






Implementation and Analysis of Covert Channel Using iBeacon

Ye-Sol Oh¹^a, Yeon-Ji Lee¹^b, Jiwon Jang¹^c, Hyunwoo Choi²^d and Il-Gu Lee³^e

¹Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, 02844, Korea

²Korea Advanced Institute of Science and Technology, Daejeon, Korea

³Department of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Korea

Keywords: Covert Channel, BLE, iBeacon, iBeacon Payload, Advertising Interval.

Abstract: Covert channels are typically employed to transmit information and bypass security policies and controls simultaneously to maintain undetected communication. Various techniques have been proposed for establishing covert channels, including those at the network level, and for using different components. This study investigated the security implications of Apple's iBeacon broadcast messages by focusing on the establishment of covert channels. We introduce two Bluetooth Low Energy (BLE) covert channels: one using broadcast payloads and the other employing broadcasting intervals. These channels can be used in a complementary manner, balancing covertness and bandwidth. In our evaluation, the payload-based covert channel achieved a maximum throughput of 911,600 Bytes per second (Bps) with a Packet Delivery Rate (PDR) exceeding 75%, demonstrating its capability to transmit substantial data via iBeacon covertly. This study focuses on enhancing the security of BLE Beacon deployment.


1 INTRODUCTION


Covert channels are concealed or unauthorized communication methods within computer systems and networks. These channels are typically used to transmit information or data in a manner that circumvents or violates security policies and controls, ensuring that the communication content remains undetected. Over the past few decades, numerous techniques have been proposed for establishing covert channels at the network level (Tian et al., 2020; Saenger et al., 2020; Schmidbauer et al., 2022; Li et al., 2020). Covert channels can be established using various components such as Bluetooth (Claeys et al., 2019), voltage (Gnad et al., 2021), sound (Coyac-Torres et al., 2021), and light (Maiti and Jadliwala, 2019). Among these, particular attention to Bluetooth-based covert channels is essential, particularly with the increasing number of Things (IoT) devices. According to ABI Research, a global technology market advisory firm,


over 815 million Bluetooth-enabled products (ABIResearch, 2020). Moreover, internet companies such as Amazon, Alibaba, Google, Baidu, and Xiaomi not only provide Bluetooth-based services such as speech recognition, but Bluetooth's presence is also growing in various fields, including smart lighting, smart appliances, door locks, and sensors (ABIResearch, 2020).


BLE technology, designed for short-range communication between devices, has experienced explosive growth as a technology for communication and location-based services, particularly in the IoT context. BLE has become ubiquitous worldwide and is used in everyday life and various industrial environments owing to its high availability, low cost, low power consumption, and ease of deployment. They can operate on coin-cell batteries or even without batteries (Mackey et al., 2020). Currently, BLE is integrated into most smartphones by default and supported by major operating systems such as iOS, Android, Linux, and Windows (Hernández-Rojas et al., 2017).

A BLE Beacon message implemented through the Apple iBeacon (iBeacon Homepage, 2015) or Google Eddystone (Eddystone, 2018) protocols is a small packet of data transmitted by a BLE device. These messages are typically designed to be broadcast at

^a <https://orcid.org/0009-0004-9934-4715>

^b <https://orcid.org/0000-0002-0482-2381>

^c <https://orcid.org/0000-0002-2418-5850>

^d <https://orcid.org/0009-0009-9528-4002>


^e <https://orcid.org/0000-0002-5777-4029>

Table 1: Previous studies on covert channels.

