Locker-Scale Positioning and Dynamic Access Key Management for IoT-based Smart Delivery Services

Woojin Park*, Hyeyoung An*, Soochang Park*, and Euisin Lee†
*Department of Computer Engineering, Chungbuk National University, Cheongju, Republic of Korea
†School of Information & Communication Engineering, Chungbuk National University, Cheongju, Republic of Korea
Email:*{woojin415, elinyoung, cewinter}@chungbuk.ac.kr † elsee@chungbuk.ac.kr

***Abstract*—The delivery service has become an essential service for daily use. Customers can purchase items easily and conveniently through the delivery service. The advantage of the delivery service is that the item someone purchases is delivered to the recipient's house. So, the recipient doesn't have responsibility for going to a market to buy something. Additionally, even if the recipient does not stay house, he/she can receive the parcel by using an Unmanned Delivery Locker (UDL). Almost UDL is used as an access key, such as a password, QR code, etc., to open the locker. The access key is used to prevent non-designated persons from opening locker doors. However, if the access key is leaked, the security of the parcel is at risk. To address this issue, this paper comes up with a novel delivery system using a dynamic access key management scheme based on locker-scale positioning. The system does not provide an access key to the recipient when the parcel is stored. Instead, the access key is provided to the recipient at a time when he/she arrives at the UDL. To identify that the recipient has arrived at UDL, the positioning with Bluetooth Low Energy (BLE) is used and experimented with. The results of an experiment show that the accuracies are achieved 86.67% with 4 lockers, 89.61% with 6 lockers.**

***Index Terms*—Parcel delivery, Positioning, Bluetooth Low Energy (BLE), Machine-learning**

I. Introduction

The development of the internet enables people to send requests remotely without having to go somewhere to request something. It allows individuals to order a wide variety of items from the comfort of their homes using devices connected to the internet. It provides convenience and a chance, which people to buy something without location constraints. Furthermore, advancements in transportation have made it possible for individuals to receive parcels quickly and conveniently at their doorsteps. For these advantages, systems such as grocery delivery, parcel delivery, and food delivery have grown rapidly. In addition, delivery method such as contactless delivery [1], delivery scheduling [2], drone delivery [3] are also being continuously researched.

In a traditional delivery system, the recipient is requried to remain at home to receive their ordered items. However, it is difficult to predict the parcel's arrival time. If the delivery person leaves the parcel at the recipient's doorstep when the recipient is not at home, it's at risk of being stolen. To resolve this theft problem, an Unmanned Delivery Locker (UDL) is proposed. If the recipient sets a designated destination where the UDL is located, the delivery person delivers the parcel to the UDL at the destination. When the recipient receives the parcel, the recipient uses his access key to open the UDL and takes the parcel. Thanks to the UDL, the recipient can receive the parcel without considering arrival time.

Various methods are used to authenticate locker access authority using access keys, such as phone number, passcode [6], QR Code [7], etc. In these methods, the access key is provided to the recipient when the delivery person deposits the parcel in the locker. Then, the recipient goes to the UDL and opens the locker to take the parcel. It is worth noting that the above methods generate and provide the access key to the recipient as soon as the parcel is stored in the UDL. So, if the access key is leaked before the recipient takes the parcel, there is a risk that the parcel can be stolen. However, it cannot do that the system does not provide the access key to prevent the access key leakage. Because the recipient cannot open the locker without the access key. To mitigate this problem, a new method to provide the access key is required.

The timing of access key distribution to the recipient needs adjustment to solve the aforementioned problem. Since the problem arises before the recipient receives the parcel, the most appropriate time to provide the access key is when the recipient arrives at the UDL. Importantly, the recipient doesn't possess the access key and cannot use it until they receive it. To verify the recipient's presence at the UDL, a positioning approach is used. Among these approaches, Bluetooth Low Energy (BLE) is a widely used method [4], [5]. BLE offers several advantages, including the fact that most smartphones come equipped with BLE modules, and the cost of deploying BLE beacons is relatively low.

