sensors

MDPI

Article

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

Chi-Jan Huang [1], Cheng-Jan Chi [2] and Wei-Tzu Hung [3,*]

[1] General Education Center, Ming Chuan University, Taipei 111013, Taiwan
[2] R&D Department, THLight Company, Ltd., New Taipei 241407, Taiwan
[3] Department of Civil Engineering, National Taipei University of Technology, Taipei 106344, Taiwan
* Correspondence: jones155376jones@gmail.com

Abstract: iBeacon systems have been increasingly established in public areas to assist users in terms of indoor location navigation and positioning. People receive the services through the Bluetooth Low Energy (BLE) installed on their mobile phones. However, the positioning and navigation functions of an 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 took the iBeacon system of Taipei Main Station, the major transportation hub with daily traffic of at least three hundred thousand passengers, as an example for exploring its potential attacks and further studying the defense technologies, with the assistance of AI techniques and human participation. Our experiments demonstrate that in the early stage of iBeacon system information security planning, information security technology and a rolling coding encryption should be included, representing the best defense methods at present. In addition, we believe that the adoption of rolling coding is the most cost-effective defense. However, if the security of critical infrastructure is involved, the most secure defense method should be adopted, namely a predictable and encrypted rolling coding method.

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

check for updates

Citation: Huang, C.-J.; Chi, C.-J.; Hung, W.-T. Hybrid-AI-Based iBeacon Indoor Positioning Cybersecurity: Attacks and Defenses. *Sensors* **2023**, *23*, 2159. https://doi.org/10.3390/s23042159

Academic Editor: Chris Rizos

Received: 26 December 2022
Revised: 15 January 2023
Accepted: 13 February 2023
Published: 14 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

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 utilizes signal strength to estimate the distance between the Beacon itself and the target mobile phone when locating the user's position, thus becoming an effective solution for indoor positioning. It solves the problem that the global positioning system (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 new-generation solutions [1] as they meet the accuracy requirements of indoor positioning at a lower power consumption compared to outdoor positioning systems.

According to the latest research report by Verified Market Research [2], the global market size of Bluetooth Low Energy (BLE) Beacon and iBeacon in 2019 was up to USD 696 million, with an expected growth in significance to USD 109.532 billion by 2027, recording a compound annual growth rate (CAGR) of 87.74%.

To date, various technologies for indoor micro-positioning, including Bluetooth, infrared (IR), ultrasound, radio frequency identification (RFID), Wi-Fi, ZigBee, ultra-wideband (UWB), and others, have been released to commercial markets. Each of them has its own characteristics and features in indoor positioning. Unlike traditional outdoor applications that depend on the GPS, the global navigation satellite system (GNSS), Beidou, and other satellite systems for object positioning, indoor micro-positioning with greater accuracy may collect real-time information via a variety of communication facilities, including satellite systems, various radio frequency systems (cellular, Wi-Fi, Bluetooth), micro-electromechanical systems (MEMS), sensors (accelerometer, gyroscope, and compass), etc.

Gradually, applications of iBeacon and BLE Beacon have been increasingly popular on mobile devices, since a majority of these devices have built-in Bluetooth protocol.

On the product end, iBeacon and BLE Beacon have been integrated. For example, Beacon can be found in many camera lenses [3], LED lighting [4], PoS devices [5], and digital billboards [6]; meanwhile, the popularity of smartphones, network devices, and location-based applications [7], as well as the low accuracy of GPS systems in indoor environments, have contributed to the expansion of the global indoor positioning market. The potential applications include locating children [8], the elderly [9], or pets [10] who have been lost; shopping mall navigation [11]; entry, exit, and crowd flow management at large venues (e.g., supermarkets or department stores) [12]; and vehicle management and identification [13]. The higher expansion of iBeacon and BLE Beacon applications often leads to higher risks associated with these applications. At present, the security issues that face the use of Beacon include spoofing, piggybacking and privacy concerns, etc. [14]. Moreover, indoor positioning requests high positioning accuracy and signal availability and accessibility. Chan and Chung in [15] described different attacks against wireless Beacon systems and possible defense mechanisms.

As there is little iBeacon security research involving information security, this study focused on the information security features of iBeacon and introduced possible attacks by hackers and their defense approaches.

The iBeacon system deployed in this study is located in a large area—about 500,000 people pass through Taipei Main Station every day. Therefore, the management unit of Taipei Main Station uses the iBeacon system for business use and provides API to charge externally. iBeacon is public broadcast data, and hackers can easily use mobile phones to collect broadcast information and create fake iBeacon location information. Assuming that it takes 30 min to go around the Taipei Main Station with a mobile phone, it only takes 64 h to build a fake iBeacon system and provide the same service; consequently, the iBeacon built by the institute will be criticized by the public and reviewed by the government. Therefore, the focus of this study is how to design a system that would require a hacker to spend a lot of time and money to crack.

The rest of this paper is organized as follows. Section 2 introduces the background and related work of this study. Section 3 describes the design of the iBeacon system at Taipei Main Station and possible attacks issued by hackers, with defense methods against these attacks. Section 4 concludes this paper and addresses our future studies.

1.1. iBeacon-Related Mechanisms

This section introduces iBeacon, the Eddystone protocol, LINE Beacon, and the advanced encryption standard (AES), which are described one by one in the following subsections.

1.1.1. iBeacon

Proposed by Apple, iBeacon is a small transmitter with features of low cost, low power consumption, long component lifetime, and easy deployment. It is applicable to indoor positioning systems. The iBeacon technology enables smartphones or other BLE devices to receive signals/messages from iBeacon systems and execute the corresponding commands. It has features of easy mounting and hardware-free configuration before a mobile phone can join the system and receive the required services.

Basically, any micro-positioning signal/message transmitter using BLE can be identified as a Beacon, and the difference between a Beacon and an iBeacon is the signal frequency they employ [16].

1.1.2. Eddystone Protocol

Eddystone, an open-source system launched by Google, is a communication protocol similar to the Beacon protocol. It also adopts a cross-platform BLE signal format. Eddystone was developed for both iOS and Android operating systems, thus allowing all Bluetooth devices to join this system. Its fields of a data frame for data transmission include a

unique identifier (UID), uniform resource locator (URL), telemetry (TLM), and ephemeral identifiers (EID) [14]. All Bluetooth devices can easily follow these fields to communicate with each other.

1.1.3. LINE Beacon

LINE is an instant messaging software. In 2017, its developer launched a Bluetooth transmitter called LINE Beacon, which allows LINE Bot, the chat robot service powered by LINE, to receive information from those nearby devices. Mobile phones with a distance of less than 50 m from a LINE Beacon can receive signals from this LINE Beacon [17].

1.1.4. Advanced Encryption Standard (AES)

In 2001, the National Institute of Standards and Technology formulated AES, the most widely used symmetric key today. Its encryption process is composed of four steps, i.e., SubBytes, ShiftRows, MixColumns, and AddRoundKey [18]. The key lengths of AES can be 128, 192, or 256 bits, depending on the required security level. A key length of 128 bits would require 10 rounds of repeated executions, while that of 192 bits needs 12 rounds, and that of 256 bits would request 14 rounds.

1.2. Related Work

1.2.1. Recent Applications of RFID

For enhancing the food management level in India, Biswal et al. [19] presented an RFID-based model to comprehend the key factors affecting the humanitarian supply chain in the warehouse operation of the Indian food storage system. The purpose was to improve warehouse management and inventory efficiency. Jha et al. [20] applied technologies such as RFID and biometric scanning to improve India's necessities distribution system, addressing the fragility and management flaws of this system and ensuring that necessities could actually be delivered to poor families. Kant et al. [21] took Indian cheese as the research object and proposed a low-cost, non-destructive, and RFID-based method to detect food spoilage.