Category	Ref.	Contribution	Limitation
Covert Storage Channel	Priest et al. (2015)	- Analyze fields within the iBeacon packet that can be used for a covert channel	- Do not analyze the throughput adequately across various advertising intervals
	Zhang et al. (2020)	- Even in a highly monitored environment, detecting the tampering of fields is challenging	- Low transmission bandwidth - Limited modifiable bits
Covert Timing Channel	Seong et al. (2022)	- Microsecond-level precision time interval Adjustment - Enhancing security through encryption	- Hardware Modification Required - Limited payload length limits significant performance improvements in transmission
	Zhang et al. (2018)	- Improved robustness compared to IPD-based approaches - Encoding messages in gray code for channel noise mitigation	- Inefficient for large amount of data transfer - Prolonged messages may impact voice quality

regular intervals and serve a specific purpose: to convey information to nearby devices or applications. The BLE Beacons are commonly used in proximity marketing, location-based services, and context-aware applications. However, most existing beacon systems omit protection from the transmitted BLE beacon messages and other crucial protocol-specific parameters, which can lead to security vulnerabilities. This allows unauthorized devices to exploit beacons, such as eavesdropping, spoofing, and data interception (Kolias et al., 2017). Furthermore, the inherent nature of beacons, in which devices continuously broadcast their unique identifiers to signal their presence at specific locations, has the potential to establish covert communication through advertising without establishing connections between endpoint devices (Priest and Johnson, 2015; Na et al., 2021). Therefore, ensuring the security of beacon deployment is essential for protecting user privacy, preventing unauthorized access, and maintaining the integrity of the transmitted data.

In this study, we investigate the security implications of beacon broadcasts with a focus on Apple's iBeacon. Based on our analysis, we designed two BLE covert channels using storage and timing methods: one based on broadcast payloads (similar to a previous study (Priest and Johnson, 2015) and the other on broadcasting intervals. The two proposed covert channels can be used complementarily. For example, a payload-based covert channel can be used to transmit data when there is no monitoring or logging and a need to maximize the channel capacity. By contrast, the interval-based covert channel offers higher concealment than the payload-based channel but with a lower channel capacity. Among them, in this paper, we implement and evaluate the payload-based covert channel and evaluated its performance in terms of Packet Delivery Ratio (PDR) and throughput. Our experimental results reveal that the proposed channel has a maximum throughput of 911,600 Bytes

per second (Bps), making it an efficient covert channel.

Specifically, this study makes the following contributions:

- We investigated the security implications of iBeacon's broadcast messages with a focus on establishing covert channels.
- We designed two BLE covert channels using storage and timing methods: broadcast payload- and interval-based covert channels.
- We implemented and evaluated the proposed payload-based covert channels in terms of PDR and throughput. Our evaluation results show that the payload-based covert channel had a maximum throughput of 911,600 bps.

The structure of this paper is organized as follows. In Section 2, we analyze prior research on covert channels. In Section 3, we introduce iBeacon's background. In Section 4, we analyze the Apple iBeacon and design two covert channels using storage and timing channels. In Section 5, we describe the implementation and evaluation of the proposed payload-based covert channel from the perspectives of PDR and throughput. In Section 6, we discuss the covert timing channel case using iBeacon. Finally, Section 7 concludes the paper and proposes future research directions.

2 RELATED WORK

In this Section, we review previous studies on covert channels and analyze their contributions and limitations. A Covert Storage Channel (CSC) uses reserved or empty locations in legitimate packet fields (Tian et al., 2020; Seong et al., 2022), exploiting the imperfections in modern network protocol designs (Zhang et al., 2020). Covert Timing Channels (CTC) use differences in transmission time intervals, such as inter-packet delay (IPD) or packet retransmissions (Zhang

Table 2: iBeacon packet field description.

Field	Sizes (bytes)	Description
Flags	3	Each of Length, Type, and Value is composed of 1 byte. The '02' serves as a length indicator, indicating that an additional 2 bytes are present in the Flags field. The '01' in the Value field signifies the inclusion of flags, and '1A' represents the flag value.
Length	1	Displays the length of frame payload that comes after that field
Type	1	Indicates that the content of the frame is manufacturer-specific data
Company ID	2	Beginning of the manufacturer-specific advertising payload, '4C' indicates the Apple company ID number
Beacon Type	2	'02' is the protocol identifier, and '15' indicates the length of the subsequent payload
UUID	16	Application developers should define a UUID specific to their app and deployment use case
Major	2	Further specifies a specific iBeacon and use case. For example, this could define a sub-region within a larger region defined by the UUID.
Minor	2	Allows further subdivision of region or use case specified by the application developer
TX power	1	Value measured by Bluetooth device manufacturer from a 1 m distance