We propose a novel system with dynamic access key management based on locker scale positioning. The characteristic of the system is that the access key is only provided to the recipient upon their arrival at the UDL. Because the recipient doesn't possess the access key until their arrival, the risk of access key leakage is minimal. Of course, the access key is generated when the delivery person delivers the parcel to the UDL and is stored on the local server. The positioning method using the BLE is used to identify the recipient arriving at the locker of the UDL. If the recipient arrives at the locker, the system provides the access key to the recipient. Additionally, we experiment with locker-scale positioning using BLE beaons and smartphones.

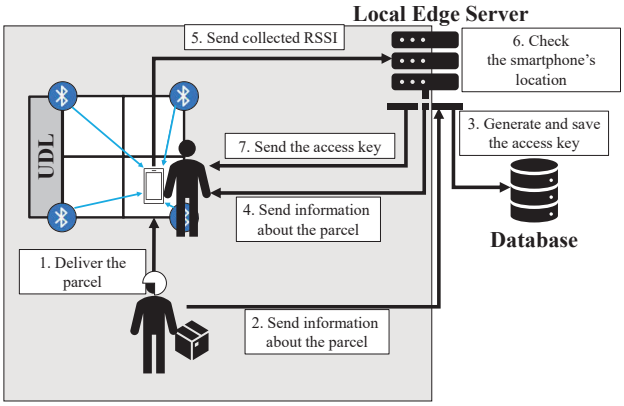

Fig. 1. System architecture

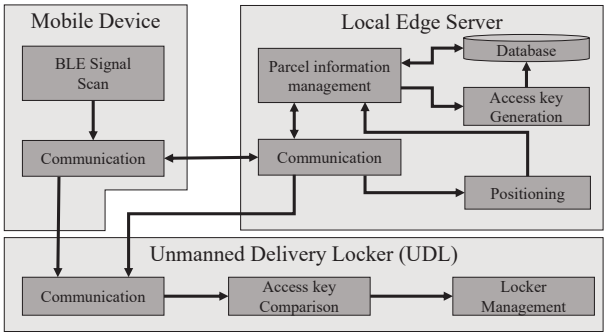

Fig. 2. Framework

II. Related work

In this section, previous studies on locker systems for storing items are explained. Nonthaputha et al. propose the smart box using Arduino [6]. The smart box is linked to the recipient's mobile phone and can deliver storage information about the parcel to the recipient. The passcode is used to open the smart box. Alghfeli et al. propose a smart delivery system for secure parcel delivery [7]. The system includes the smart box and mobile application, which provides information about the parcel. When the recipient receives the parcel, a QR code is used to open the smart box. In [8], a parcel delivery locker with C51 CMU and GSM/GPRS is proposed. The locker generates the password when the parcel is stored. After that, the GSM module will send the password to the phone number. In [9], a smart post box system based on RFID is proposed. The delivery person has RFID card that can open all lockers and the recipient has RFID card that is used to open the locker. The work in [10] focuses on facilitating the sharing of lockers among selected individuals. Users can transmit access keys, which are used to open specific lockers, to others via a LINE bot. The work in [11] makes a smart key box that stores several physical keys. By using the bar-code in the identity card, users can borrow and return the physical key. The identity card should be registered with the system before use.

The above research uses various access key that allows the recipient to open the door of the locker. However, consideration of access key leakage is lacking. If the access key is leaked, the reason for using a delivery locker becomes meaningless due to the risk of theft. Therefore, the proposed system focuses on preventing access key leakage to ensure the security of the parcel delivery process.

III. System Design

A. System Architecture

The proposed system aims to mitigate the potential risk of access key leakage. The system should not give an access key to the recipient before the recipient arrives at the parcel. The system solely provides the recipient with information regarding the whereabouts of the stored parcel. Because the system does not give an access key from the beginning, it is important to select the time when the access key is provided to the user without the risk of access key leakage. In the system, to arrive at the recipient at the UDL is a condition that the access key can be given to the recipient without the risk of leakage.