Focusing on animal safety and conservation in France, Testud et al. [22] designed an automatic device with a detector using RFID to track and record the individual traces of critters in wildlife tunnels to provide valuable suggestions regarding how to maintain these tunnels. To safely protect young salmon passing through the fish-only channel downstream of a river containing a hydroelectric power plant, Tomanova et al. [23] used RFID antennas to detect the behaviors and survival rates of migratory salmon passing via the channel. They confirmed that the two protection systems were significantly effective for young salmon. Bouletreau et al. [24] installed RFID antennas on the turbines of hydropower stations to track and study the predator Silurus glanis and its threat to the endangered species Petromyzon marinus. The results concluded that in the overlapping living environment of the two species, Silurus glanis showed a high rate of predation, potentially endangering the lives of Petromyzon marinus.

Mohammedi et al. [25] proposed a biometrics-based mobile lightweight patient authentication scheme, which was developed by integrating it with information security. Mikhailovskaya et al. [26] introduced the idea of ensuring the stability of information security systems using RFID technology to counter possible attacks through remote scatterers mitigation. To improve the stability of information security in an IoT medical network, Shariq et al. [27] presented an RFID authentication protocol using an encryption system to defend against hacker attacks and avoid personal information leakage.

1.2.2. Safety Promotion of iBeacon

Bai et al. [28] proposed an iBeacon base station containing a Bluetooth 4.0 module and an emergency evacuation system to accurately locate users whose mobile phones were connected to this base station for receiving Bluetooth services, thus enabling them to be guided for evacuation from their current location in case of a disaster. Chen and Liu [29]

designed a system to guide the evacuation of people indoors, 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 was released to the market [30]. It can calculate the shortest path from the emergency exits to reduce the time for personnel evacuation so as to safely navigate the user groups outside.

Chen et al. [8] proposed a mobile system using IoT devices with components including iBeacon nodes and GPS to locate lost children. From the perspective of prevention, Liu et al. [31] designed a zipper specialized for iBeacon fixation on T-shirts to prevent children from going missing. Lu et al. [32] created a system that guides blind individuals with regard to their spatial location to enhance their safety in the environment they are situated in, and help them have a better quality of life.

1.2.3. Information Security Challenges of iBeacon

Previous studies have examined the integrity and importance of IoT security from different perspectives, including the classification of attacks [33], the timeliness of encryption, algorithm deployment [34], mobile crowdsourcing [35], cloud computing, etc. [36]. Such research on security has also extended their functions by using BLE [37,38]. 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 [39]. However, compared with other BLE technologies, Beacon can be widely applied to various areas/domains due to its low cost and accurate object location identification. Campos-Cruz et al. [40] analyzed the 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. [41] revealed the feasibility of attacking iBeacon services via Wi-Fi devices.

2. Materials and Methods

Taipei City is the largest political and economic center in Taiwan, and Taipei Main Station, as the transportation hub for foreign travelers entering and leaving Taipei City, is a big rail transportation field including six lines under four different administrations, namely Taiwan Railways Administration (TRA), Taiwan High-Speed Rail (THSR), Airport MRT (mass rapid transit), and three lines of the Taipei Metro, or Taipei MRT. The environments surrounding this field include four underground malls and one highway bus terminal. In 2019, the daily passenger traffic of Taipei Main Station consisted of 86,000 people via high-speed rail, 122,000 via Taiwan Railway, and 319,000 via MRT; the number of passengers taking MRT from various stations was considerably reduced in 2021 due to the impact of COVID-19, yet the passenger traffic at Taipei Main Station remained the highest among all stations at 177,000 passengers [42], totaling 305,000 passengers combined with the daily passengers taking the THSR and TRA. This study therefore adopted Taipei Main Station as the subject in exploring iBeacon security issues.

Due to the complex building structure and the shops and underground malls occupying significant areas of this building, the design of pedestrian passing routes and signs at Taipei Main Station have increased day by day. In order to protect the safety of the public and keep visitors from getting lost, the Taipei City Government launched the app "Taipei Navi" in 2018, which connects to more than 4000 iBeacons deployed across the station to solve issues such as passenger positioning, wayfinding, and commuting. Figure 1 shows the distribution of iBeacons in this station, where 317 and 108 iBeacons are installed on the 1st and 2nd floors, respectively, while 535 iBeacons are set up in the basement.

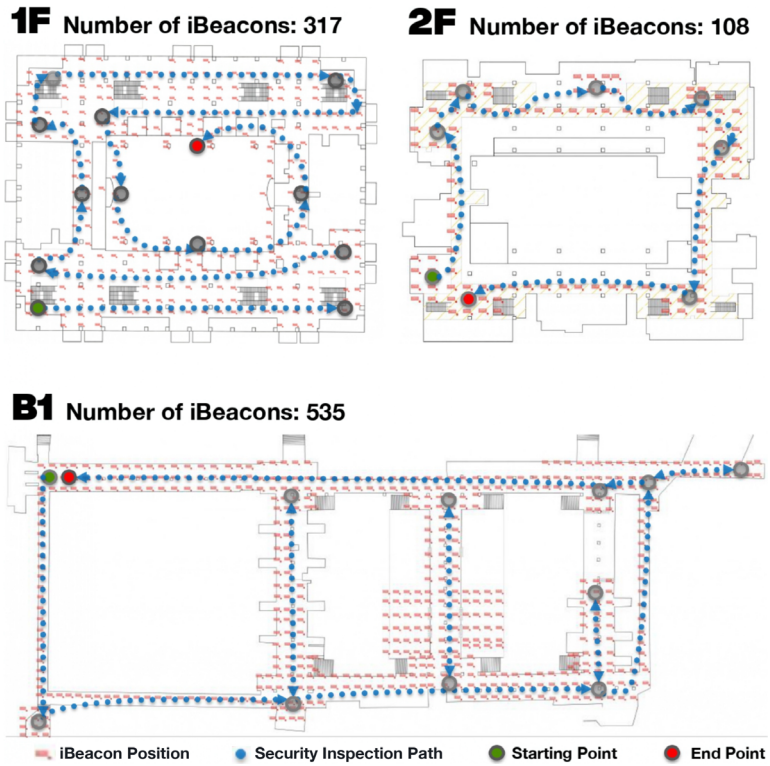


Figure 1. iBeacon locations and regular query route planning at Taipei Main Station.

2.1. iBeacon System Design Architecture

The design architecture of the iBeacon system in this study is shown in Figure 2, the number in brackets is the transmission time sequence. First, the Beacon plaintexts (e.g., a restaurant promotion advertisement) are encrypted by invoking the AES algorithm, and then transmitted to mobile phones via the BLE protocol through broadcasting, before the encrypted plaintext is transmitted to the server of the iBeacon system for decryption. After that, mobile phone users may receive the content of plaintext from the server and decide whether to dine at the restaurant or not. Users wishing to have their needs met by one of the promoted restaurants may be guided to this restaurant using the indoor navigation function of the Taipei Navi app.