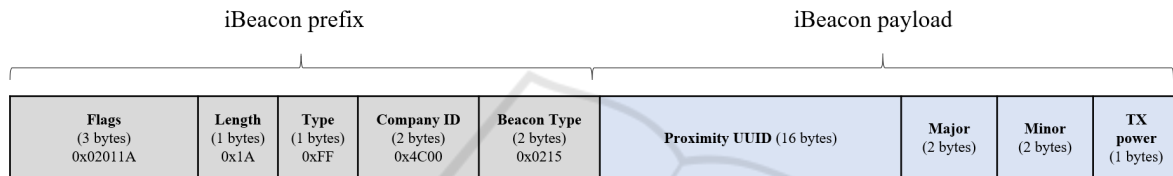


Figure 1: iBeacon packet structure.

et al., 2018; Tian et al., 2020; Seong et al., 2022). Table 1 categorizes and analyzes the previous research on CSC and CTC. Priest et al. (2015) asserted the possibility of applying a covert channel to Apple's iBeacon. The iBeacon prefix plays a role in identifying the identity of the iBeacon and modifying it would prevent it from being recognized as an iBeacon. Therefore, modifiable fields were analyzed without modifying the prefix to enable legitimate iBeacon receivers to interpret a packet as an iBeacon. They confirmed that by modifying the second byte of the Company ID, Universally Unique Identifier (UUID), Major, Minor, and TX power fields, a valid iBeacon could be created. They further investigated the number of advertisements a receiver could receive during the default advertising interval using a MacBook Pro and iPad Air 7. Priest et al. (2015) analyzed iBeacon fields to identify the fields in which a valid covert channel can be established. However, a limitation exists in that the performance of the covert timing channel using iBeacon has not been fully evaluated owing to the failure to analyze various advertising intervals. Zhang et al. (2020) proposed a covert storage channel by modifying the RTCP payloads in the Voice over Long Time Evolution (VoLTE) channel. They set up an environment by installing a TCP dump on two different mobile devices running on an Android operating system. These devices have varying security levels, and this study differentiates between a strictly monitored

environment and an unmonitored environment to establish a covert channel. In a strictly monitored environment, they created a covert channel by modifying only the lowest bit of the jitter field in the RTCP packets using the time difference between the data packets arriving at the endpoint and application processing those packets. Conversely, they increased the transmission bandwidth in a less strictly monitored environment using the EHSNR and BLP fields to compensate for the slow transmission speed. Zhang et al. (2020) validated the difficulty of detecting tampered fields in a constructed covert storage channel, even in a strictly monitored environment, by using the K-S test. However, they encountered limitations owing to their low transmission bandwidth and limited number of modifiable field bits.

Seong et al. (2022) has developed a covert wireless unidirectional communication mechanism using the Beacon Interval (BI) of public Access Points (APs) in an IEEE 802.11 environment. They proposed a frame structure to ensure the confidentiality and integrity of the transmitted information and introduced the Ping Pong Covert Timing Channel (PPCTC) data encoding method to reduce detectability. Although the proposed mechanism is unidirectional, it ensures stable communication by providing error recovery capabilities for consecutive 2-bit errors. To implement an AP that simultaneously provides legitimate services to authorized users while

