm). As the distance increases, the signal strength will decrease [5]. While dBm has a definite value with international validity, the received signal strength indicator (RSSI) value is determined by companies and has no definite value. Its value is determined as a percentage. At -90 dBm, the signal strength begins to get very low, and loss of control occurs. Signal loss in a short distance is due to logarithmic variation and ideal signal strength is determined between -30 and -80 dBm. The presence of the devices may be computed with such as the trilateration method where the relative distance from each receiver is calculated based on the RSSI value.

In the experimental study, the ESP32 device is located in a room with four reference nodes (ESP32 devices) whose locations are predetermined. It has been observed that the location of a device outside the room can be detected by RSSI value. The data transmission of the devices that is not in the specified area is blocked. In addition, the location information of the device belonging to the application is calculated with RSSI and the error rate is specified.

The remainder of the paper is organized as follows: Section 2 provides a state-of-the-art review on the methodologies and techniques of the indoor position systems. Section 3 gives brief information about implementation of the cases of ESP32 positioning and the experimental studies are presented and discussed. Finally, Section 4 gives some concluding remarks and future directions.

II. Related Work

Misal et al. [6] represented a prototype that includes determining the position of three ESP32 devices in the indoor area. For this purpose, RSSI information is gathered with BLE beacon and transmitted to the server via MQTT protocol in order to calculate RSSI to distance. The trilateration algorithm also predicts the coordinate of the BLE beacon with the distance information. The output of the study gives accuracy up to 2.3 meters to the actual position of the BLE beacon.

GPS is not proposed for tracking physically indoor devices due to no visibility and the disadvantages of signal spreading from walls. AlQahtani et al. [7] suggested a proximity-based authentication on the ad-hoc networks via Wi-Fi communication by calculating Euclidean distance with device service set identifier (SSID), basic service set identifier (BSSID), and RSSI information. Sophia et al. [8] determined the coordinates of four ESP32 devices with a fixed location using RSSI and trilateration algorithm by using BLE based indoor positioning system. This reference [9] is yet another work using the trilateration algorithm to perform an indoor navigation system where a mobile application assists the users to navigate inside a building without the need for external maps or human intervention by using BLE. Dijkstra algorithm is used to indicate the shortest path in their navigation system.

The participation of the students in the class was carried out with location information using Bluetooth [10]. The Bluetooth-based indoor positioning is preferred because of the various easily accessible devices such as mobile phones, smartwatches, and smart wearables with Bluetooth wireless communication technology. Also, Bluetooth has ultra-low power consumption with a small amount of data transmission. Students are registered with their mobile phone's media access control (MAC) address. Fingerprinting technique was used to collect and verify RSSI, and trilateration algorithm was used to calculate the distance using RSSI values.

Wi-Fi-based indoor positioning techniques are indicated with the latest research results by comparing range-based positioning methods and performance in terms of accuracy, complexity, extensibility, and cost [11].

In the paper [12], a random statistical method is proposed to improve the positioning accuracy of IPS using Wi-Fi fingerprinting. And the suggested method is compared with weighted k-nearest neighbor (WKNN) algorithm based on Euclidean distance to indicate the accuracy of indoor positioning. The experimental result of the paper is that the statistical method with the maximum positioning error is less than 0.75 meters, while the average positioning error with the WKNN algorithm is 1.5 meters. Wi-Fi fingerprint positioning technique is mainly described by He and Chan [13]. Different from the application areas of the studies mentioned in the literature, the security of the devices has been tried to be ensured. Wireless communication skills were tested by using an IoT device with limited processing capability instead of the advanced devices used in the studies.

III. Implementation and Testbed

The security need of IoT applications may vary according to the resource constraints of IoT devices and the sensitivity of the data. Our study aims to perform physical tracking of resource-constrained devices that cannot run compute-intense cryptographic algorithms due to the fact that cryptographic algorithms that can ensure data confidentiality and device verification include computations that require processing power. For this purpose, our example case is four ESP32 IoT devices located at fixed points in an indoor area, communicating with each other and transmitting their data to the gateway. It is aimed to ensure that our devices are in their positions without human intervention so that the data flow transmitted from these devices is not interrupted by a physical intervention. ESP32 devices work as both stations and access points. Thus, RSSI signals were collected and sent to the gateway with the MQTT protocol for distance calculation. The fixed position and distance information of our devices are shown in the Figure 1. At the same time, the actual distance information of our devices is recorded on our server with the device's MAC information to compare with the calculated RSSI to distance. Distance from RSSI information was calculated with the following formula [6]. Indicated n in the formula, used as 4 in our calculation, is an external factor varying between 2 and 4.