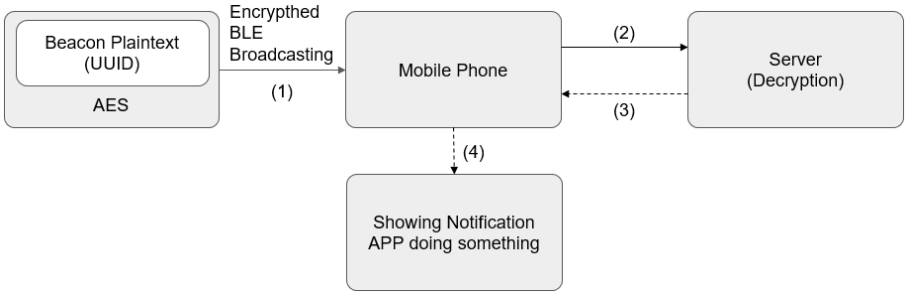


Figure 2. System diagram of the iBeacon system in this study.

2.2. Positioning Algorithms

The following is our method of positioning mobile phones. The positioning calculation was divided into three stages: initial, estimate, and regression.

2.2.1. Initial Stage

Stage 1, the initial stage, refers to determining the initial point of a mobile phone. The strengths of radio waves received from the mobile phone at the initial point by Beacons

1, 2, and 3 are shown in Figure 3, where W_a = 10^(RSSI_1), W_b = 10^(RSSI_2), and W_c = 10^(RSSI_3) are the signal strengths that Beacons 1, 2, and 3 receive from the mobile phone, respectively. Each Beacon computes its distance to the mobile phone according to the strength of the radio wave; 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:

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

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

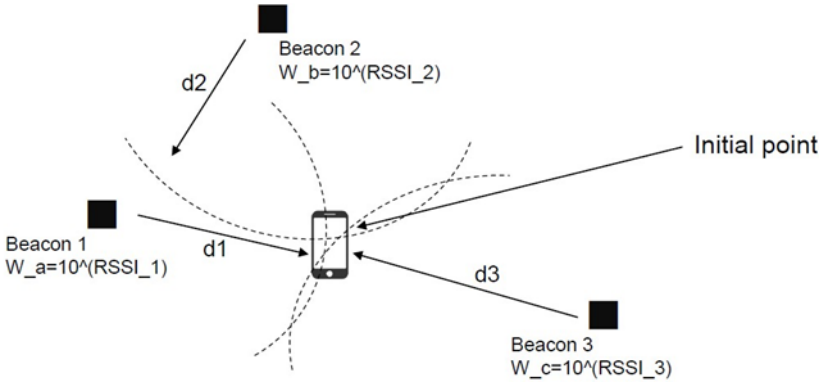


Figure 3. Method of initial point computation.

2.2.2. Estimate Stage

Following the completion of the initial point positioning, it was discovered that instant computation of the current location of users was difficult since the Beacon positioning system may only compute the relative position between each Beacon and the mobile phone, while the radio waves required an average based on stable readings. For a better user experience, this system refers to the method of Kok et al. [43] in Stage 2 by acceleration computations run by accelerators. The accelerator, illustrated in Figure 4, was a wireless three-axis accelerator. Currently, hardware devices with built-in acceleration computation only provide acceleration information. In this study, an algorithm was applied to integrate the acceleration from the user's phone position into a velocity that would receive a second integration to transform the velocity to a displacement, so that a position with the movement direction could be determined according to the gyroscope angle. In addition, Chang et al. [44] pointed out the five main services of the Taipei Main Station intelligent system, which includes the pedestrian indicator guide, i.e., the application of the "Taipei Navi" app, as shown in Figure 5.

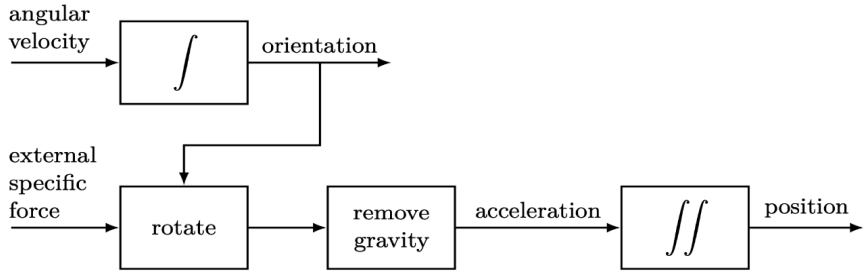
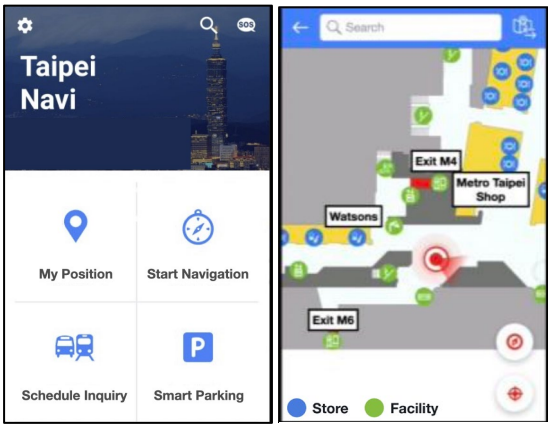


Figure 4. Schematic illustration of dead reckoning, where the accelerometer measurements (external specific force) and the gyroscope measurements (angular velocity) are integrated into the position and orientation of a mobile phone [44].



(**a**) (**b**)

Figure 5. (**a**) Taipei Navi app home screen; (**b**) Taipei Navi app navigation screen.

2.2.3. Regression Stage

Stage 3 concerns data regression. The results gained from Stage 2, the "estimate" stage, estimated a user's position once every 30 s. The results were compared with the initial points identified in Stage 1. In addition, the Beacon value prevailed when the error exceeded 15 m, since the errors of the accelerometer were accumulated. For specific Beacons, such as the ones near an escalator, regression was executed immediately upon a numerical strength excess over 70 dB, since the user would soon move to another floor when riding the escalator and they would be in close proximity to Beacons as they came near to the floor. At such a moment, the Beacon radio wave strength would become extremely high, and a rapid regression, also known as quick regression, was required.

2.3. Hybrid-AI-Based Positioning Algorithm

In a real field, mobile phones continuously receive values from more than one Beacon. These messages are still unavailable as the strength of signal reception fluctuates due to unstable radio waves, thereby affecting the results obtained via the mathematical positioning algorithm. To solve this problem, this system applied a hybrid-AI-based scheme to our positioning algorithm.

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

Figure 6, representing the results of Stage 2, is an example of a four-by-four grid graph. In actual operation, it is a graph composed of 80 × 80 grids, i.e., each positioning position is an 80 × 80 grid. There are 6500 groups of 80 × 80 squares in the railway station. In this study, strength values were stored per second, and the average strengths every seven seconds as one cycle were mapped into this graph, which was immediately submitted to TensorFlow [45]; CNN in TensorFlow was then applied for point identification.

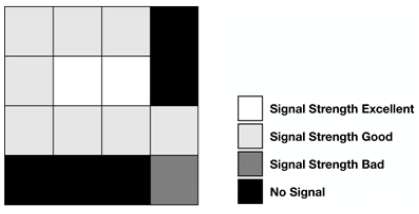


Figure 6. Graph of radio wave strengths received by mobile phones (strengths are indicated in descending order, i.e., white, light gray, dark gray, and black).

In Stage 3, the hybrid-AI-based positioning algorithm transformed the position of a user's mobile phone to a radio wave strength graph. The positions of the Beacons with the strongest wave signal were identified as the user's current position.

3. Results

3.1. Possible Attacks

In the following section, we describe possible attacks on Beacon systems.

