Hybrid AI-Based iBeacon Indoor Positioning Cybersecurity Attacks and Defenses Thereof

Fang-Yie Leu[1], Chi-Jan Huang[2], Cheng-Jan Chi[3], and Wei-Tzu Hung[4(✉)]

[1] Department of Computer Science, Tunghai University, 407224 Taichung, Taiwan
[2] General Education Center, Ming Chuan University, 111013 Taipei, Taiwan
[3] THLight Company, Ltd., 241409 New Taipei, Taiwan
[4] Department of Civil Engineering, National Taipei University of Technology, 106344 Taipei, Taiwan
jones155376jones@gmail.com

Abstract. Currently, iBeacon systems have been increasingly established in public areas to position people and assist users in indoor for location navigation. People receive the services through the Bluetooth Low Energy (BLE) installed on their mobile phones. However, the positioning and navigation functions of iBeacon system may be compromised when faced with cyberattacks issued by hackers. In other words, its security needs to be further considered and enhanced. This study takes the iBeacon system built in Taipei Main Station, the major transportation hub with daily traffic of at least 300 thousand passengers, as an example for exploring its potential attacks and further studying on the defense technologies under the assistance of AI techniques and human participation. Our experiments demonstrate that the prior information security planning of a iBeacon system and the rolling coding encryption on its issued messages in Taipei Main Station, are the best defense methods.

Keywords: cyberattacks · BLE · information security · rolling encryption · hybrid AI-based · iBeacon systems

1 Introduction

In general, Beacon is a small data transmitter developed for low-power applications of Bluetooth (4.0 and above). It is suitable for being applied to indoor positioning, which solves the problem in that GPS of a mobile phone is unable to receive satellite signals indoors due to obstruction by the building. More importantly, people consider that Beacon systems are the new generation solutions [1] as it meets the accuracy requirements of indoor positioning at a lower power consumption compared to those outdoor positioning systems.

Gradually, applications of iBeacon and BLE Beacon have been increasingly popular on mobile devices since a majority of these devices are with built-in Bluetooth protocol. The potential applications include shopping mall navigation [2] and vehicle management and identification [3]. The higher expansion of iBeacon and BLE Beacon applications

D.-J. Deng et al. (Eds.): SGIoT 2022, LNICST 497, pp. 65–71, 2023.
https://doi.org/10.1007/978-3-031-31275-5_7

often lead to higher risks to these applications. At present, the security issues faced in the use of Beacon include spoofing, piggybacking and privacy concerns, etc. [4]. Also, indoor positioning requests high positioning accuracy and signal availability and accessibility.

As there are rare iBeacon security research involving information security, this study will therefore focus on the information security features of iBeacon and introduce the possible attacks by hackers and their defense approaches.

2 Related Work

2.1 Safety Promotion of iBeacon

Bai et al. [5] proposed an iBeacon base station containing a Bluetooth 4.0 module and an emergency evacuation system to accurately locate users whose mobile phones are now connected to this base station for receiving Bluetooth services, thus able to guide them for evacuation from their current locations when a disaster occurs. Chen & Liu [6] designed a system to guide the evacuation of indoor people, and track the items left by people during the evacuation through the sensor network composed of iBeacon nodes.

Recently, the world's first indoor navigation and evacuation framework with iBeacon IoT positioning has been released to the markets [7]. It can calculate the shortest path from the emergency exits to shorten the time for personnel evacuation so as to safely navigate the user groups to outdoor.

2.2 Information Security Challenges in iBeacon

BLE is a part of Bluetooth 4.0 which is different from the conventional Bluetooth protocols and can be applied to various wearable devices, such as Beacon [8]. However, compared with other BLE technologies, Beacon can be widely applied to various areas/domains due to its low cost and accurate object location identifications. Campos-Cruz et al. [9] analyzed potential threats faced in the practical operation of wireless Beacon systems, and proposed a lightweight cryptography-based security protocol for establishing shared keys. Na et al. [10] revealed the feasibility of attacking iBeacon services via WiFi devices.

3 Research Design

Taipei City is the largest political and economic center in Taiwan, and Taipei Main Station, also the transportation hub for foreign travelers entering and leaving Taipei City. In 2019, the daily passenger traffic of Taipei Main Station consists of 86,000 via high-speed rail, 122,000 via Taiwan Railway, and 319,000 via MRT.