$$Distance = 10^{\wedge}(Measured\ Power - RSSI)/10*n \quad (1)$$

As seen from Figure 1, four ESP32 devices are positioned to form a rectangular area and act as access points. ESP32 device operating in station (STA) mode is placed in this area and it scans Wi-Fi and collects RSSI data periodically according to the four devices at our reference points. The collected RSSI values related to each device are sent to the gateway located on the Raspberry Pi using the MQTT protocol. And the RSSI values are stored in the server. The server also keeps the actual distance values of the ESP32

devices according to the reference points. Mosquitto is used as the message queue telemetry transport (MQTT) broker and includes added Python script plugin to calculate the distance according to the RSSI-to-distance formula. The most repeated out of 10 collected RSSI values is taken as an input to the formula. The error rate is found by comparing the calculated distance value with the actual distance value.

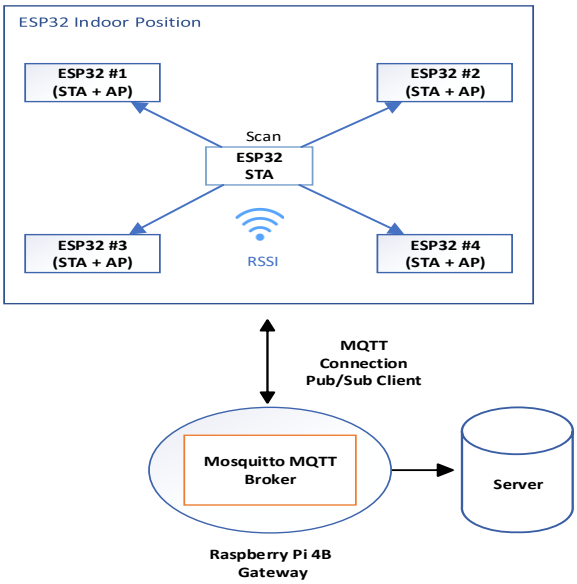

Fig. 1. The component, relation and interaction of indoor position scheme.

The RSSI values of the four reference fixed points are measured as between -61 and -67 that are shown in Figure 2. When the ESP32 device is away from the reference point, the RSSI value gets lower. RSSI values are measured according to the locations within this area where device boundaries are specified. The reference point is determined as respectively 4 and 2, and the situations where the device is inside and outside the area are considered. The device and its reference nodes are examined in 4 cases that are illustrated in Figure 3. The first case is positioned so that the device is outside the reference points. And the actual distance between the device's current location and the reference points is set to more than 1 meter. The purpose is to detect an unauthorized device that does not belong to the application. In this way, the data of the device whose location is not verified will not be included in the network.

```
scan start
scan done
15 networks found
esp1 (-61)*
esp_3 (-64)*
esp_4 (-66)*
esp_2 (-67)*

scan start
scan done
15 networks found
esp1 (-61)*
esp_3 (-66)*
esp_4 (-67)*
esp_2 (-68)*

scan start
scan done
15 networks found
esp1 (-63)*
esp_3 (-64)*
esp_4 (-65)*
esp_2 (-66)*
```

Fig. 2. The output of RSSI value of references nodes at fixed points.