3.1.1. Recording and Use

Figure 7 describes how the code (ID) of the normally working iBeacon system is illegally recorded and stored by hackers. Figure 8 illustrates how a hacker disguises a Beacon to deliver fake messages or broadcast its own services to users. Owing to high hardware deployment and maintenance costs of the Beacon system, the operator will expect the system costs to be partially shared by mobile phone users. At the very least, unauthorized use should be prohibited. However, from a technical viewpoint:

1. Any mobile phone which has a BLE protocol can receive and decode the message from the iBeacon system, meaning any mobile application that can obtain the Beacon broadcasts is able to position the mobile phone. Therefore, hackers may use such a 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 obtaining any permission beforehand.
2. By writing this information into the APP, identification may be mounted to nearby devices without the owner's agreement. This may leak the user's location information to the public, making the entire system a target vulnerable to hacker attacks.
3. Company A, investing a huge amount of capital in the deployment of 1000 Beacons at an airport, would like to recover its investment from the location-based service (LBS) provided. However, it is unable to achieve this once the system is utilized by Company A's competitor. In fact, Company A's competitor may assign one person to walk into the field holding a smartphone. Then, this person can gain access to this system without prior notice to Company A or without receiving usage agreement from Company A.

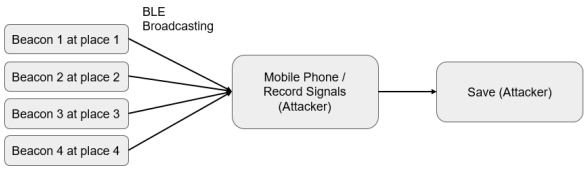


Figure 7. Normal iBeacon codes recorded and stored by hackers.

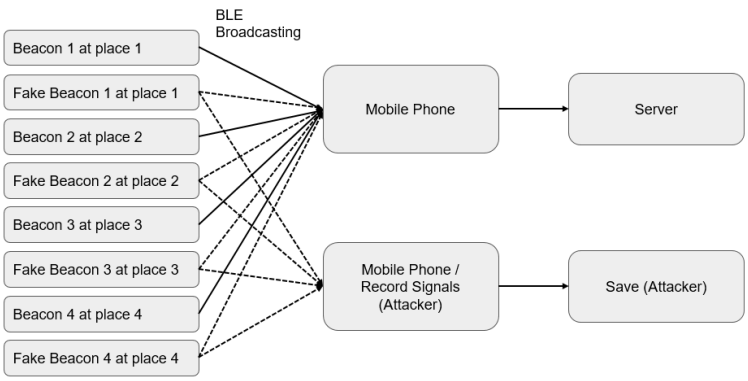


Figure 8. iBeacon hacker sends other users' messages or broadcasting his/her own services via a mobile phone to disguise as a Beacon.

3.1.2. Impersonation Attack

As is shown in Figure 9, a Beacon broadcasts messages to the public, and in most cases, these messages are usually not encrypted; therefore, an attacker can detect and replicate the Beacon codes. An attacker can first hack a Beacon and then attack the users connected to this Beacon. He/she may even replicate a faked Beacon in another field using the same ID, when possible. For example, Attacker B sends false messages to users through a faked Beacon. Another example is that Company B uses a Beacon as an attendance assessment device, which would allow a malicious employee to duplicate this Beacon and fake his/her attendance by tricking the Beacon through clock-ins and -outs at abnormal hours, thereby making himself/herself always present at work.

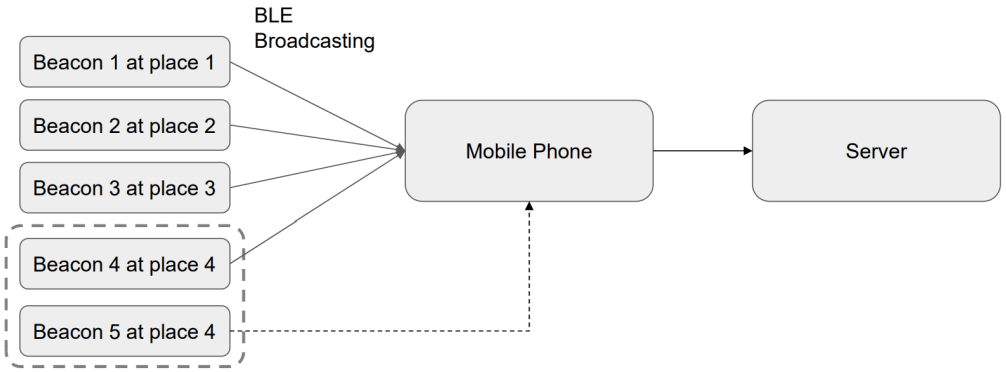


Figure 9. The presentation attack (faked Beacon 5 placed in the place of Beacon 4, leading to delivery of incorrect LBS information).

If there is an LBS service, only one faked Beacon needs to be prepared. As is shown in Figure 9, fake Beacons 5 and 4 placed in the same location could cause the app to distribute wrong information in the wrong place. For example, Beacon 5 should send data of place 5; however, a mobile phone will receive the data messages issued by Beacons 4 and 5 at the same time, as Beacon 5 has been wrongly placed in place 4. According to our own experience, one Beacon with maximum power can serve 50,000 passengers at Taipei Main Station in a day. The spread of such misinformation may lead to terrible situations. People receiving place 5 from iBeacon 5 may consider that this place is place 5, instead of place 4. Another example is that iBeacon distributes a message telling passengers that there is currently a disaster nearby, and everyone has to leave immediately, i.e., distributing fake news.

3.1.3. Obfuscation Attack

An obfuscation attack is one of the easiest attacks at the physical level. Hackers put multiple Beacons in the same location. Since applications mostly rely on the Beacon to determine their position and implement behaviors, hackers may use multiple faked Beacons and Beacons under the original system can be placed in the same position, e.g., Beacons 4, 5, and 6 can be placed in the position where Beacon 3 is deployed. As is shown in Figure 10, this may cause serious interference or delay in the transmission of data by Beacon 3 [41]. This, in turn, affects the integrity and correctness of the data, resulting in messages conveying correct information being lost or faked or Beacons triggering wrong behaviors. An impersonation attack does not interfere with the operation of the original system, while an obfuscation attack is a malicious attack with the potential to paralyze the original system.

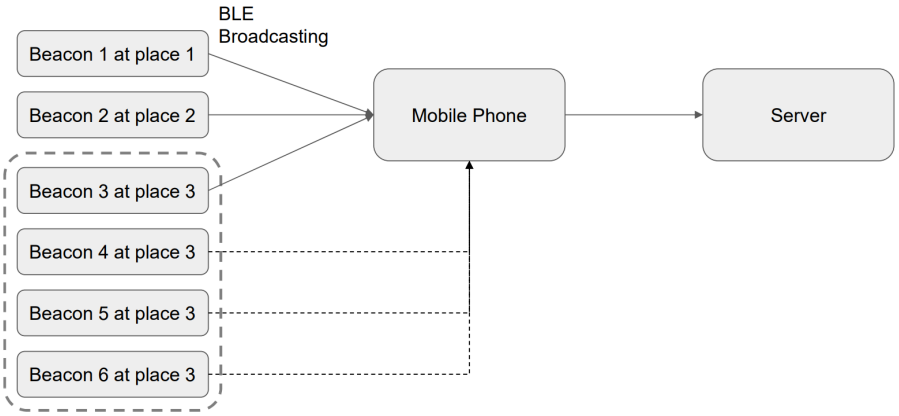


Figure 10. Obfuscation attack (faked Beacons 4, 5, and 6 and Beacon 3 under the original system are all placed at location place 3, sending obfuscation information to users).

3.1.4. 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. As is shown in Figure 11, when a Beacon has 999 codes, hackers can, at most, record a set of 40 codes, due to time restraints. However, in the case of limited recording, the codes will ultimately be repeated. This type of attack against the Beacon will be found eventually.