transmitting signals to covert receivers, Seong et al. (2022) used OpenWiFi, following 802.11 a/b/n standards and Xilinx Zynq. They also controlled the time differences within tens of microseconds by switching from a jiffies-based Linux kernel timer to high-resolution kernel timer. The study by Seong et al. (2022) significantly increased confidentiality by precisely adjusting the time intervals and implementing more covert messages using SHA-1 and XOR encryption. However, there are limitations, such as the need for hardware modifications and restricted payload length, which significantly hamper transmission performance. Zhang et al. (2018) proposed a covert channel that adjusts the silence periods in the VoLTE environment. Because the IPD of VoLTE traffic is fixed and cannot be applied at the application level, covert messages are encoded into unique symbols by adjusting the silent periods and transmitting them. Before transmission, the sender and receiver share custom parameters, and the receiver decodes the covert messages upon reception. They used gray coding to encode messages to mitigate channel noise and tested undetectability using KS and KLD tests. Zhang et al. (2018) increased robustness compared with IPD-based methods demonstrated undetectability in the VoLTE environment. However, transmitting large amounts of data is inefficient, and longer silent periods can affect voice quality.

Previous research had limitations related to payload length, making it challenging to improve the transmission performance or transmit large amounts of data efficiently. In addition, although numerous studies have been conducted on building covert channels in 802.11 networks or VoLTE, research on creating covert channels in Bluetooth environments, particularly using beacons, has not been as active. This study aims to implement and evaluate a high-throughput covert channel using beacons.

3 BACKGROUND

3.1 iBeacon

Bluetooth beacons are low-cost, low-power, location-based technologies that use the BLE protocol. The two standard communication protocols for beacons are iBeacon, developed by Apple, and Eddystone, developed by Google (Mackey et al., 2020; Griffiths et al., 2019). Beacons can broadcast Bluetooth signals with several bytes of information and a Universally Unique Identifier (UUID) to the surrounding environment (Griffiths et al., 2019). BLE operates in the unlicensed 2.4 GHz ISM band and uses frequency

hopping to minimize interference with other RF devices operating in the same band, making it suitable for building covert channels (Hernández-Rojas et al., 2017). iBeacon technology is industrially available and has real-world applications, making it a valuable research target (Kolias et al., 2017). The iBeacon protocol, introduced in 2013, uses a one-way discovery mechanism to transmit small data packets at predefined intervals. While Bluetooth allows for various advertising intervals, iBeacon fixes the advertising interval at 100 ms (Gast, 2014). The maximum range of iBeacon transmission can vary depending on location and placement, with long-range beacons capable of reaching up to 450 m (Griffiths et al., 2019). Fig. 1 and Table 2 illustrate the structure of the iBeacon advertising packet (Priest and Johnson, 2015; Gast, 2014; Dalkılıç et al., 2017; Developer, 2014). The fields before the UUID constitute the iBeacon prefix, and modifying this part prevents the packet from being correctly identified by iBeacon receivers. However, modifying the UUID and major and minor parts does not affect the transmission validity, enabling the use of a 20-byte data payload. The distance to the beacon device can be estimated using the TX power and current Received Signal Strength Indicator (RSSI) of the received signal (Dalkılıç et al., 2017). Apple's API provides developers with four states: immediate, near, far, and unknown (Priest and Johnson, 2015; Developer, 2014). Therefore, if the TX power byte is modified and the distance cannot be estimated accurately, the API returns an 'unknown' descriptor, creating a valid covert channel without disrupting the iBeacon protocol unknown (Priest and Johnson, 2015).

4 iBeacon COVERT CHANNEL

4.1 Design Overview

Payload-based Covert Channel. The payload-based iBeacon covert storage channel model is shown in Fig. 2. The sender and receiver agree that the advertising packet received at a particular interval in advance contains covert message. The sender advertises the iBeacon packet by forging the payload according to the agreed rules. For example, they agree that a packet received at 500 ms contains covert message. The sender advertises the packet by including the covert message in the UUID, Major, and Minor fields, the sequence number in the TX power, and setting the advertising interval to 500 ms. The sender and receiver can exchange messages without establishing a connection, and message reception is possible without hardware modifications.

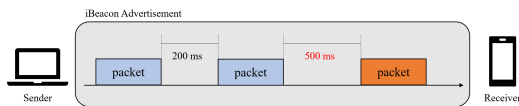


Figure 2: Payload-based covert channel (CSC-style) using iBeacon.

