Practical Covert Wireless Unidirectional Communication in IEEE 802.11 Environment

Hayoung Seong, *Student Member, IEEE*, Ikkyun Kim, Yongsung Jeon, Mi-Kyung Oh, Sangjae Lee, and Dooho Choi, *Member, IEEE*

***Abstract*—Covert communications, or covert channels, are commonly exploited to establish a data exfiltration channel from an insider on a trusted network to a malicious receiver outside the network without using normal communication of the network. It is because the malicious receiver is an unauthorized user of the communication network and so he cannot communicate with any entity in the network. In this study, we construct a new covert wireless unidirectional communication mechanism in an IEEE 802.11 environment. Our covert communication is based on a covert timing channel exploiting the beacon interval of a given commercial-like AP. Because the wireless covert channel we proposed can be implemented only with firmware modification to the WLAN MAC protocol, it is very suitable for application in a real public AP environment. In order to dramatically reduce the chance of covert signals being detected by others, a new and simple covert data encoding scheme, called ping-pong covert timing channel (PPCTC), is proposed, and we show that the covertness of the PPCTC is excellent compared to the previous timing-based covert channels. Although this wireless covert communication is unidirectional communication, since PPCTC has recovery characteristics against consecutive 2-bit errors, stable communication is guaranteed. Furthermore, a covert frame structure is presented for providing the confidentiality and integrity of the information transmitted via our covert channel. To the best of our knowledge, this is the first attempt.**

***Index Terms*—Covert AP, covert frame structure, covert timing channel (CTC), interpacket delay (IPD) CTC, packet loss recovery.**

I. Introduction

A. Background

COVERT communication is a type of attack to create an abnormal communication channel to transfer information to a malicious entity that is not supposed to be authorized to communicate. The covert channel was defined as a hidden communication method that guarantees that people can communicate without being noticed by others in legitimate communication [1]. The covert channels are categorized as network covert channels and wireless covert channels (WCCs). A network covert channel is one that is built into the network layer (or upper protocol layer) [2], [3], [4], [5], [6], [7], [8], [9], [10], whereas a WCC is one that primarily exploits the MAC/physical-layer characteristics of wireless communication [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37]. Network covert channels are also divided into storage and time aspects depending on the type of resource shared in the legitimate channel [38].

1) *Covert Storage Channel (CSC):* It is a technique that utilizes a reserved or empty position in the field of a legitimate packet. The covert data of the CSC method still remains in the transmitted packet, and hence, the covert channel based on the CSC can be easily detected if the transmitted packets are carefully investigated.
2) *Covert Timing Channel (CTC):* It exploits the time difference between time intervals to transmit, such as interpacket delay (IPD) or packet retransmissions. However, since CTC may violate the specification of the protocol, legitimate user communication may be interrupted, and by analyzing the distribution of the time difference between overt and covert time intervals statistically, the covert channel may be detected.
3) *WCC:* It is mainly designed by hiding the data in the modulation process on the physical layer or embedding the data into the redundant fields of the MAC layer protocol of wireless communication. It is very difficult that the modulation modification method be applied to the commercial wireless device environment, since it is necessary to modify the modulation/demodulation processes of the transmitter/receiver, respectively. However, in the case of the MAC layer protocol modification method, there is a possibility that it can be applied to commercial equipment through firmware modification.

Traditionally, network covert channels have been actively studied as wired network layer targets. However, research on the covert channel has recently been extended to a wireless environment, such as a WLAN and mobile phone, and various WCC methods suitable for the wireless environment have been proposed [6], [15], [16], [18], [19], [20], [21], [22], [23].

Manuscript received 30 June 2021; revised 31 October 2021, 27 December 2021, 27 February 2022, and 17 April 2022; accepted 5 September 2022. Date of publication 8 September 2022; date of current version 6 January 2023. This work was supported in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant funded by the Korea Government (MSIT, Study on Wireless Covert Channel Risk Verification) under Grant 2020-0-00913. *(Corresponding author: Dooho Choi.)*

Hayoung Seong is with the Department of Information Security Engineering, University of Science and Technology, Daejeon 34113, South Korea (e-mail: shy2028@ust.ac.kr).

Ikkyun Kim, Yongsung Jeon, Mi-Kyung Oh, and Sangjae Lee are with the Information Security Research Division, Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea (e-mail: ikkim21@etri.re.kr; ysjeon@etri.re.kr; ohmik@etri.re.kr; leestrike@etri.re.kr).

Dooho Choi is with the Department of AI Cyber Security, College of Science and Technology, Korea University Sejong, Sejong 30019, South Korea (e-mail: doohochoi@korea.ac.kr).

Digital Object Identifier 10.1109/JIOT.2022.3204987

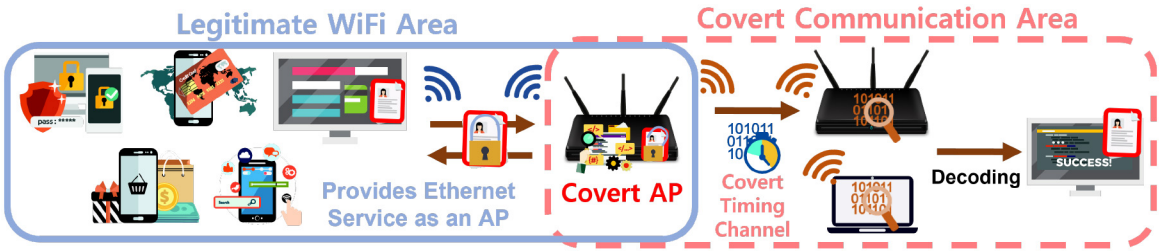

Fig. 1. Application scenario of covert unidirectional communication.