Fig. 1 illustrates a system architecture representing system flow. The system consists of the delivery person, the recipient, the UDL, and the local edge server. First, the delivery person delivers the parcel to the UDL and sends information about the parcel, such as the UDL's location, the locker number where the parcel is stored, etc., to the server. The server generates and stores the access key to open the locker and sends the location information of the parcel to the recipient. When the recipient arrives at UDL by referring to the location information received, the recipient places his/her smartphone at the location where the parcel is stored. Then, the smartphone collects the RSSI values of the BLE beacons placed in UDL and transmits them to the server. The server uses RSSI to verify that the smartphone's location is the same as the parcel's location. If the location is the same, the access key in the server is transmitted to the recipient. The recipient opens the locker to use the access key and receives the parcel.

Generating the access key can be done in a variety of ways such as passwords, QR codes, OTP, etc. Depending on what type of access key is used, the way the recipient authenticates will also vary. However, the type of access key is not discussed in the paper. This is because the topic covered in this paper focuses on when access keys are provided rather than what types of access keys are used.

B. Framework

Fig. 2 illustrates a framework that shows the modules performed on mobile devices, UDLs, and local edge servers and the relationships between them. The mobile device consists of the "BLE signal scan" module and the "Communication" module. The "BLE signal scan" module is performed to collect RSSI data from the BLE beacon's signal. By using this module, the mobile device collects RSSI data per each

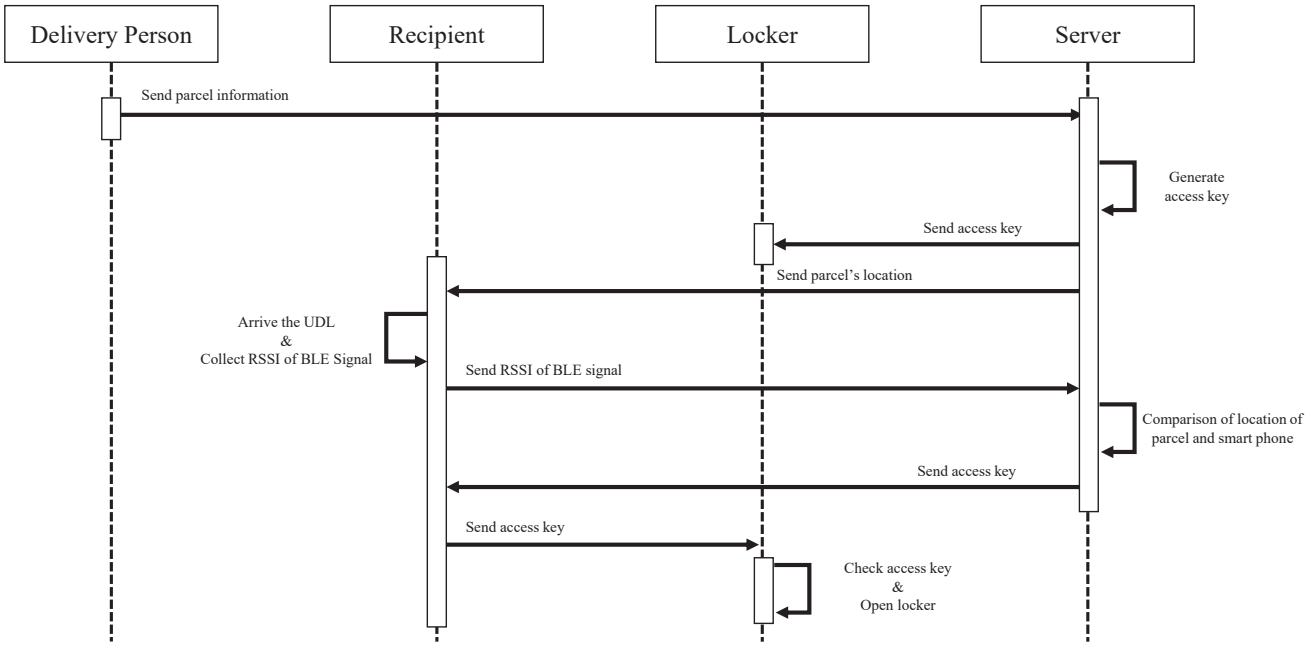

Fig. 3. Sequence diagram for access key management

beacon, which is deployed at the UDL, and passes it to the "communication" module. The mobile device's "communication" module sends RSSI data to the local edge server or sends the access key to the UDL. By using the "communication" module, the mobile device gets the access key from the local edge server.