Due to the design of pedestrian passing routes and signs in Taipei Main Station have been increased day by day, the Taipei City Government launched the APP "Taipei Navi" in 2018, which connects to more than 4,000 iBeacons deployed across the station to solve issues such as passenger positioning, wayfinding and commuting. This study therefore adopts Taipei Main Station as the subject in exploring iBeacon security issues.

3.1 iBeacon System Design Architecture

The design architecture of the iBeacon system in this study is shown in Fig. 1. First, the Beacon plaintexts (e.g., a restaurant promotion advertisement) are encrypted by invoking AES algorithm and then transmitted to mobile phones via the BLE protocol through broadcast before encrypted plaintext is transmitted to the server of this iBeacon system for decryption. After that, mobile-phone users may therefore receive the content of plaintext from the server and decide whether to dine at the restaurant or not. Users wishing to have their needs at one of the promoted restaurants may be guided to this restaurant using the indoor navigation function of App Taipei Navi.

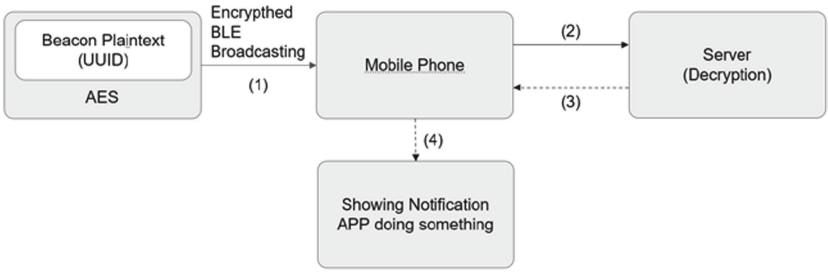

Fig. 1. System diagram of our iBeacon system.

3.2 Positioning Algorithms

The Stage 1, Initial, refers to determining the initial point of a mobile phone. Each Beacon computes its distance to the mobile phone according to the strength of the radio wave and then the Beacon system employs the triangulation method to determine the position of the mobile phone. The strengths are presented in log scale.

The coordinate positioning equations are as follows:

$$x_0 = \frac{\sum_{i=1}^{n} x_i W_i}{\sum_{i=1}^{n} W_i} \; n = 3 \tag{1}$$

$$y_0 = \frac{\sum_{i=1}^{n} y_i W_i}{\sum_{i=1}^{n} W_i} \; n = 3 \tag{2}$$

Following the completion of the initial point positioning, it is discovered that instant computation of current location of users is difficult since the Beacon positioning system may only compute the relative position between each Beacon and the mobile phone, while the radio waves require average based on stable readings.

For better user experience, this system refers to Kok et al. [11] in Stage 2 by acceleration computations run by accelerators. In this study, an algorithm is applied to integrate the acceleration from the user's phone position into a velocity which will receive second integration to transform the velocity to a displacement so that a position with the movement direction can be determined according to the gyroscope angle.

Stage 3 concerns data regression. The results gained from stage 2 "Estimate" estimates over user's position once every 30 s. The results are compared with the Initial Points identified in Stage 1. In addition, the Beacon value shall prevail when the error exceeds 15 m since the errors of the accelerometer are accumulated. For specific Beacons, such as the ones near an escalator, Regression will be executed immediately upon numerical strength excess over 70 dB since the user will soon move to another floor when riding the escalator and they will be at near proximity to Beacons as they come near to the floor. At such moment, the Beacon radio wave strength goes extremely high, and a rapid regression, also known as quick regression, is required.

3.3 Hybrid-AI-Based Positioning Algorithm

In the real field, mobile phones will continuously receive values from more than one Beacon. To solve this problem, this system applies a Hybrid AI-based scheme to our positioning algorithm.

In Stage 1, the Hybrid AI-based positioning algorithm will set the location of the mobile phone to a "N × N" square, and the brightness will be proportional to the signal strengths received, hence forming a graph.

In Stage 2, there are 6,500 groups of 80 × 80 squares in the railway station. In this study, strength values are stored per second, and the average strengths every seven seconds as one cycle are mapped into this graph, which will be submitted to TensorFlow immediately [12]; CNN in TensorFlow is then applied for point identification.