AP broadcast packet is a packet that informs the AP information periodically so that it helps a mobile device access the AP and anyone receive this broadcast packet without any connection. Therefore, this allows the covert channel receiver to receive and decode covert data sent by the AP without accessing the AP if it is possible to construct a wireless CTC exploiting this broadcasting packet. Conventional proposed covert channels also use the broadcast transmission characteristics of 802.11 WLAN. The most popular method in the 802.11 WLAN CTC is the IPD method [17], [18], [19].

In the case of the existing IPD-based CTCs, a covert channel is implemented at the application level, and the values used for packet delay are tens of milliseconds (ms). Since the packet delay of several tens of ms has a considerable large broadcast packet transmission interval difference, this unusual time interval difference of the broadcast packet of the CTCs might be detected by the legitimate receivers easily. To overcome this problem, several WCC methods based on subtle distortions of the physical level wireless signal have been proposed in [20], [21], and [34]. However, these WCCs require a transmitter and receiver equipped with special wireless communication hardware that is different from a general commercial wireless AP.

B. Motivations

An AP in the open wireless communication environment can covertly transfer some information to unauthorized receiver(s) if a covert wireless communication mechanism can be implemented by firmware modification of a commercial AP. And, it is quite reasonable that a covert wireless unidirectional communication should meet the following properties. The similar metrics were presented in [29]

1) *Covertness:* It should be highly difficult for anyone to notice these covert signals except for a receiver of the covert communication. That is, covertness means the undetectability for the covert signals in the legitimate signals. To verify the covertness, several studies [9], [10] used the distribution similarity between legitimate and covert signals.
2) *Concealment:* Even if anyone recognizes the covert signal, it should be impossible to decode the information over the covert channel.
3) *Transparency:* The covert communication should not interfere with existing legitimate user communications. If there is a small change, slowness, or abnormality in legitimate user communication during the covert communication works, it can be evidence of the presence of a covert communication signal.
4) *Robustness:* Covert unidirectional communication has to have an adequate error recovery capability since it is impossible that the receiver requests retransmission to the transmitter.

The purpose of this study is to design and implement a covert wireless unidirectional communication satisfying the above four properties in an actual WLAN environment. Fig. 1 shows a conceptual application scenario of covert unidirectional communication in the public WLAN environment. In fact, the user in the covert communication area of Fig. 1 might be an attacker who wants to obtain some information from the entities in the legitimate WiFi area. The AP with the covert communication mechanism provides Internet service to legitimate users, while at the same time acting as a covert communication transmitter (a covert AP).

C. Our Contributions

As we described, there are four ways to construct a covert channel, that is, CSC, CTC, and WCC in the physical layer, and WCC in the link layer. And each method has the following technological drawbacks.

1) Covertness of CSC is weak, since it can be easily detected if the network packets are carefully investigated.
2) In the case of CTC, a large time difference (e.g., tens of ms) between normal and covert signals can break its covertness and the specification of its network protocol.
3) In the case of WCC in the physical layer, its covertness is very high. However, since a special transmitter/receiver is required, it is impossible to apply the commercial AP in public wireless communication.
4) For WCC in the link layer, a method hiding covert messages in the redundant field of MAC protocol of wireless communication might be detected easily since it is similar to the CSC method.

Therefore, a CTC exploiting tiny variations in the time interval of the broadcast packet of an AP could be a good candidate to build a covert wireless unidirectional communication in the public WLAN environment. In this work, we attempt to construct a covert wireless unidirectional communication satisfying the covertness, concealment, transparency, and robustness. More precisely, the main contribution of this study can be addressed as follows.

1) *Implementation to Strengthen the Covertness of Covert Signals:* In IPD-based CTC, the time difference of time

interval of broadcast packets is the main key for transmitting covert signals, but it might be easy that covert signals are detected by others if this time difference is large. Therefore, an attempt to reduce this time difference is directly related to strengthening the covertness of a given CTC. We implement a covert AP that provides legitimate service to legitimate users and transmit covert signals to a covert recipient at the same time. In our implementation, we can control the precise time difference within tens of microseconds (μs). Note that the time difference of the previous works [20], [21] is tens of ms.

2) *Adequate Encoding Scheme for Increasing the Covertness and Robustness:* We propose a data encoding scheme that is called ping-pong CTC (PPCTC). The PPCTC basically has a complementary and iterative characteristic in time differences of covert time intervals, and the characteristic that the occurrence of "1" among all transmitted bits is very dominant. These characteristics and μs-level time difference control induce a huge improvement in covertness compared to other CTCs. We prove it by checking the Jaccard index, ϵ-similarity, and KL-divergence. Furthermore, our PPCTC has the capability to be able to recover consecutive 2-bits errors. This error recovery property is directly related to robustness.
3) *Frame Structure to Prevent Data Exposure:* We design a message frame structure with a simple data encrypting mechanism using SHA-1 hash function and XOR-ing (called a covert frame). This does not cause a decrease in communication latency when adding our covert frame over the PPCTC, since it does not require heavy computation costs for computing SHA-1 and XOR-ing, and hence, it can be a practical solution to satisfy the concealment property.