The server consists of the "Communication" module, "Parcel information management" module, "Positioning" module, "Access key generation" module, and a database. In the "communication" module, RSSI data from the mobile device is passed to the "Positioning" module, and parcel information from the delivery person's mobile device is passed to the "Parcel information management" module. Additionally, this module sends the access key to the mobile device or the UDL. The server's "Parcel information management module" manages the states of the parcel. When the server receives parcel information from the delivery person, the server uses the "access key generation" module to generate the access key and stores the information in the database. When the server receives the RSSI value from the recipient, the "Positioning" module is used to estimate the position of the recipient's smartphone. When the "Positioning" module estimates the position using RSSI, the machine-learning model is used. The "Parcel information management" module compares the estimated position and the parcel's position. If the estimated position is the same as the parcel's location, the server sends the access key in its database to the recipient.

The UDL consists of the "Communication" module, "Access key comparison" module, and "Locker management" module. The UDL's "Communication" module receives and stores the access key from the server, or receives the access key from the recipient and passes it to the "Access key comparison" module. In "Access key comparison" module, checks whether the access key received from the server and stored is the same as the access key received from the recipient. If the above two access keys are the same, the locker that stores the parcel is opened using the "Locker Management" module.

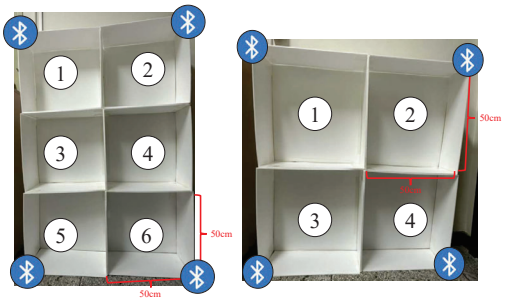

Fig. 4. The UDL settings with 4 BLE beacons

C. Sequence diagram

A sequence diagram representing the communication between system components, such as delivery person, recipient, locker, and server, is shown in Fig. 3. At the time the delivery person stores the parcel to the UDL, information about the

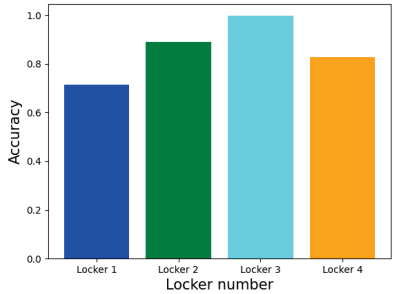

Fig. 5. The accuracy of measuring the smartphone's location per each lockers when 4 lockers are used

	Locker 1	Locker 2	Locker 3	Locker 4
Locker 1	**214**	16	1	1
Locker 2	46	**267**	0	47
Locker 3	32	0	**299**	4
Locker 4	8	17	0	**248**
Accuracy	0.713	0.89	0.997	0.826

Fig. 6. Confusion matrix of measuring the smartphone's location per each lockers when 4 lockers are used

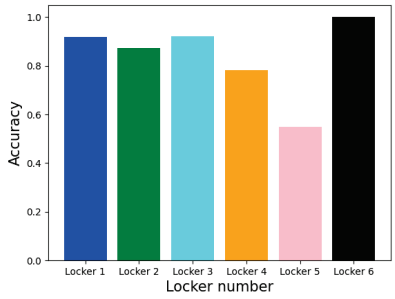

Fig. 7. The accuracy of measuring the smartphone's location per each lockers when 6 lockers are used

	Locker 1	Locker 2	Locker 3	Locker 4	Locker 5	Locker 6
Locker 1	**275**	37	0	37	0	0
Locker 2	4	**262**	0	0	0	0
Locker 3	0	0	**276**	9	0	0
Locker 4	21	1	24	**235**	0	0
Locker 5	0	0	0	0	**165**	0
Locker 6	0	0	0	19	135	**300**
Accuracy	0.917	0.873	0.92	0.783	0.55	1