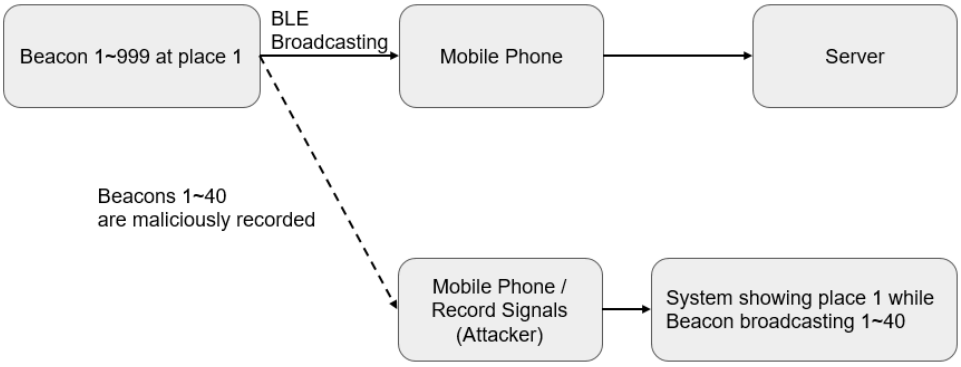


Figure 11. Recording and limited reproduction.

3.2. Beacon System Defense Methods

This study proposes five methods to defend against the attacks mentioned above.

3.2.1. Data Encryption/Decryption

This method involves simple steps of encrypting Beacon messages and then decrypting them by the receiver; however, such a method is meaningless in the security of the system, since all of the abovementioned attacks may still work as long as the issued messages remain unchanged. The reason for this is that the encryption keys used at different time points would be the same, i.e., the generated ciphertext C would always be the same. Hackers do not need to decrypt C. They can realize that the messages are issued by a specific iBeacon.

For example:

Given that fa is the message sent via the Beacon at location A, the ciphertext sent is converted to AES Code AES(fa). (3)

The app receives AES(fa) for further decoding to fa (which is the code indicating location A). (4)

$$\text{fb} \rightarrow \text{AES(fb)}, \text{i.e., the app receives AES(fb) and decodes fb (which is the code indicating location B).} \quad (5)$$

The location code of the Beacon at location A, i.e., fa and its ciphertext AES(fa), form a one-to-one relationship. Even hackers cannot solve fa from AES(fa), as the Beacon at location A transmits the same AES(fa) code for fa at all times, hackers can ensure that the current position is place A. Hence, the same AES(fa) continuously sent from the Beacon at point A will ultimately be recognized as place A, meaning that AES encryption will not be defensive.

As is shown in Figure 12, we used the following methods to evaluate the time cost of cracking:

a. Impersonation: Assuming that the user only wants to create the illusion of "I am somewhere" (such as for roll call at work, or for the application location service, which is used at Taipei Main Station), a hacker only needs to copy one iBeacon to confuse the system. Assuming that there is no protection, the hacker only takes 1.5 min to copy the position of one iBeacon and carry out an impersonation attack.
b. Obfuscation: If a hacker wants to interfere with the data, he/she needs to make 5%, that is, 535 × 5% = 27 fake iBeacon positions, which can interfere with the system operation at a large scale. Assuming that there is no protection, the hacker takes 40.5 min to carry out an obfuscation attack.
c. Recording and use: The hacker must record all iBeacon–location relationships before establishing a new system. Assuming that there is no protection, the hacker takes 802.5 min (30 min for one iBeacon) to create a new fake iBeacon system.

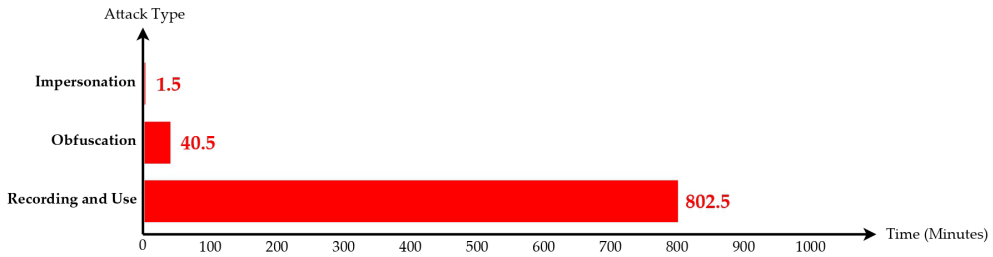


Figure 12. No defense attacks (since AES encryption only has the effect of confusion, it takes only 802.5 min to complete the signal replication and only 40.5 min to start the obfuscation attack; thus, the time required is low).

3.2.2. Rolling Coding

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

The classic descriptive equation of rolling coding is

$$f(t) = f(t + 1) \quad (6)$$

1. Unpredictable Rolling Coding

In the unpredictable model,

$$f\,(t + 1) = g\,(t, \text{random}) \quad (7)$$

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

$$f\,(t + 1) = g\,(\text{code}, \text{random}) \quad (8)$$

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

$$f(t+1) = AES(code, random) \quad (9)$$

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

For example, f (t + 1) = AES (code, random) = YCL2KXHTLDN2XHPA (000, 369)

The decoder may only obtain the code and random variable after decoding AES (code, random). We would like to know the following:

- Whether the code is shown at a preset reasonable number of digits, e.g., between 1 and 100, which means that the code between 1 and 100 is normal. If the Beacon code exceeds 100, it means that the system has been illegally recorded and is subjected to an impersonation attack or obfuscation attack.
- Random variable being a random value

  Assuming that the hacker has copied three random codes of Beacon location A, if the server S has been hacked and duplicate random in AES (code, random) are found (for example, if the Beacon has 4 codes, all of which are 100), the fake Beacon from the hacker will be found; then, all AES (code, random) is subject to comparison, plus the time stamp T when they are launched, i.e., AES (code, random)||T, denoted by R, is sent to a mobile phone. On receiving R, this mobile phone sends R to server S to verify whether $T - T' \leq \Delta T$, where T' is the time stamp when S receives R, and ΔT is the longest time for a message to travel from a Beacon to S. The purpose is to confirm whether a replay attack has been triggered.

Hackers or attackers may utilize a recording and use attack, impersonation attack, obfuscation attack, and recording and limited reproduction attack to destroy not only the correctness of LBS broadcasts, but also the relationship between "encrypted messages broadcast" and "the corresponding location". The detection methods of this type of attack are as follows:

(1) Recording and use attack: Following the decoding of false messages which are recorded, it can be discovered that its random value is same as the random value in the original message. For example, hackers record all iBeacon system codes and store them for eventual transmission of false information or to broadcast his/her own advertisement using this iBeacon system. The random values of several messages will be the same, and this type of attack may therefore be detected.

(2) Impersonation attack: If an iBeacon issues two messages in which the iBeacon codes are the same, e.g., both are 56, the ciphertexts generated will be different since the random values of the two messages vary. If a recorded ciphertext is broadcast N times, $N \geqq 2$, it remains unchanged. For example, user C passes by a location and user D, who passes by the same location after 10 min, receives the identical ciphertext AES (code, random) sent by the same iBeacon. This means that what C or D receives is the ciphertext recorded and sent by a hacker. It can therefore be detected that this iBeacon has been subjected to an impersonation attack by a hacker.