It is emphasized that the PPCTC, which is a new encoding scheme for our wireless CTC on WLAN, plays a central role to support to strengthen the covertness and robustness properties compared to other CTCs on WLAN. Therefore, the PPCTC design itself is the main novelty of our work, which is described in this article. It is also noted that our PPCTC does not interrupt synchronization for normal wireless communication between legitimate users and the AP, although the PPCTC distorts the beacon packet intervals of the AP.

Furthermore, the covert frame, which provides message structure and concealment, is the first attempt among this kind of WCCs on the WLAN environment.

D. Organizations

The remainder of this article is organized as follows: In Section III, we discuss components required for making the CTCs using AP, such as the WLAN beacon packet, which is related to a periodic signal for using CTC, and a commonly used component of the frame structure, which is related to our proposed frame structure. In Section II, we discuss the related works including the existing CTC methods. In Section IV, we construct our covert wireless unidirectional communication mechanism exploiting the beacon interval (BI) of a public AP in detail. The experimental results and analysis are provided in Section V to prove that our mechanism is a good candidate satisfying the covertness, transparency, robustness, and concealment. Finally, the discussion and conclusions are drawn in Sections VI and VII, respectively.

II. Related Works

In this section, we review conventional covert communication according to the method and medium for delivering covert data. As we mentioned, we categorized covert communication as CSC, CTC, and WCC. The CSC and CTC are commonly performed at the upper layer, including the network layer. On the other hand, the WCC represents covert communication using wireless characteristics and is performed at the lower layer, such as the MAC layer and physical layer.

CSC: Szary *et al.* [2], Mazurczyk *et al.* [3], [4], and Saenger *et al.* [5] represented the upper layer of CSCs. Szary *et al.* [2] and Mazurczyk [3] applied the concept of reversible data hiding to storage network covert channels. Szary *et al.* [2] proposed an HTTP header CSC for an efficient and robust covert data injection mechanism. Mazurczyk *et al.* [3] implemented using IPv4 flows and they exploited the covert CSC using reversed fully or partially for the transmission data. Mazurczyk *et al.* [4] proposed six different data hiding techniques for the IPv6 environment. The IPv6 protocol has a bigger header size compared with the IPv4 protocol and the author proposed hiding mechanisms using a larger size of the IPv6 header field. Most CSCs were proposed by the methods using the header field. Saenger *et al.* [5] proposed HTTP header CSC for the efficient and robust covert data injection mechanism. Szary *et al.* [2], Mazurczyk [3], [4], and Saenger *et al.* [5] modified some specific bits or changed the order of bits. Therefore, this kind of method is easy to implement covert communication. However, since all hiding data remains in the packet field, there is a risk of being detected by others.

CTC: The CTC represents the network layer CTCs [6], [7], [8], [9], [10]. Tian *et al.* [6] proposed CTC VoIP streams using bit rate switching, and they designed a new carrier encoding scheme to improve security. Hovhannisyan *et al.* [7] proposed a new framework for IP-timing where the main idea is to use the routes to carry information. The IP-timing-based covert channels are based on TCP and UDP.

Rezaei *et al.* [8] proposed a delayed packet one indicator (DPOI) that increases capacity and reduces bit errors. The DPOI method removes the rest timing, which means the bit value "0," in on–off covert timing channel (on–offCTC), and uses the covert timing interval to inform the bit value "0." Here, the covert timing interval means delayed packet transmission, but the covert timing itself does not mean a bit value of "0," and serves as an indicator to inform that the following overt timing interval is a bit value "0." For example, in the DPOI method, when the covert transmitter sends packets at overt time intervals, it means a bit value of "1." On the other hand, when the covert transmitter sends a packet with a covert time interval and then sends a packet with an overt time

TABLE I
GENERAL PROS AND CONS FOR THE COVERT CHANNELS

	Pros.	Cons.
CSC	Easy to implement covert communication	Since all hiding data remains in the packet field, the presence of the covert communication can be easily detected
CTC	According to the real-time characteristics, no remains covert data	Covertness fully depends on the reveal of the time difference pattern of the normal communication packets
WCC (MAC)	Hard to detect the presence of the covert communications	It has similar drawbacks with the CSC and CTC. It is hard to synchronize the communication
WCC (PHY)	Very high covertness	Since dedicated transmitter and receiver are required for the covert communication, it is very hard to implement and apply(*i.e.* not practical)

interval, it means a bit value of "0." Since the DPOI method is CTC for a wired network environment that does not consider packet loss or wireless characteristics, it is not suitable for application to wireless CTC.

Cabuk *et al.* [9], [10] proposed an on–offCTC using network layer IP packets as a CTC in the network layer. On–offCTC is a method for transmitting covert data by transmission or rest. If the transmitter sends a packet, it means bit "1" of the covert data, and if it does not send a packet, it means bit 0.