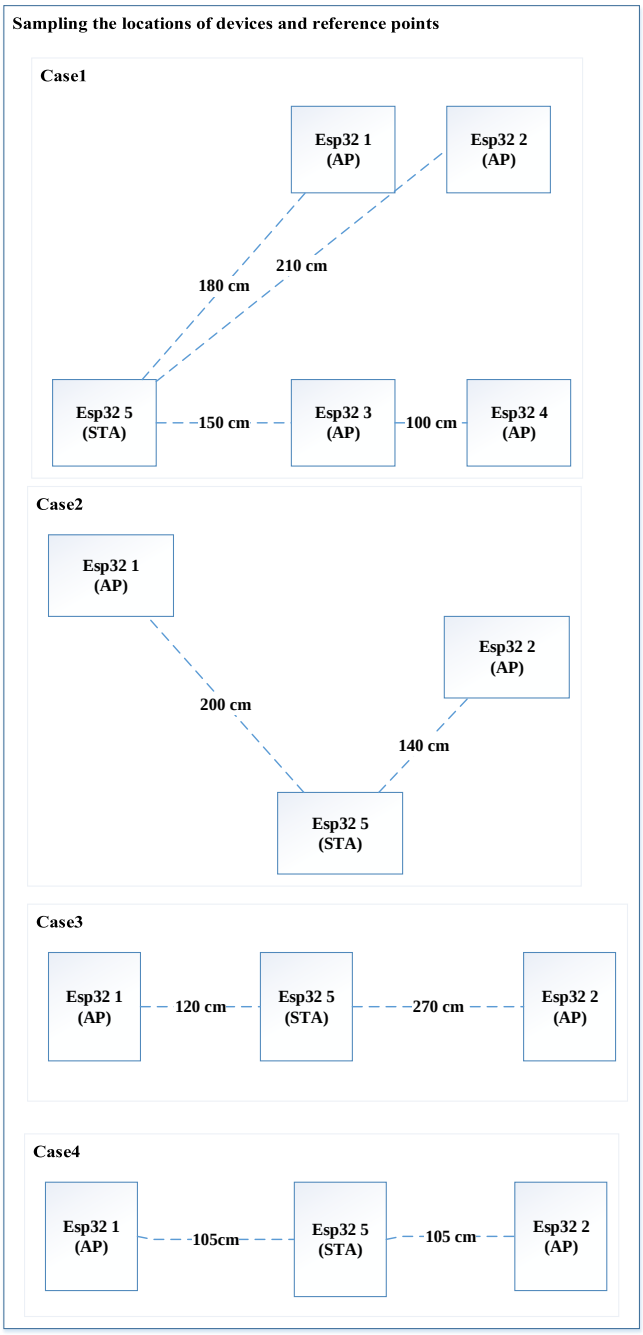

Fig. 3. RSSI value of references nodes at fixed points.

In Case2 and Case3, the number of reference nodes has been reduced to 2 and the device is positioned between the reference points. Distance based on RSSI values is calculated by positioning away from more than 1 meter between reference points and the ESP32 device. And in the last case, the RSSI value was measured at a distance of approximately 1 m between 2 reference points.

The results of RSSI measurement and RSSI-to-distance formula calculation 4 cases are shown in Table 1. The measured power value in the formula means the RSSI value measured at 1m. Considering the actual distance and the calculated distance, the error rate is indicated as a percentage.

TABLE I. ACTUAL DISTANCE COMPARED WITH RSSI-TO-DISTANCE

References Nodes	RSSI	Measured Power	N	Distance (cm)	Result From Calculation (cm)	Distance Error (cm)	Average Error Margin (%)
Case1 - Four References Nodes / ESP32 outside							
ESP32 1	-74	-68	4	180	141	39	20.54
ESP32 2	-85	-68	4	210	266	56	
Esp32 3	-77	-68	4	150	167	17	
Esp32 4	-90	-68	4	250	354	104	
Case2 - Two References Nodes / ESP32 inside							
ESP32 1	-40	-28	4	200	199	1	2.75
ESP32 2	-33	-28	4	140	133	7	
Case3 - Two References Nodes / ESP32 inside							
ESP32 1	-31	-27	4	120	125	5	7.26
ESP32 2	-46	-27	4	270	298	28	
Case4 - Two References Nodes / ESP32 inside							
ESP32 1	-71	-69	4	105	112	7	6.66
ESP32 2	-71	-69	4	105	112	7	

In the first case, as 4 devices are used as access points, the coverage area is much higher than the following cases that also causes higher error rates. Another core reason of the error is the electromagnetic interference as the experiments are not proceeded in a laboratory environment. Also the ESP32 device is not so much stable in wireless communication. In the remaining cases, the error rate is much lower. Considering all the cases, error rates are acceptable to detect whether the device is in the coverage area or not.