(3) Obfuscation attack: As per that described for the impersonation attack, N AES (code, random) that S received via the same or different mobile phones are identical, $N \geqq 2$, indicating that the random values of multiple false Beacons are the same as under an impersonation attack. For example, if N iBeacon-code AES (code, random) received by user E passing by a location is identical to that received by user F, who passed by the same location 10 min later, it shows that this iBeacon has been subjected to an obfuscation attack. The contents of legal messages are constantly changing due to the change in the random variable. In fact, the impersonation and obfuscation attacks mentioned above only record "the same group of messages" or "N groups of messages, where $N \geq 2$". Therefore, the server would detect that the Beacon is under the abovementioned attack and disable this iBeacon's false message broadcast.

(4) Recording and limited reproduction: Assuming that the user, without knowing the coding mechanism, directly recorded m groups of messages, m < n, where n is the number of iBeacons, if the unpredictable and encrypted rolling coding method was adopted, the data received by the server S of this system could not be applied to identify whether the message was false or legal. However, as the server may detect duplicate random values from the decoded message, S will discover that the Beacon has been subjected to an impersonation or obfuscation attack.

As is shown in Figure 13, in the method of rolling coding, if only one set of data needs to be copied, the effect of copying will be invalid after 15 s. Since the time required to copy an iBeacon is six times the code hopping period of an iBeacon, the cost of cracking is not proportional to the benefit, so the copying will not actually be performed. Of course, a hacker can exhaustively collect the data of each iBeacon, and the time cost is explained as follows:

a. Impersonation: Hacker takes 1500 min to copy the location of one iBeacon and carry out an impersonation attack.
b. Obfuscation: Hacker takes 40,500 min to crack 27 iBeacons and interfere with the iBeacon system.
c. Recording and Use: Hacker takes 802,500 min (30 min for one iBeacon) to crack 535 iBeacons to create a new fake iBeacon system.

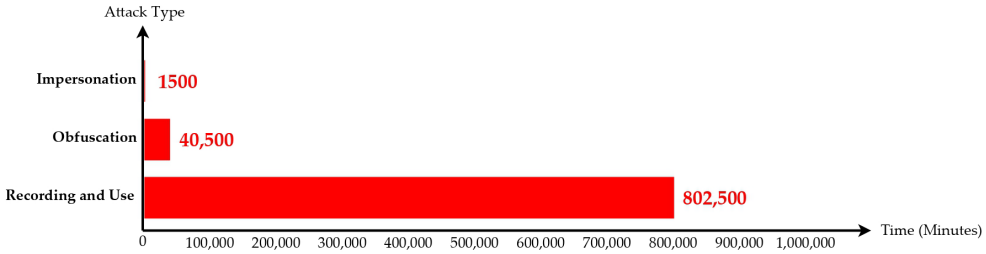


Figure 13. Since recording and use takes 802,500 min to complete signal replication and obfuscation attack takes 40,500 min, the time required is high.

2. Predictable and Encrypted Rolling Coding Method

In the predictable model, f(t + 1) in Equation (6) is the code existing in regularity. Generally, the change happens 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 a 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 variable can be omitted. For example, Eddystone uses PDU count/time as an index [46] 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 [47].

The advantage of using the predictable and encrypted 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 [37]. The system owner must carefully consider the flash's lifetime 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 an impersonation attack or obfuscation attack, the server must detect whether the constraint $T' - T \leq \Delta T$ has been met or not. If not, the system administrator shall be warned for further processing. Basically, personnel inspections and active monitoring via an app are probable solutions.

The cracking cost of the predictable and encrypted rolling coding method is the same as rolling coding, and the time cost is explained as follows:

a. Impersonation: Hacker takes 1500 min to copy the location of one iBeacon and carry out an impersonation attack.
b. Obfuscation: Hacker takes 40,500 min to crack 27 iBeacons and interfere with the iBeacon system.
c. Recording and use: Hacker takes 802,500 min (30 min for one iBeacon) to crack 535 iBeacons to create a new fake iBeacon system.

Different from rolling coding, at the moment of impersonation attack, if there is a properly designed code, we can immediately analyze whether the iBeacon is under an impersonation attack.

3. Personnel Inspection

Installing an iBeacon sensor as a part of security personnel's devices may facilitate the inspection of intrusions or attack behaviors by suspecting individuals patrolling Taipei Main Station and the surroundings. The inspection involves checking whether the time constraint $T' - T \leq \Delta T$ has been met or not by the server. If not, it means that the Beacon is under impersonation or obfuscation attacks, and the administrative personnel must take charge of excluding the information broadcast from these malicious Beacons.

4. App Active Monitoring

The app Taipei Navi has accumulated more than 100,000 downloads since its release in 2018. The messages received by users using the app from iBeacon are aggregated into the server at the back end of iBeacon. By comparing timestamps, it is possible to see whether an iBeacon is under a replay attack and whether the location of the attacked iBeacon can be identified.

The following experiment assumes that all Beacons can send 1000 signals. The assumptions are as follows:

True positives (TP): How many times attacks are detected as attacks.
True negatives (TN): How many times normal behaviors are detected as such.
False negatives (FN): How many times attacks are detected as normal behaviors.
False positives (FP): How many times normal behaviors are detected as attacks.

(1) Recording and Use Experiment

We referred to the frameworks shown in Figures 7 and 8 to conduct our recording and use experiment, assuming that the user is using unencrypted Beacon signals, and that the pirated signals are not passing through the user's node at all. The experimental results are given in Figure 14.

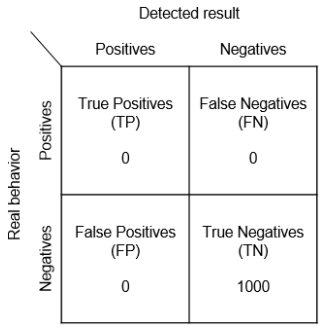


Figure 14. Recording and use confusion matrix.

As there was no rolling coding, the server could not detect the problem at all and treated it as a normal signal.

(2) Impersonation Attack Experiment

The framework shown in Figure 9 is the one we adopted to perform our impersonate attack experiment. Impersonation attack can be detected during inspection. Therefore, the Beacon 5 signal is aborted (however, this also disables the normal Beacon 4). Figure 15 shows the confusion matrix.

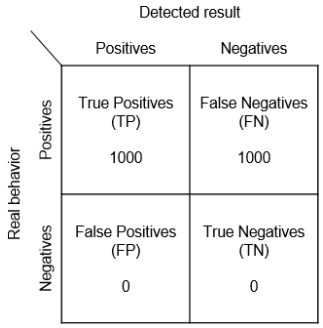


Figure 15. Impersonation attack confusion matrix.

Both real and fake signals have been received; there are 1000 normal signals and 1000 fake signals. Without rolling encryption, the 2000 signals have the same password and are treated as attacks at the same time.

(3) Obfuscation Attack Experiment

Figure 10 shows the framework we employed to carry out our obfuscation attack experiment, where Beacon 3 is disabled (however, this will also disable Beacon 6, which is normal). The confusion matrix is given in Figure 16.

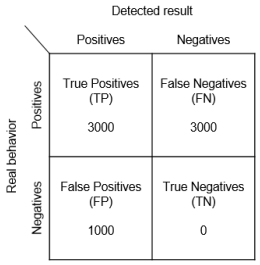


Figure 16. Obfuscation attack confusion matrix.

Beacons 4, 5, and 6 sending 3000 signals were treated as attacks, while Beacons 4, 5, and 6 with 3000 signals were treated as errors when the original position should have been correct.

(4) Recording and Limited Reproduction Experiment

Figure 11 illustrates the framework we utilized to perform our recording and limited reproduction experiment. Repeated signals were discarded. The confusion matrix is given in Figure 17.