WCC: The WCC refers to the covert channels in the wireless environment. It can be categorized into two types. One is a type to exploit the upper layer, including MAC layer protocol, such as in mobile network [11], [12], [13], [14], [15], [16], in IEEE 802.11 WLAN [17], [18], [19], [20], [21], [22], in IoT covert channel [24], [25], [26], [27], [28]. And, the other type is based on the physical layer which is commonly used in radio frequency (RF) signal characteristics. The study of physical covert channels are focused on countermeasure schemes as well as hiding schemes [23], [29], [30], [31], [32], [33], [34], [35], [36], [37].

The most of all the mobile environment CTCs are based on Voice over Long-Term Evolution (VoLTE) packets. Zheng *et al.* [11], Liang *et al.* [12], Li *et al.* [13], and Zhang *et al.* [14], [15], [16] proposed various CTC algorithms called ZM-CTC, MSC-CTC, RPDCRC, VRCTC, NoP-GCTC, and SPCC. To communicate covertly in LTE, they used packet drop, silence period, interleaving ordering, and rearrangement for the VoLTE packets. Also, they showed their performance in terms of communication according to the code word or modulation. Especially, Liang *et al.* [12] which called MSV-CTC focused on reliable communication in active packet loss and its interference environment. Their perspective of reliable communication is similar to our study, which uses Hash and XOR calculation for the multistage verification and error correction. However, MSV-CTC is targeted at the LTE environment and focused on modulation using code words. Despite these differences in communication environment and performance, in Section V, their performance metrics, such as BER or throughput are compared with our CTC informatively.

The WLAN covert channels are studied in terms of CSC [21], [22], CTC [17], [18], [19], [20]. To make CSC in 802.11, the covert channel sender injects covert data into a less used field, such as an empty field or reserved bit of a packet [21], [22]. However, The CSC method has a possibility of detection that possibility always exists regardless of wired or wireless because covert data is left in the packet field. Sawicki *et al.* [17], Walker and Fairbanks [18], Holloway and Beyah [19], and Radhakrishnan *et al.* [20] proposed WLAN CTC using back off time, modified schedule of control packets which is periodic packets of AP.

Walker and Fairbanks [18] proposed CTC in a WLAN environment using interarrival time of packets which are beacon and probe request packets. Through USP wireless adapters with Scapy and python script that allowed to set the packet intervals in software levels. They can control ms unit in terms of interarrival times of beacon packet. In this article, we proposed CTC which has μs unit delayed through implementation adjusting the timing at the firmware level.

Sawicki *et al.* [17] proposed a CTC called StegoFrameOrder (SFO). The SFO is slightly different for convention WLAN CTCs. They used multiple stations which can be sending 802.11 packets to construct covert channel. In other words, the SFO can not be constructed by one covert data sender. The sending order of each station represents the covert data. Thus, the throughput depends on the number of stations. In Section V, we compare the BER and throughput of SFO with our proposed CTC informatively.

Recently, the covert channel are studied in terms of physical layer [29], [30], [31] and IoT environment [24], [25], [26], [27], [28]. However, the physical layer covert channel which modified RF signals is not the scope of in this study. As we mentioned in Section I, in a public WLAN environment with commercial APs, it seems difficult to apply a physical-layer WCC, since it is required a special transmitter/receiver for covert communications.

We summarize common pros and cons for each kind of covert channels in Table I. In this article, to establish a practical WCC in the public WLAN environment, we exploit two kinds of covert communications, such as CTC and WCC(MAC). To overcome the cons of CTC and WCC(MAC), We exploit μs timing differences to communicate covertly through implementation and propose an encoding algorithm that can provide synchronization and self-recovery when a covert bit is lost.

III. PRELIMINARY

This section describes the beacon packet of IEEE 802.11, frame structure, and encoding technique, which are important

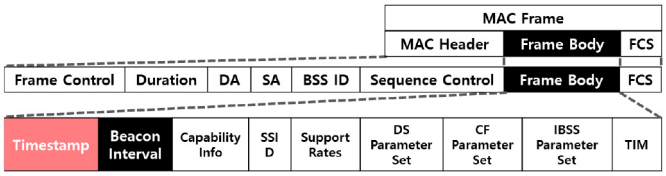

Fig. 2. WLAN 802.11 beacon frame.

components of the proposed PPCTC and covert frame, and deals with the contents applied to PPCTC. These three components are used to satisfy the requirements of covert communication.

A. IEEE 802.11 WLAN Beacon Frame

The IEEE 802.1 MAC layer generates a beacon packet and performs a scheduling function to always transmit the beacon at the same interval. To practically implement PPCTC, the interval of the beacon packet, which is a periodic packet of IEEE 802.11 AP, is used, and Fig. 2 shows the MAC beacon frame of IEEE 802.11. In covert communication, using the periodic packet can satisfy the requirements, which are covertness and satisfaction. First, in terms of covertness, through using periodic signals, we do not have to make additional signals. In other words, the timestamp field indicates the beacon generation time and is recorded based on the AP timer time. The value of the BI field indicates the interval of periodically transmitted beacon packets. Devices connected to the AP check the time in the BI field to synchronize with the AP. Therefore, when creating a CTC using a beacon in a WLAN environment, it is necessary to minimize the change in the time interval of the beacon so that the effect on legitimate users is minimal.

We implement the practical IEEE 802.11 CTC by sending packets a little earlier or slower than the time interval specified in the BI field, while the BI field value is not changed and the initial set value is maintained. At this time, the actual generation time of the beacon packet is automatically written in the timestamp field. Thus, the covert receiver can calculate the correct BI by subtracting the time of the previously received timestamp of the beacon packet from the timestamp of the currently received beacon packet. In this way, the covert receiver knows whether the bit value of the covert data is 0 or 1 through the calculated BI.