In Stage 3: The Hybrid AI-based positioning algorithm will transform the position of a user's mobile phone to a radio wave strength graph. The positions of the Beacons with the strongest wave signal are identified as the user's current position.

3.4 Possible Attacks

Recording and Use. From technical viewpoint, any mobile phone which has BLE protocol can receive and decode the message from the iBeacon system, meaning any mobile application which can obtain the Beacon broadcasts is able to position this mobile phone. Therefore, hackers may use such channel to leak the positioning information. That is, a hacker may walk in the field holding a smartphone to fetch field Beacon codes (ID). Any attacker may enter the field open to the public to obtain data without any beforehand permission.

Impersonation Attack. Beacon broadcasts messages usually are not encrypted, an attacker can detect and replicate the Beacon codes. An attacker can hack a Beacon first and then attack the users who are connected to this Beacon. He/she may even replicate a faked Beacon at another field using the same ID when possible, causing the APP to distribute wrong information in the wrong place.

Obfuscation Attack. Hackers put multiple Beacons at the same location. Since applications mostly rely on Beacon to determine their position, when multiple faked Beacons and Beacons under the original system are placed in the same position, the situation may cause serious interference or delay in the transmission, and affect the integrity and correctness of the data.

Recording and Limited Reproduction. The three types of attacks above can be prevented via rolling coding. However, rolling coding can also be attacked by means of limited reproduction, hackers can record a set of several codes at most for time concerns.

4 Beacon System Defense Methods

This study proposes four methods to defense those attacks mentioned above.

4.1 Data Encryption/Decryption

This method involves simple steps by encrypting Beacon messages and decrypting them by the receiver; however, such method is meaningless in the security of the system, since all the attacks above may still work as long as the issued messages remain unchanged.

4.2 Rolling Coding

This Rolling coding can be divided into two models, i.e., unpredictable and predictable. Unpredictable model means that the code will not be repeated at all; predictable code refers to the code produced following some rules.

The classic descriptive equation of rolling coding is

$$f(t) = f(t+1) \tag{3}$$

Unpredictable Rolling Coding. In the unpredictable model,

$$f(t+1) = g(t,\ \text{random}) \tag{4}$$

For example, assuming that the Beacon number is expressed by Code t, and "random" refers to a certain random variable which is a random number for enhancing system security. This series of code can be described as

$$f(t+1) = g(\text{code},\ \text{random}) \tag{5}$$

For example, f(t + 1) = (000,632), and after 10 min f(t + 1) = (000,787). The variation from (000,632) to (000,787) shows no regularity.

Let g = AES, then

$$f(t+1) = \text{AES}(\text{code},\ \text{random}) \tag{6}$$

The parameter random of the encrypted variable code may not be applied to predict the next code result even AES is cracked.

Predictable Rolling Coding Method. In the predictable model, f(t + 1) in Eq. (3) is the code existing regularity. Generally, the change is once every 10 min, and the count is incremented by 1, i.e., t + 1. For example, assuming that the coding position is the date, i.e., t, plus 1, and today is the 5th day of the month, t = 5, f(t + 1) = f (6). The purpose is to reduce the risk of the code being accessed and hacked. It also increases the security of the system.

Basically, predictable rolling coding is added with the predictable mark of Origin = O(code, index, random), i.e., index. For Origin = O(code, index, random) in the original text, the random can be omitted. For example, Eddystone uses PDU Count/Time as an index [13] in Beacon. Line Beacon not only has a timestamp in the plaintext, but also adopts the SHA256 encryption function to encrypt messages. The key length of SHA256 encryption function is 256-bits. It is hard for hackers to crack this function [14].

The advantage of using the predictable rolling coding method is to distinguish whether a message is false or not through timestamps. However, these parameters must be stored in the Flash ROM, and the number of Flash accesses is limited, excessively frequent accesses will damage the hardware [12]. The system owner must carefully consider flash's life time and limit the number of changes.

In the meantime, the watchdog/battery replacement may cause the timestamp to be zero in practical management. When detecting impersonation attack or obfuscation attack, the server must detect whether the constraint T-T' $>$ ΔT or not. The system administrator shall be warned for further processing. Basically, personnel inspections and active monitoring by App are probable solutions.