Fig. 8. Confusion matrix of measuring the smartphone's location per each lockers when 6 lockers are used

parcel, such as the recipient's name, phone number, locker number, etc., is sent to the server by the delivery person's mobile device. After the server identifies the parcel that is stored in the locker, the server generates and stores the access key that is used to open the locker. The access key is only sent to the locker. The locker stores it and will use it to authenticate the recipient. The recipient only receives the information about the parcel's location. The reason the access key is not provided to the recipient is to prevent leakage of the access key. The recipient moves to the UDL and uses a smartphone to collect RSSI values from the BLE beacons deployed on the UDL. After collecting data from each beacon, it is sent to the server. In the server, the smartphone's location is measured with the RSSI, and the location is compared with the parcel's location. If it is the same, the server sends the access key to the recipient. The recipient uses the received access key to open the locker.

IV. Experiment Environment

Timing for providing the access key to the recipient from the server is a critical process in the proposed system. In this process, the location of the recipient's smartphone is utilized in the process that the system gives the access key to the recipient. In order to receive the access key to open the locker, the recipient should place their smartphone exactly in the locker where their parcel is located. If the estimated position of the smartphone is the same as the parcel's location, the system provides the access key to the recipient. Therefore, the system is affected by the accuracy of measuring the smartphone's location. So, an experiment about measuring the smartphone's location is implemented in this paper.

The experiment setting is shown in Fig. 4. Experiments were conducted with 4 and 6 lockers of size 50 x 50 cm. The BLE beacons are placed at the 4 vertices of UDL. The beacon's Tx power and broadcasting interval are set to 0dBm and 100ms, respectively. Because a method to measure the smartphone's location uses RSSI of BLE signals, RSSI is collected using a smartphone, which is Galaxy S7, for each locker. The position where the smartphone collects RSSI data is the center of each locker. 1000 RSSI data set is collected for each locker. 700 data set is used to train the machine-learning model and 300 data set is used to estimate the accuracy. When the smartphone collects RSSI data, its location is in the center of the locker. Multi-layer perceptron (MLP) is used in the machine-learning model. The tensorflow library is used to implement the machine-learning model. The input data consists of 4 RSSI data that are collected for each beacon.

V. Results

A. Accuracy

In this section, results for locker-scale positioning using the smartphone and BLE beacon are shown. Fig. 5 shows the accuracy of measuring the smartphone's location when 4 lockers are used. All of the accuracy per locker achieves over

70% accuracy. The average accuracy is 85.56%. A confusion matrix is shown in Fig. 6. Examining the confusion matrix, it can be seen that most positioning errors are caused by mistaking them for adjacent lockers.

Fig. 7 shows the accuracy of measuring the smartphone's location when 6 lockers are used. All of the accuracy per locker achieves over 50% accuracy. The average accuracy is 89.61%. As a result, both environments achieved an average accuracy of over 85%. Although the result of 6 lockers has a higher average accuracy than the result of 4 lockers, the accuracy of locker 5 has the lowest accuracy. A confusion matrix is shown in Fig. 8. Examining the confusion matrix, it can be seen that most positioning errors are caused by mistaking them for adjacent lockers. In the case of locker 5, especially, it is visibly confirmed that the position in locker 5 is incorrectly measured as the position in locker 6.

Smartphone positioning errors may affect the system but are not a critical problem. Because the system does not provide the access key when the measured smartphone's location is not the same as the parcel's location. If the recipient does not receive the access key, the recipient just sends RSSI data again while the access key is provided. Of course, it has a negative impact on the convenience of users who use the system. Therefore, increasing the accuracy for measuring the smartphone's location is one of the future works.

B. Time

The proposed system provides the access key when the recipient arrives at the UDL. This means that the recipient has an additional process for using the UDL. Therefore, the recipient spends more time obtaining access keys compared to traditional system at the field. Fig. 9 shows the difference in execution time between the proposed system and the traditional system. The proposed system needs additional time for the positioning process, such as BLE scan, Model query, and Access key transmission, compared to the traditional system. The process of the proposed system after receiving the access key is the same as the traditional system. So, the times such as access key check, enter access key, and locker open are the same for the proposed system and the traditional system. As a result, the proposed system consumes 463 ms more time than the traditional system.