B. Communication Frame Structure

Most communication systems have an appropriate frame structure for better communication. The frame structure is continuously upgraded to apply the latest communication method, and many studies are being conducted, such as erasing existing fields or adding new fields [39], [40], [41], [42]. Nevertheless, there are fields that are necessarily included among the numerous frame structures. This section deals with fields that are essential in the communication frame structure. Examples of such fields are preamble, start frame delimiter (SFD), header, payload (data), and frame check sequence (FCS). Fig. 3 shows

Fig. 3. Common components of frame structure.

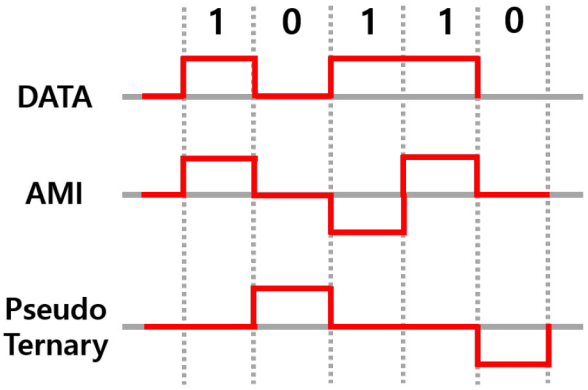

Fig. 4. Complement line coding scheme.

the fields that are essential for communication, regardless of whether it is wired or wireless.

The role of each field is as follows. First, the preamble field serves to synchronize the transceivers. The SFD field serves to inform the start of a packet after synchronization. When Rx receives the SFD, it recognizes the rest of the packet as meaningful data and starts decoding it. The header field contains information about the packet, such as packet type, source address, destination address, data length, and sequence number. Through the header field, the receiver can know the destination of the packet and can know the transmission order of the packet. The payload field contains the message sent by the sender. Finally, the FCS field serves to check whether there is an error in the data of the received packet. In some cases, the receiver requests retransmission from the sender through the step of checking the FCS field.

The proposed covert frame includes the five fields mentioned above, but some components of the header field are excluded. In particular, the reason for excluding the address part of the header field is that PPCTC is a communication method using broadcast packets and is a covert channel for communication between promised people. The covert frame is described in detail in Section IV-C.

C. Complement Line Code

There are two types of digital line coding methods: 1) alternating mark inversion (AMI) and 2) pseudo-ternary code [43]. The two-line coding schemes are characterized by their own complementarity. Here, complementarity means that the average of all amplitudes is zero. Fig. 4 shows binary bipolar-AMI and pseudo-ternary digital line coding methods according to data. In the AMI code method, the amplitude is changed when the data is 1, and in the pseudo-ternary code method, the amplitude is changed when the data is 0. Our designed PPCTC is similar to the pseudo-ternary code in that when the bit value is 0, the BI increases and decreases alternately. However, the

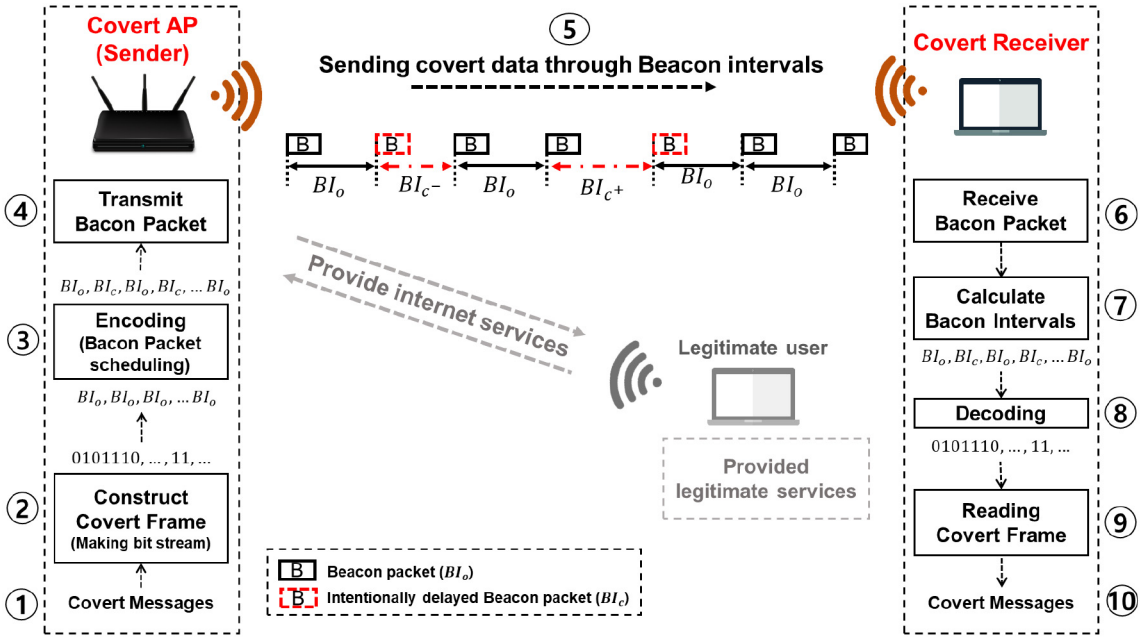

Fig. 5. Communication flow of the proposed covert unidirectional communication.