Interval-Based Covert Channel. The interval-based iBeacon covert timing channel model is shown in Fig. 3. If the sender and receiver agree on an interval rule beforehand, the sender encodes the message and advertises the iBeacon packets according to the agreed-upon rule. For example, if we consider Morse code - as 0 and - as 1, 'A' can be converted to '0 1.' Let us assume that they agree on the rule that if the packet arrives between 200 and 300 ms, it is interpreted as 0, and if it arrives between 400 and 500 ms, it is interpreted as 1. In this scenario, the sender can transmit 'A' by advertising a packet once between 200 and 300 ms and once between 400 and 500 ms. Like the payload-based covert channel, there is no need for device-to-device connection or hardware modification.

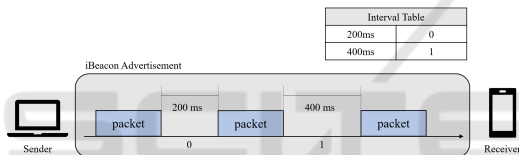


Figure 3: Interval-based covert channel (CTC-style) using iBeacon.

4.2 Covert Channel implementation

Payload-Based Covert Channel. Based on Section 4.1, the payload-based iBeacon covert channel forges the iBeacon's UUID, Major, Minor, and TX power fields. Fig. 4 shows an example of a payload where UUID, Major, and Minor are arbitrarily set, and TX power is used as the sequence number. Fig. 5 shows the commands used to configure the Bluetooth interface with the advertisement payload from Fig. 4. The OGF code for the LE Controller Commands is defined as 0x08. '0x0008' corresponds to the LE Set Advertising Data Command, which allows for the configuration of data used in advertising packets with data fields (Bluetooth, 2016). The value '1E' represents the length of the entire payload, excluding itself (Priest and Johnson, 2015; Bluetooth Core Specification 5.0., 2016).

Interval-Based Covert Channel. The interval-based covert channel encodes data within the advertising intervals by modifying the advertising interval of the iBeacon packet. The range of BLE advertising intervals should be between 20 ms and 10.24 s and a mul-

tiples of 0.625 ms (Bluetooth, 2016; Shan and Roh, 2018). Fig. 6 shows the commands used to modify the advertising interval. '0x0006' corresponds to the LE Set Advertising Parameters Command, allowing the configuration of advertising parameters. Advertising_Interval_Min should be less than or equal to Advertising_Interval_Max, and it is advisable not to set them to the same value when determining the optimal advertising interval. The 2 bytes at positions 'A0 00' represent Advertising_Interval_Min, and the 2 bytes at positions '40 01' represent Advertising_Interval_Max. On multiplying 0x00A0 by 0.625 ms, 100 ms is obtained, and on multiplying 0x0140 by 0.625 ms, 200 ms is obtained, indicating that it is configured to advertise at intervals of 100 to 200 ms. The '03' represents Advertising_Type, indicating nonconnectable advertising. When Advertising_Type is 0x03 (ADV_NONCONN_IND), Advertising_Interval_Min and Advertising_Interval_Max should not be set to values less than 0x00A0 (100 ms) (Bluetooth Core Specification 5.0., 2016). Therefore, in this study, the advertising interval range was set from 100 to 2000 ms in 100 ms increments for performance measurement. '0x000A' is the LE Set Advertising Enable Command, allowing the start of advertising by setting the Advertising Enable command to '0x01' (Advertising is enabled).

5 PERFORMANCE EVALUATION

5.1 Experimental Environment

In this Section, we describe the experimental environment for implementing a covert storage channel using iBeacon based on the commands outlined in Section 4. The experiment was conducted in a Raspberry Pi 3 B+ environment using Python 3, and the transmitter and receiver codes were implemented by entering the commands into the terminal using hcitool. Bluez is a library that enables efficient Bluetooth modular implementation on Linux systems (bluez Homepage, 2016), and version 5.55 was installed. The transmitting Raspberry Pi advertises iBeacon packets with packet data, as described in Section 4, whereas the receiving Raspberry Pi receives iBeacon packets from the transmitting Raspberry Pi and outputs the reception time, raw data, and raw data converted into hexadecimal.