VI. Conclusion

This paper proposes a novel delivery system using dynamic access key management based on locker-scale positioning. The system aims to prevent the risk of access key leakage before the recipient receives the parcel. A fundamental reason why the access key is leaked is that the access key is provided to the recipient when the parcel is stored in the UDL. So, the access key leakage can occur between the time the parcel is stored and the recipient goes to receive it. To solve this problem, the system provides the access key to the recipient when the recipient arrives at the UDL. Because the recipient does not have the access key until he/she arrives at the UDL, the access key leakage does not occur. To confirm that the recipient has arrived at UDL, the positioning technique using a BLE beacon signal and machine-learning technique is used. As a result, the positioning accuracy achieves 86.67% when 4 lockers are used and 89.61% when 6 lockers are used.

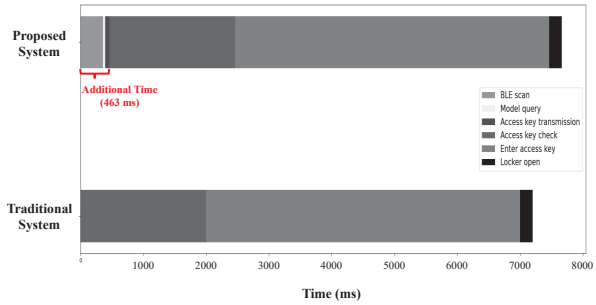

Fig. 9. Execution time comparison between proposed system and traditional system

If an error occurs in the measuring location, it is inconvenient for the recipient to send the data again. Therefore, increasing the accuracy of the measuring location is our future work.

References

[1] W. Park, S. Park, D. Lee, T. Yang and S. -H. Kim, "Inter-Twin Connectivity for Digital Twin Networks in Secure Contactless Delivery Service Scenarios," *Proc. of 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, 2023, pp. 1-5.

[2] J. Kwon and J. Jeong, "A Parcel Delivery Scheduling Scheme in Road Networks," *Proc. of 2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 1750-1755.

[3] M. Perreault and K. Behdinan, "Delivery Drone Driving Cycle," *in IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1146-1156, Feb. 2021.

[4] E. Essa, B. A. Abdullah and A. Wahba, "Improve Performance of Indoor Positioning System using BLE," in *Proc. of 2019 14th International Conference on Computer Engineering and Systems (ICCES)*, pp. 234-237, 2019.

[5] Y. Bae and D. Shin, "BLE-Based Indoor Positioning Using Extended Advertisement," in *Proc. of 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, pp. 667-670, 2022.

[6] T. Nonthaputha, M. Kumngern, J. Phookwantong and S. Keawwang, "Arduino Based Smart Box for Receiving Parcel Posts," *Proc. of 2020 18th International Conference on ICT and Knowledge Engineering (ICT&KE)*, 2020, pp. 1-5.

[7] M. Alghfeli, M. Alnuaimi, N. Alsebaiha, S. Alnuaimi, B. Pradeep and P. Kulkarni, "DroParcel: Smart System for Secure Parcel Delivery," *Proc. of 2022 IEEE 12th International Conference on Consumer Electronics (ICCE-Berlin)*, 2022, pp. 1-6.

[8] S. Ze-hong and Z. Guang-yuan, "Multi-functional Parcel Delivery Locker system," *Proc. of 2015 International Conference on Computer and Computational Sciences (ICCCS)*, 2015, pp. 207-210.

[9] A. Plašilová and J. Procházka, "RFID-based Multi-purpose Smart Post Boxes in Smart Cities," *Proc. of 2022 6th International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2022, pp. 184-189.

[10] J. Sa-ngiampak et al., "LockerSwarm: An IoT-based Smart Locker System with Access Sharing," *Proc. of 2019 IEEE International Smart Cities Conference (ISC2)*, 2019, pp. 587-592.

[11] T. Nonthaputha, U. Torteanchai, M. Kumngern and J. Phookwantong, "Design of Smart Key Box Using IoT," *Proc. of 2021 19th International Conference on ICT and Knowledge Engineering (ICT&KE)*, 2021, pp. 1-4.