TABLE II
NOMENCLATURE

Symbol	Meaning
BI	Beacon Interval
BI_o	Overt beacon interval which refers to a time interval specified in the BI field of the beacon packet. BI_o is typically 102.4 ms. $BI_o \pm\delta$ is regard as BI_o Here, the δ is margin time.
BI_c	Covert beacon interval which a small delay is added or subtracted from the BI_o. $BI_c = BI_o \pm \alpha \pm \delta$, where α is intended small value of delay for implementation of covert AP ($\alpha = 30\mu s$). BI_c always existed pair as BI_{c+} and BI_{c-}.
BI_{c+}	$BI_o + \alpha\pm\delta$
BI_{c-}	$BI_o - \alpha\pm\delta$

method for encoding bit values in PPCTC is completely different from that of pseudo-ternary code. This is described in Section IV-B in detail.

IV. Constructing New Covert Wireless Unidirectional Communication

In this section, we propose a new covert unidirectional communication mechanism that exploits the BI of the public AP. We provide three aspects for our mechanism. First, we implement a covert AP with normal AP functionality to control the time of the BI within tens of microseconds (μs). Second, we propose a CTC, which is called the PPCTC, based on a small distortion of BIs. When transmitting data using the covert AP in a WLAN environment, PPCTC applies an encoding method to strengthen the covertness of transmitted covert data as much as possible, and the proposed encoding method provides 2-bit error recovery functionality. Finally, we describe a covert frame over the PPCTC to be able to provide the encryption and integrity of the covert data, and so it prevents data exposure to unauthorized users.

Fig. 5 demonstrates the overall communication flow of the proposed covert unidirectional communication in a practical environment. Each step of Fig. 5 is briefly described as follows.

1) A message is prepared to be transmitted.
2) To make bit stream, the covert AP constructs the covert frame according to the covert massages.
3) The encoding process controls the BIs according to the bit stream of the covert frame.
4) The covert AP transmits the beacon packets at each modified BIs according to the transmitted covert bits.
5) Covert messages through time differences of beacon packets are sent to a covert receiver.
6) Covert receiver receives beacon packets from covert AP.
7) The covert receiver calculates the BIs for series of beacon packets.
8) The calculated BIs are decoded to the bit value.
9) Covert messages are obtained by parsing the covert frame.
10) Covert receiver gets the covert messages.

In the covert communication flow, the modified BIs have no affect on legitimate users being provided the Internet services from the AP acting as the covert AP.

Before explaining our proposed covert scheme in detail, we provide Table II that is provided all symbols and notations

TABLE III
COVERT AP ENVIRONMENT SETTING

OS	Linux Ubuntu 18.04
Hardware	Xilinx zynq 7000 zc706
RF Board	Analog Devices AD-FMCOMMS3-EBZ
FPGA compiler	VIVADO 18.3
AP driver	Openwifi

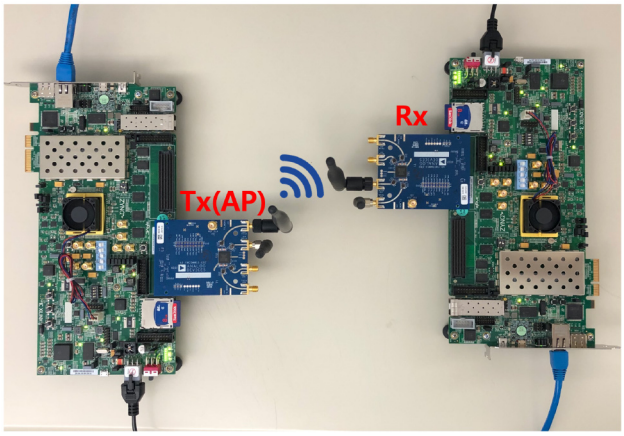

Fig. 6. Zynq board setting as AP and Rx.

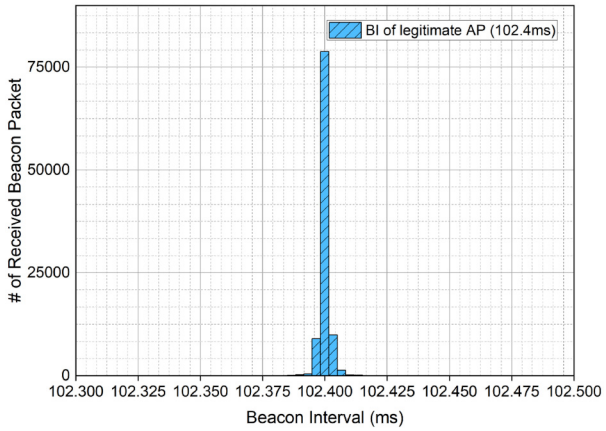

Fig. 7. BI distribution of AP.

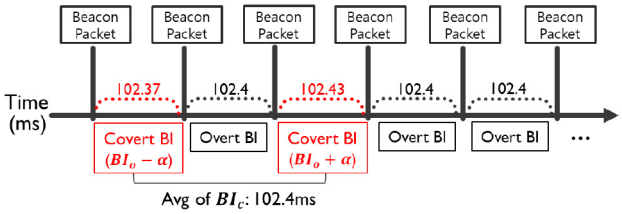

Fig. 8. Complementarity of covert BI. ($\alpha = 30\ \mu$).

used in this section. First of all, we describe the process of implementation for the covert AP to control the sophisticated timing in the following section.