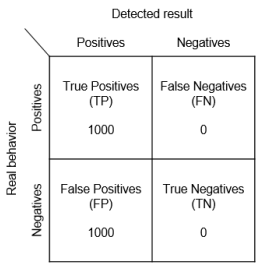


Figure 17. Recording and limited reproduction confusion matrix.

Due to the rolling encryption, the server will receive real and false signals that can be disabled immediately.

5. iBeacon Attack and Defense Comparison Experiment

Table 1 shows the cracking time of the iBeacon attack and defense comparison experiment. The total number of iBeacons in Taipei Station in this study is 535. Assuming that the three attack types are not discovered by any defense, rolling coding, or predictable and encrypted rolling coding method, the times required to crack the different defense methods are different. For example, impersonation takes 1.5 min to crack without any defense. Under the condition that the defense system is not activated, rolling coding and the predictable and encrypted rolling coding method take the same time to crack the attack. However, after the defense system is activated, rolling coding will discover the attack once it suffers an impersonation attack, while the predictable and encrypted rolling coding method can detect the attack immediately without facing an impersonation attack.

Table 1. iBeacon attack and defense comparison.

Attack Type/Defense Method	No Defense	Rolling Coding	Predictable and Encrypted Rolling Coding Method
Impersonation (1 iBeacon)	1.5 min	1500 min	1500 min
Obfuscation (27 iBeacons)	40.5 min	40,500 min	40,500 min
Recording and Use (535 iBeacons)	802.5 min	802,500 min	802,500 min

4. Conclusions and Future Studies

The iBeacon system has been widely used to date and it is available for any mobile device that supports BLE; nevertheless, the question of how to protect its security remains. This study explored the possible attacks on iBeacon launched by hackers and proposed defense strategies. This study did not explore how hackers attack via the MAC address owing to the fact that almost 95% of BLE applications in Taiwan are based on iBeacon and iOS cannot obtain the BLE broadcasting MAC address, making it difficult for hacker attacks to reach their economic scales; in addition, versions after BLE 5 contain various security methods against MAC address attacks [48].

Our experiments demonstrated that, during the early stage of iBeacon system information security planning, information security technology and rolling coding encryption should be included, which represent the best defense methods at present. In addition, rolling coding will discover the attack once it suffers an impersonation attack, while the predictable and encrypted rolling coding method can detect the attack immediately without facing an impersonation attack. In terms of economic considerations, the design cost of rolling coding is low, while the design cost of the predictable and encrypted rolling coding method is relatively high. Therefore, based on the results of this study, we believe that the adoption of rolling coding is the most cost-effective defense. However, if the security of critical infrastructure is involved, such as the Taipei Main Station, the most secure defense method should be adopted, namely the predictable and encrypted rolling coding method.

In the future, we will further study the feasibility of other AI-based technological applications in terms of iBeacon information security. The effect of automatic comparison between the accelerometer and graphs of radio wave strengths received has been described in detail in this work. In the future, these technologies will be integrated into the server to establish an AI-based automatic management platform to be used to defend against hacker attacks.

Author Contributions: Conceptualization, C.-J.H. and C.-J.C.; methodology, C.-J.C.; software, C.-J.C.; validation, C.-J.H. and C.-J.C.; formal analysis, C.-J.H., C.-J.C. and W.-T.H.; resources, C.-J.C.; data curation, W.-T.H.; writing—original draft preparation, W.-T.H.; writing—review and editing, C.-J.H.; visualization, C.-J.H.; supervision, C.-J.H.; project administration, W.-T.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The supporting data of this study are available from the author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kao, C.L. The Application of Beacon Micro Positioning Technology. *Arch. Semiannu.* **2021**, *20*, 88–97.
2. Verified Market Research, Bluetooth Beacon and iBeacon Market Size, Opportunities & Forecast. Available online: https://www.verifiedmarketresearch.com/product/bluetooth-beacon-and-ibeacon-market/ (accessed on 16 July 2022).
3. Liaw, J.J.; Chen, K.L.; Huang, T.C.; Cheng, Y.H. The Simulation of the Indoor Positioning by Panoramic Camera and Point Cloud Scanner. In *Mobile and Wireless Technology*; Springer: Singapore, 2018; 513p. [CrossRef]
4. Qiu, C.; Hussain, B.; Yue, C.P. Bluetooth Based Wireless Control for iBeacon and VLC Enabled Lighting. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019; pp. 614–615. [CrossRef]
5. Senthazhai, M.S.; Keerthika, B.; Sathya, S. An Innovative Wearable Device for Women Safety Using IBEACON Technology with BLE. *Int. J. Res. Eng. Sci.* **2022**, *10*, 653–657.
6. Gan, C.C.; Lee, Y.J. enRoute: An Indoor Navigation Application Using Digital Signage. *Sens. Mater.* **2022**, *34*, 523–531. [CrossRef]
7. Liu, Q.; Yang, X.; Deng, L. An IBeacon-Based Location System for Smart Home Control. *Sensors* **2018**, *18*, 1897. [CrossRef] [PubMed]
8. Chen, L.W.; Chen, T.P.; Weng, C.C. iBaby: A Mobile Children Monitoring and Finding System with Stranger Holding Detection Based on IoT Technologies. In Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos, Beijing China, 19–23 August 2019; pp. 66–68. [CrossRef]
9. Chantaweesomboon, W. Bluetooth Geo-Fence for Elderly and Patient Care. In Proceedings of the 2021 25th International Computer Science and Engineering Conference (ICSEC), Chiang Rai, Thailand, 18–20 November 2021; pp. 252–255. [CrossRef]
10. Qu, M.; Sun, Y. An IoT-Based Crowd Sourcing System for Object Tracking and Information Sharing. *Int. J. Artif. Intell. Appl.* **2019**, *10*, 47–54. [CrossRef]
11. Meliones, A.; Sampson, D. Blind MuseumTourer: A System for Self-Guided Tours in Museums and Blind Indoor Navigation. *Technologies* **2018**, *6*, 4. [CrossRef]
12. Kwok, C.Y.T.; Wong, M.S.; Griffiths, S.; Wong, F.Y.Y.; Kam, R.; Chin, D.C.W.; Xiong, G.; Mok, E. Performance Evaluation of iBeacon Deployment for Location-Based Services in Physical Learning Spaces. *Appl. Sci.* **2020**, *10*, 7126. [CrossRef]
13. 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.* **2018**, *125*, 637–648. [CrossRef]
14. Spachos, P.; Plataniotis, K. Beacons and the City: Smart Internet of Things. In *Cooperative and Graph Signal Processing: Principles and Applications*, 1st ed.; Djurić, P.M., Richard, C., Eds.; Academic Press: Cambridge, MA, USA, 2018; pp. 757–776. [CrossRef]
15. Chan, A.C.-F.; Chung, R.M.H. Security and Privacy of Wireless Beacon Systems. Cornell University. *arXiv* **2021**, arXiv:2107.05868. [CrossRef]
16. Huang, K.H. Beacon Application for Museum Indoor Positioning System: A Case Study of National Museum of Taiwan History. *J. Mus. Cult.* **2018**, *15*, 5–29.
17. Yen, P.Y.; Fanjiang, Y.Y.; Hung, C.H.; Zhang, T.M. Design and Implement a Roll Call System with Body Temperature Measurement and the Instant Messaging Software. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 10–12 January 2021. [CrossRef]
18. Zhang, Y.; Wang, X. Pipelined implementation of AES encryption based on FPGA. In Proceedings of the 2010 IEEE International Conference on Information Theory and Information Security, Beijing, China, 17–19 December 2010; pp. 170–173. [CrossRef]
19. Biswal, A.K.; Jenamani, M.; Kumar, S.K. Warehouse efficiency improvement using RFID in a humanitarian supply chain: Implications for Indian food security system. *Transp. Res. Part E Logist. Transp. Rev.* **2018**, *109*, 205–224. [CrossRef]
20. Jha, R.K.; Srivastav, V.; Sumbli, V.; Trisha; Gandhi, V.; Jain, S. RFID based food rationing system. *HardwareX* **2018**, *4*, 1–13. [CrossRef]
21. Kant, R.; Samadder, S.; Srivastav, P.P.; Pathak, S.S.; Datta, A.K. Development and evaluation of low-cost frequency based sensor for non-destructive detection of Paneer spoilage. *J. Biochem. Technol.* **2018**, *9*, 10–15.