To identify successfully Received and Missing Packets, we included sequential sequence numbers from 1 to 60 at the end of the payload. The PDR for each advertising interval was calculated using Equation (1) and rounded to the third decimal place.

iBeacon prefix (9 bytes) 0x02011A1AFF4C000215	Proximity UUID (16 bytes) 0x112233445566778899AABBCCDDEEFF12	Major (2 bytes) 0x0000	Minor (2 bytes) 0x0000	TX power (1 bytes) sequence number
---	--	-------------------------------------	-------------------------------------	---

Figure 4: Payload that uses the TX power field as a sequence number.

```
hcitool -i hci0 cmd 0x08 0x0008 1E 02 01 1A
FF 4C 00 02 15 11 22 33 44 55 66 77 88 99 AA
BB CC DD EE FF 12 00 00 00 00 C8 00
```

Figure 5: Advertisement payload configuration command.

```
hcitool -i hci0 cmd 0x08 0x0006 A0 00 40 01
03 00 00 00 00 00 00 00 00 07 00
hcitool -i hci0 cmd 0x08 0x000A 01
```

Figure 6: Advertising interval configuration command.

$$PDR(\%) = \frac{(Received\ packets) * 100}{(Total\ packets)} \quad (1)$$

As shown in Fig. 1 in Section 3, the UUID, Major, Minor, and TX power can be used as covert channel fields in the iBeacon payload; therefore, 20 bytes of information can be transmitted per packet. Therefore, the Max Throughput equation and Min Throughput equation for each advertising interval are as follows formula (2) and (3) (Ameri and Johnson, 2017), respectively, rounded from the first decimal place.

$$Maxthroughput (Bps) = \frac{(Received\ packets) * 20}{min_advertising_interval} \quad (2)$$

$$Minthroughput (Bps) = \frac{(Received\ packets) * 20}{max_advertising_interval} \quad (3)$$

5.2 Experimental Results

In this Section, PDR and throughput are used as evaluation indicators to verify the performance of the proposed covert channel using iBeacon. We transmitted 60 packets per advertisement interval from the transmitter to the receiver and repeated this process 100 times to calculate the average number of successfully received and missing packets. Table 3 and Fig. 7 represent the PDR by Advertising Interval, while Table 4 calculates the throughput from 100 to 2000 ms with a 100 ms difference between the min and max advertising intervals. If the advertising interval is 100–200 ms, packets are sent randomly at intervals between 100 and 200 ms.

As a result of the experiment, the best PDR was 77.1% for 1700–1800 ms, and the worst PDR was 75.25% for 600–700 ms, showing a 1.85%p difference, confirming that they are similar overall. The shorter the advertising interval, the greater the throughput, with the largest throughput of 100–200 ms. This means that no matter which advertising interval is selected and sent, packets are sent constantly, and information can be exchanged by selecting the appropriate advertising interval according to the circumstances of the sender and receiver.

6 DISCUSSION

In this study, we designed and implemented two types of iBeacon covert channels. The Payload-based covert channels can be used to transfer data if there is no monitoring or logging and the channel capacity needs to be maximized; however, they have low concealment. Interval-based covert channels offer higher concealment than payload-based channels but have low channel capacity and can cause delays depending on the transmission environment. These two channels can be used complementarily. For example, data can be sent to an interval-based covert channel

Table 3: PDR per Advertising Interval.