A. Implementation Covert AP

A covert AP is an off-the-shelf-like AP with an additional capability of generating covert signals. Therefore, implementing the covert AP is essential for constructing covert communication. In this section, we introduce how to implement this covert AP. Through our implementation, we can control the sophisticated timing of the BIs. In addition, sophisticated delay can reduce the negative effect to the legitimate uses and increase their covertness. To implement the covert AP, we start with an AP that provides public Internet service using Openwifi [44], an open source that follows 802.11 a/b/n standards, and Xilinx Zynq board, which is an embedded board.

We modified the AP's driver timer to precisely control the BI in microseconds. The existing AP timer uses a Linux kernel timer based on jiffies, and the AP operates in ms. However, we changed the Linux kernel timer to high-resolution kernel timer (hrtimer) [45] to enable control the BI in microseconds. Through the modification of the timer, the covertness of our covert communication is increased and on the other hand, the negative effect on the legitimate users is decreased at the same time. The covert AP uses 802.11a channel 40 of 5-GHz band (center frequency: 5220 MHz, frequency range: 20 MHz).

Table III lists the H/W and S/W specifications used to implement the covert AP. Fig. 6 shows the covert AP test environment using two Zynq boards. The left board is the covert AP, and the right board is the covert receiver.

Typically, the BI of the AP is initially set to 102.4 ms, and the distribution of BIs is as shown in Fig. 7. In Fig. 7, the total number of received beacon packets is 100 000, but the number of BIs of exactly 102.4 ms is less than 70 000 due to subtle deviations in the timing of AP generating beacon packets.

In this distribution, it is investigated that 102.4 ms–15 μs $<$ BI_o $<$ 102.4 ms + 15 μs, and therefore, α is set as 30 μs for BI_c to avoid any overlap with the BI_o in consideration of the distribution range of the BI_o. It is possible because any BI can be controlled in microseconds in our implementation.

In WLAN, beacon packets have a lower priority than data packets as described in Section III-A. This means that if a legitimate user is currently using the Internet and requests data from the AP, the AP may cancel or delay beacon packets for data packets transmission. Ultimately, the low priority of the beacon packet helps adjust the BI to generate BI_c. In our implementation of covert AP, if the BI_c is set to $\mathrm{BI}_o + \alpha$ ($\mathrm{BI}_o - \alpha$, resp.), then the next BI_c is set to $\mathrm{BI}_o - \alpha$ ($\mathrm{BI}_o + \alpha$, resp.) as shown in Fig. 8. As a result, the average of two consecutive BI_cs always equals BI_o.

Therefore, though the covert AP produces BI_os and BI_cs, the average of the overall BIs is always the same as that of BI_o. Fig. 9 shows the distribution of covert AP's BIs. As shown in Fig. 9, it is checked that this covert AP's BI distribution is highly similar to that of legitimate AP in Fig 7, and the distribution of BI_cs appears symmetrically to the left and right of BI_o.

A legitimate user of an AP synchronizes its beacon packet receiving time by the BI field of the beacon packet. Hence, if the BI is different from the value written in the BI field, it may affect not only time synchronization but also Internet use. However, in our implementation, the negative effect of time synchronization on legitimate AP users can be minimized, because BI_cs are the same as BI_o on average.

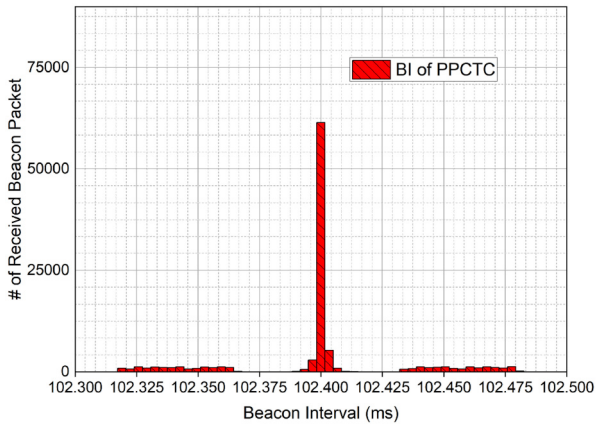

Fig. 9. BI distribution of the covert AP.

B. PPCTC: Ping-Pong Covert Timing Channel

In this section, we describe in detail the proposed PPCTC encoding method and recovery process. Our PPCTC is basically a CTC that uses both BI_o and BI_c, and also a WCC exploiting tiny distortion to the MAC layer protocol of WLAN wireless communication.

First, a receiver can recognize the transmitted covert bits as follows.

1) If a beacon packet is received after BI_o, the receiver regard as transmitted bit is "1."
2) If a beacon packet is received after BI_c, the receiver regard as transmitted bit is "0."

As shown in Fig. 9, since α of BI_c is selected to be larger than the range of distribution of BI_os, the receiver can recognize the transmitted covert bit without any confusion. Now, a transmitted bit "0" meaning BI_c, and the transmitted bit "1" meaning BI_o, are encoded as information bits as follows. The number of repeated transmitted bit "1" means the information bit to be really transmitted, and the transmitted bit "0" is used as a delimiter to divide the number of transmitted bits "1." In this study, we denote the transmitted bit as 1/0 and information bit as $\hat{1}/\hat{0}$. Our PPCTC encoding rules can be summarized as follows.