IV. CONCLUSION

In our study, unlike cryptographic algorithms that require high processing power to verify devices in IoT applications, physical tracking has been used for a simple authentication. By calculating the distance with the RSSI value, it is examined whether the devices are in the coverage area we have determined. The ESP32 devices are located in a room and have been tested to observe whether there is interference to the network from a device outside the home or not. To experiment this, measurements are taken at different locations according to the reference points of the ESP32 devices. The process is repeated with 2 and 4 nodes at the reference points. While the average RSSI value at a distance of 1 m from the reference points of the ESP32 device is -67 dBm, the RSSI value (-90 dBm) of an external device and its distance calculation shows that the device is not in the coverage area and it is unauthorized. The error rates that occur when detecting that the ESP32 device in its location are negligible due to the fact that the environment is affected by the magnetic field.

In future works, moving devices can be detected in the environment and the physical tracking of the RSSI data collected by both BLE and Wi-Fi communication technologies will be tested by trilateration and fingerprint methods.

REFERENCES

[1] Ö. Şeker and G. Dalkiliç, “Implementation and Performance Analysis of a Multi-Protocol Gateway,” in 2022 Innovations in Intelligent Systems and Applications Conference (ASYU),” pp. 1-6, September 2022.

[2] S. M. Asaad and H. S. Maghdid, “A comprehensive review of indoor/outdoor localization solutions in iot era: Research challenges and future perspectives,” Computer Networks, 109041, 2022.

[3] S. J. Hayward, K. van Lopik, C. Hinde and A. A. West, “A survey of indoor location technologies, techniques and applications in industry,” Internet of Things, vol. 20, 100608, ISSN 2542-6605, 2022.

[4] ESP32-S ESP-IDF programming guide, Jan. 2023, [online] Available: https://docs.espressifcomlprojects/esp-idf/en/v4.2-beta1/esp32s2/esp-idf-en-v4.2-beta1-esp32s2.pdf.

[5] S. Akleylek, E. Kiliç, B. Söylemez, T. E. Aruk and A. Çavuş,“Kapalı mekan konumlandirma üzerine bir çalışma, ” Mühendislik Bilimleri ve Tasarım Dergisi, vol. *8*(5), pp. 90-105, 2020.

[6] S. R. Misal, S. R. Prajwal, H. M. Niveditha, H. M. Vinayaka and S. Veena, “indoor positioning system (IPS) using ESP32, MQTT and Bluetooth,” in Fourth International Conference on Computing Methodologies and Communication (ICCMC),” pp. 79-82, March 2020.

[7] A. A. S. AlQahtani, H. Alamleh and B. Al Smadi, “IoT Devices Proximity Authentication In Ad Hoc Network Environment,” in International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1-5, June 2022.

[8] S. Sophia, B. Maruthi Shankar, K. Akshya, AR. C. Arunachalam, V. T. Y. Avanthika and S. Deepark,” Bluetooth Low Energy based Indoor Positioning System using ESP32,” in Third International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 1698-1702, 2021.

[9] A. Rakshith, V. H. Navneeth, P. S. Dravya, K. U. Holla, K. N. Pushpalatha, “Indoor Navigation System using BLE and ESP32,” in International Journal for Research in Applied Science & Engineering Technology (IJRASET), November 2020.

[10] A. Puckdeevongs, N. K. Tripathi, A. Witayangkurn and P. Saengudomlert,” Classroom Attendance Systems Based on Bluetooth Low Energy Indoor Positioning Technology for Smart Campus,” Information, vol. 11(6):329, 2020, https://doi.org/10.3390/info11060329.

[11] F. Liu, J. Liu, Y. Yin, W. Wang, D. Hu, P. Chen and Q. Niu,” Survey on WiFi-based indoor positioning techniques,” The Instution of Engineering and Technology, vol. 14(9), pp. 1372-1383, 2020.

[12] D. B. Ninh, J. He, V. T. Trung, D. P. Huy, “An effective random statistical method for Indoor Positioning System using WiFi fingerprinting, ”Future Generation Computer Systems, vol. 109, pp. 238-248, 2020.

[13] S. He and S. H. G. Chan, “Wi-Fi Fingerprint-Based Indoor Positioning: Recent Advances and Comparisons,” IEEE Communications Surveys & Tutorials, vol. 18(1), pp. 466-490, 2016.