22. Testud, G.; Vergnes, A.; Cordier, P.; Labarraque, D.; Miaud, C. Automatic detection of small PIT-tagged animals using wildlife crossings. *Anim. Biotelemetry* **2019**, *7*, 21. [CrossRef]
23. Tomanova, S.; Courret, D.; Alric, A.; De Oliveira, E.; Lagarrigue, T.; Tetard, S. Protecting efficiently sea-migrating salmon smolts from entering hydropower plant turbines with inclined or oriented low bar spacing racks. *Ecol. Eng.* **2018**, *122*, 143–152. [CrossRef]
24. Bouletreau, S.; Carry, L.; Meyer, E.; Filloux, D.; Menchi, O.; Mataix, V.; Santoul, F. High predation of native sea lamprey during spawning migration. *Sci. Rep.* **2020**, *10*, 6122. [CrossRef] [PubMed]
25. Mohammedi, M.; Omar, M.; Bouabdallah, A. Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *9*, 1527–1539. [CrossRef]
26. Mikhailovskaya, A.; Shakirova, D.; Krasikov, S.; Yusupov, I.; Dobrykh, D.; Slobozhanyuk, A.; Bogdanov, A.; Filonov, D.; Ginzburg, P. Anapole-enabled RFID security against far-field attacks. *Nanophotonics* **2021**, *10*, 4409–4418. [CrossRef]
27. Shariq, M.; Singh, K.; Bajuri, M.Y.; Pantelous, A.A.; Ahmadian, A.; Salimi, M. A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario. *Sustain. Cities Soc.* **2021**, *75*, 103354. [CrossRef] [PubMed]
28. Bai, D.T.; Zhang, J.N.; Pan, Y. Research on the principle and technology of indoor positioning navigation escape rescue system. *Fire Sci. Technol.* **2018**, *37*, 1560–1563.
29. Chen, L.W.; Liu, J.X. EasyFind: A Mobile Crowdsourced Guiding System with Lost Item Finding Based on IoT Technologies. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 343–345. [CrossRef]
30. Chen, L.W.; Liu, J.X. Time-Efficient Indoor Navigation and Evacuation With Fastest Path Planning Based on Internet of Things Technologies. In *IEEE Transactions on Systems, Man, and Cybernetics: Systems*; IEEE: Piscataway, NJ, USA, 2019; Volume 51, pp. 3125–3135. [CrossRef]
31. Liu, Y.; Hong, W.; Peng, J.; Xue, Z. Design of childern's knitting security clothing based on micro-location of iBeacon technology. *Wool Text. J.* **2017**, *45*, 47–51. [CrossRef]
32. Lu, H.K.; Lin, P.C.; Chu, K.C.; Chen, A.N.; Yuan, A. Development and evaluation of a Beacon-based indoor positioning and navigating system for the visually impaired. *J. Intell. Fuzzy Syst.* **2019**, *37*, 4665–4675. [CrossRef]
33. Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O.B. Internet of Things (IoT): Taxonomy of Security Attacks. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 321–326. [CrossRef]
34. Maitra, S.; Yelamarthi, K. Rapidly Deployable IoT Architecture with Data Security: Implementation and Experimental Evaluation. *Sensors* **2019**, *19*, 2484. [CrossRef] [PubMed]
35. Ang, K.L.M.; Jasmine Kah, P.S.; Ngharamike, E. Towards Crowdsourcing Internet of Things (Crowd-IoT): Architectures, Security and Applications. *Future Internet* **2022**, *14*, 49. [CrossRef]
36. Mukherjee, B.; Neupane, R.L.; Calyam, P. End-to-end IoT security middleware for cloud-fog communication. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 151–156. [CrossRef]
37. Tay, H.J.; Tan, J.; Narasimhan, P. *A Survey of Security Vulnerabilities in Bluetooth Low Energy Beacons*; Tech. Report. CMU-PDL-16-109; Parallel Data Laboratory, Carnegie Mellon University: Pittsburgh, PA, USA, 2016.
38. Lacava, A.; Zottola, V.; Bonaldo, A.; Cuomo, F.; Basagni, S. Securing Bluetooth Low Energy networking: An overview of security procedures and threats. *Comput. Netw.* **2022**, *211*, 108953. [CrossRef]
39. Yang, Q.; Huang, L. Bluetooth Security. In *Inside Radio: An Attack and Defense Guide*, 1st ed.; Springer: Singapore, 2018; pp. 195–226. [CrossRef]
40. Campos-Cruz, K.J.; Mancillas-López, C.; Ovilla-Martinez, B. A Lightweight Security Protocol for Beacons BLE. In Proceedings of the 2021 18th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, Mexico, 10–12 November 2021; pp. 1–6. [CrossRef]
41. Na, X.; Guo, X.; He, Y.; Xi, R. Wi-attack: Cross-technology Impersonation Attack against iBeacon Services. In Proceedings of the 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Rome, Italy, 6–9 July 2021; pp. 1–9. [CrossRef]
42. Department of Budget, Accounting and Statistics, Taipei City Government. Available online: https://dbas.gov.taipei/News_Content.aspx?n=61D456768E73CD92&sms=72544237BBE4C5F6&s=45E047F8D9E61B46 (accessed on 7 July 2022).
43. Kok, M.; Hol, J.D.; Sch, T.B. Using Inertial Sensors for Position and Orientation Estimation. *Found. Trends Signal Process.* **2017**, *11*, 1–153. [CrossRef]
44. Chang, S.W.; Huang, H.H.; Su, P.C. Taipei Smart Station System Applications. *Urban Traffic Biannu.* **2018**, *33*, 27–35.
45. Hu, J.; Qian, S.; Fang, Q.; Wang, Y.; Zhao, Q.; Zhang, H.; Xu, C. Efficient Graph Deep Learning in TensorFlow with tf_geometric. In Proceedings of the 29th ACM International Conference on Multimedia, New York, NY, USA, 20–24 October 2021; pp. 3775–3778. [CrossRef]
46. Sun, M.; Kamoto, K.M.; Liu, Q.; Liu, X.; Qi, L. Application of Bluetooth Low Energy Beacons and Fog Computing for Smarter Environments in Emerging Economies. In Proceedings of the Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications: International Conference on Cloud Computing, Beijing, China, 4–5 December 2019; pp. 101–110. [CrossRef]

47. LINE Developers. n.d., LINE Beacon Device Specification. Available online: https://developers.line.biz/en/docs/messaging-api/beacon-device-spec/ (accessed on 19 July 2022).
48. Anathi, M.; Vijayakumar, K. An intelligent approach for dynamic network traffic restriction using MAC address verification. *Comput. Commun.* **2020**, *154*, 559–564. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.