App Active Monitoring. The APP "Taipei Navi" has accumulated more than 100,000 downloads since its release. The messages received by users using the App from iBeacon will be aggregated into the server at the back end of iBeacon. As shown in Fig. 2, we can compare timestamps for checking to see whether the iBeacon is under a replay attack and then the location of the attacked iBeacon can be identified.

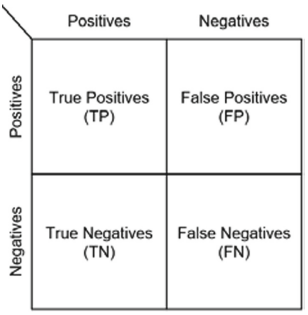

Fig. 2. Confusion matrix.

5 Conclusion and Future Studies

iBeacon is widely used to this date and available for any mobile device that supports BLE; nevertheless, how to protect its security? This study only explores the mainstream iBeacon defenses and attacks due to length constraints of this article. In the future, we will further study the feasibility of other AI-based technologies applications to iBeacon information security protection; furthermore, security personnel on patrol in the station is an intuitive strategy. Therefore, we will also understand the defense method for personnel inspection in our future study.

References

1. Kao, C.L.: The application of beacon micro positioning technology. Arch. Semiannual **20**(1), 88–97 (2021)
2. Meliones, A., Sampson, D.: Blind museum tourer: a system for self-guided tours in museums and blind indoor navigation. Technologies **6**(1), 4 (2018)
3. Zhao, Z.H., Zhang, M.D., Yang, C., Fang, J., Huang, G.Q.: Distributed and collaborative proactive tandem location tracking of vehicle products for warehouse operations. Comput. Ind. Eng. **125**, 637–648 (2018)
4. Spachos, P., Plataniotis, K.: Beacons and the City: Smart Internet of Things, 1st edn. Academic Press, USA (2018)
5. Bai, D.T., Zhang, J.N., Pan, Y.: Research on the principle and technology of indoor positioning navigation escape rescue system. Fire Sci. Technol. **37**(11), 1560–1563 (2018)
6. Chen, L.W., Liu, J.X.: EasyFind: a mobile crowdsourced guiding system with lost item finding based on IoT technologies. In: International Conference on Pervasive Computing and Communication Workshops, pp. 343–345. IEEE, Japan (2019)
7. Chen, L.W., Liu, J.X.: Time-efficient indoor navigation and evacuation with fastest path planning based on internet of things technologies. IEEE Trans. Syst. Man Cybern. Syst. **51**(5), 3125–3135 (2021)
8. Yang, Q., Huang, L.: Inside Radio: An Attack and Defense Guide, 1st edn. Springer, Singapore (2018)
9. Campos-Cruz, K.J., Mancillas-López, C., Ovilla-Martinez, B.: A lightweight security protocol for beacons BLE. In: 18th International Conference on Electrical Engineering, Computing Science and Automatic Control, pp. 1–6. IEEE, Mexico (2021)
10. Na, X., Guo, X., He, Y., Xi, R.: Wi-attack: cross-technology impersonation attack against iBeacon services. In: 18th Annual IEEE International Conference on Sensing, Communication, and Networking, pp. 1–9. IEEE, Italy (2021)
11. Kok, M., Hol, J.D., Sch, T.B.: Using inertial sensors for position and orientation estimation. Found. Trends Signal Process. **11**(1–2), 1–153 (2017)
12. Hu, J., et al.: Efficient graph deep learning in tensorflow with tf_geometric. In: 29th ACM International Conference on Multimedia, pp. 3775–3778. Association for Computing Machinery, China (2021)
13. Sun, M., Kamoto, KM., Liu, Q., Liu, X., Qi, L.: Application of bluetooth low energy beacons and fog computing for smarter environments in emerging economies. In: Zhang, X., Liu, G., Qiu, M., Xiang, W., Huang, T. (eds) Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications: International Conference on Cloud Computing, pp. 101–110. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-48513-9_8
14. LINE developers. https://developers.line.biz/en/docs/messaging-api/beacon-device-spec/. Accessed 19 July 2022