Index	Advertising interval (ms)	Received Packets	Missing Packets	PDR (%)
1	100–200	4,558	1,442	75.97
2	200–300	4,580	1,420	76.33
3	300–400	4,585	1,415	76.42
4	400–500	4,543	1,457	75.72
5	500–600	4,578	1,422	76.3
6	600–700	4,515	1,485	75.25
7	700–800	4,613	1,387	76.88
8	800–900	4,528	1,472	75.47
9	900–1000	4,575	1,425	76.25
10	1000–1100	4,581	1,419	76.35
11	1100–1200	4,580	1,420	76.33
12	1200–1300	4,572	1,428	76.2
13	1300–1400	4,580	1,420	76.33
14	1400–1500	4,581	1,419	76.35
15	1500–1600	4,566	1,434	76.1
16	1600–1700	4,569	1,431	76.15
17	1700–1800	4,626	1,374	77.1
18	1800–1900	4,614	1,386	76.9
19	1900 - 2000	4,571	1,429	76.18



Figure 7: PDR and Throughput per Advertising Interval.

Table 4: Throughput per Advertising Interval.

Index	Advertising interval (ms)	Max throughput (Bps)	Min throughput (Bps)
1	100–200	911,600	455,800
2	200–300	458,000	305,333
3	300–400	305,667	229,250
4	400–500	227,150	181,720
5	500–600	183,120	152,600
6	600–700	150,500	129,000
7	700–800	131,800	115,325
8	800–900	113,200	100,622
9	900–1000	101,667	91,500
10	1000–1100	91,620	83,291
11	1100–1200	83,273	76,333
12	1200–1300	76,200	70,338
13	1300–1400	70,462	65,429
14	1400–1500	65,443	61,080
15	1500–1600	60,880	57,075
16	1600–1700	57,113	53,753
17	1700–1800	54,454	51,400
18	1800–1900	51,267	48,568
19	1900 - 2000	48,116	45,710

while forging a portion of the payload to include a sequence number. Simply adding a sequence number to the payload allows the receiver to recognize a packet missing even if an error occurs during transmission. This not only changes the advertising interval but also involves forging the payload, allowing for achieving a higher level of accuracy in CTC.

7 CONCLUSION

Although several covert channels have been studied, research on covert channels using Bluetooth has not yet been conducted. However, Bluetooth is closely related to real life, and the possibility of abuse of covert channels cannot be ruled out. In this study, we

designed the CSC and CTC using the iBeacon payload and advertising interval. In addition, we implemented the designed CSC and evaluated its PDR and throughput. Overall, the PDR remained consistently above 75%, and the advertising interval with the highest throughput relative to the PDR was in the range of 100–200 ms. In this study, experiments were conducted based on iBeacon; however, covert channels could be established in other beacons, such as Eddystone.

We have shown from experimental results that large amounts of data can be secretly transmitted and received using the characteristics of beacon. Future studies will implement and evaluate the interval-based covert channel. Also, we would like to consider countermeasure to prevent beacon covert channel.

ACKNOWLEDGEMENTS

This work was partly supported by the Korea Institute for Advancement of Technology (KIAT) grant funded by the Korean Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialists) and MSIT under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310), supervised by the Institute of Information Communication Technology Planning and Evaluation (IITP).

REFERENCES

- ABIresearch (2020). Bluetooth iot market set to nearly quadruple by 2024 as smart home exceeds 800 million device shipments. <https://www.abiresearch.com/press/bluetooth-iot->

- market-set-nearly-quadruple-2024-smart-home-exceeds-800-million-device-shipments/.
- Ameri, A. and Johnson, D. (2017). Covert channel over network time protocol. In *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*, pages 62–65.
- Bluetooth, S. (2016). Proprietary : Bluetooth core specification v5.0.
- bluez Homepage (2016). <http://www.bluez.org/about/>.
- Claeys, T., Rousseau, F., Simunovic, B., and Tourancheau, B. (2019). Thermal covert channel in bluetooth low energy networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 267–276.
- Coyac-Torres, J. E., Rivero-Angeles, M. E., and Aguirre-Anaya, E. (2021). Cognitive radio based system for best effort communications in sound-based covert channel for iot environments. *Mobile Networks and Applications*, 26:1449–1460.
- Dalkılıç, F., Çabuk, U. C., Arıkan, E., and Gürkan, A. (2017). An analysis of the positioning accuracy of ibeacon technology in indoor environments. In *2017 International Conference on Computer Science and Engineering (UBMK)*, pages 549–553. IEEE.
- Developer, A. (2014). Getting started with ibeacon. *Retrieved May*, 10:2018.
- Eddystone (2018). <https://github.com/google/eddystone/>.
- Gast, M. S. (2014). *Building applications with iBeacon: proximity and location services with bluetooth low energy.* ” O’Reilly Media, Inc.”.
- Gnad, D. R., Nguyen, C. D. K., Gillani, S. H., and Tahoori, M. B. (2021). Voltage-based covert channels using fpgas. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 26(6):1–25.
- Griffiths, S., Wong, M. S., Kwok, C. Y. T., Kam, R., Lam, S. C., Yang, L., Yip, T. L., Heo, J., Chan, B. S. B., Xiong, G., et al. (2019). Exploring bluetooth beacon use cases in teaching and learning: Increasing the sustainability of physical learning spaces. *Sustainability*, 11(15):4005.
- Hernández-Rojas, D. L., Fernández-Caramés, T. M., Fraga-Lamas, P., and Escudero, C. J. (2017). Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through ble beacons in iot telemetry applications. *Sensors*, 18(1):57.
- iBeacon Homepage (2015). <https://developer.apple.com/ibeacon/>.
- Kolias, C., Copi, L., Zhang, F., and Stavrou, A. (2017). Breaking ble beacons for fun but mostly profit. In *Proceedings of the 10th European Workshop on Systems Security*, pages 1–6.
- Li, Y., Zhang, X., Xu, X., and Tan, Y.-a. (2020). A robust packet-dropout covert channel over wireless networks. *IEEE Wireless Communications*, 27(3):60–65.
- Mackey, A., Spachos, P., Song, L., and Plataniotis, K. N. (2020). Improving ble beacon proximity estimation accuracy through bayesian filtering. *IEEE Internet of Things Journal*, 7(4):3160–3169.
- Maiti, A. and Jadliwala, M. (2019). Light ears: Information leakage via smart lights. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3):1–27.
- Na, X., Guo, X., He, Y., and Xi, R. (2021). Wi-attack: Cross-technology impersonation attack against ibeacon services. In *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE.
- Priest, J. and Johnson, D. (2015). Covert channel over apple ibeacon. In *Proceedings of the International Conference on Security and Management (SAM)*, page 51. The Steering Committee of The World Congress in Computer Science, Computer
- Saenger, J., Mazurczyk, W., Keller, J., and Caviglione, L. (2020). Voip network covert channels to enhance privacy and information sharing. *Future Generation Computer Systems*, 111:96–106.
- Schmidbauer, T., Keller, J., and Wendzel, S. (2022). Challenging channels: Encrypted covert channels within challenge-response authentication. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–10.
- Seong, H., Kim, I., Jeon, Y., Oh, M.-K., Lee, S., and Choi, D. (2022). Practical covert wireless unidirectional communication in ieee 802.11 environment. *IEEE Internet of Things Journal*, 10(2):1499–1516.
- Shan, G. and Roh, B.-H. (2018). Advertisement interval to minimize discovery time of whole ble advertisers. *IEEE Access*, 6:17817–17825.
- Tian, J., Xiong, G., Li, Z., and Gou, G. (2020). A survey of key technologies for constructing network covert channel. *Security and Communication Networks*, 2020:1–20.
- Zhang, Q., Zhang, X., Xue, Y., and Hu, J. (2020). A stealthy covert storage channel for asymmetric surveillance volte endpoints. *Future Generation Computer Systems*, 102:472–480.
- Zhang, X., Tan, Y.-A., Liang, C., Li, Y., and Li, J. (2018). A covert channel over volte via adjusting silence periods. *IEEE Access*, 6:9292–9302.