1) "01111" is transmitted if information bit is $\hat{1}$.
2) "01" is transmitted if information bit is $\hat{0}$.

The overall process of PPCTC is detailed in Algorithm 1.

After encoding, a transmitted bit "0" cannot appear consecutively, and a transmitted bit "1" must always exist before and after a transmitted bit "0." If there are four transmitted bits "1" between transmitted bit "0," it means information bit "$\hat{1}$," and if there is one transmitted bits "1" between transmitted bit "0," it means information bit "$\hat{0}$." The reason why the number of transmitted bits "1" is encoded as four or one to indicate the information bit is related to the recovery of beacon packet loss. Fig. 10 shows the transmitted BI according to the PPCTC algorithm when the information bitstream is "0 × AAAA."

Compared with the information bit, the transmitted bit of the PPCTC algorithm has five times more bit value "1." It means BI_o is more transmitted compared with BI_c. The BI distributions related to covertness are analyzed in Section V.

Algorithm 1 Proposed Encoding Scheme: PPCTC

```
# Notation
D = {d_1, ··· .d_N}: information data set
1̂/0̂: information bit
BI_r: calculated BI for the received beacon packet
p_1,p_2,p_3 : positions of transmitted bit '0' around bit loss

# PPCTC encoding (Covert AP)
arbitrarily select random delay larger than α, j = 1
for i = 1:N do
    if j = 1 then
        BI = BI_c−
        j = 2
    else if j = 2 then
        BI = BI_c+
        j = 1
    end if
    if d_i = 1̂ then
        repeat
            BI = BI_o
        until # of BI_o = 4
    else if d_i = 0̂ then
        BI = BI_o
    end if
end for

# PPCTC Decoding (Covert Receiver)
while beacon packet received do
    BI calculate as BI_r
    if BI_r = BI_o up to margin time then
        decode as transmitted bit '1'
        store the 1 at the Buffer
    else if BI_r > BI_o ×1.5 then
        regard as beacon packet loss occurs
        find p_1,p_2,p_3 (positions of transmitted bit '0')
        call the recovery process
        decode the including repaired bits (LU)
        refers to Algorithm 2
    else if BI_r = BI_c up to margin time then
        consider as transmitted bit '0'
        store the 0 at the Buffer
        count # of 1 between bit 0 and bit 0
        if Buffer stored '011110' then
            information bit = 1̂
        else if Buffer stored '010' then
            information bit = 0̂
        end if
    end if
end while
```

This repeated BI_o occurrence guarantees the recovery of bit errors by beacon packet loss, though it lowers the data rate.

A good channel in a wireless communication environment means that there is no packet loss, and the receiver does not need to consider recovery. However, in a real environment, noise or packet loss cannot be avoided because various wireless devices and APs exist nearby.

The receiver of the covert AP cannot send acknowledge (ACK)/negative ACK (NAK) or a retransmission request to the covert AP for the lost packet by the unidirectional property of the PPCTC. Thus, error recovery capacity is required for the receiver to overcome the loss of beacon packets and successfully receive covert data in a wireless unidirectional communication environment.

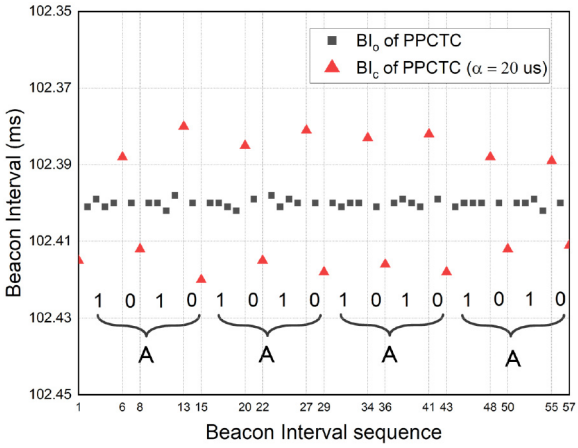

Fig. 10. Practical BIs of the PPCTC for the information "0 × AAAA" in terms of time flow.

As mentioned above, beacon packet loss leads to the loss of two transmitted covert bits. To know the value of the transmitted covert bit, PPCTC calculates BI, which is the time interval between the currently received beacon packet and the immediately preceding beacon packet. However, if the current beacon packet is lost, the receiver cannot check the time interval between previous and current packet (and current and next packet, respectively), and so two consecutive BIs are lost. We use L and U to indicate these lost consecutive bits corresponding to the lost BIs. The following notations are introduced for our recovery process.

1) *L:* It means a lost bit value by lost current BI.
2) *U:* is an unknown bit value corresponding to the next BI which cannot calculate due to the lost current BI. L and U always exist in pairs like "LU."
3) *(p_1, p_2, p_3):* p_1 and p_2 are the positions of the first and second 0-bit from the left among the 4 bits before L, respectively. And, p_3 is the position of the first 0-bit from the left among the 4 bits after U. For example, for a given $\cdots 1101LU10, \cdots$, $(p_1, p_2, p_3) = (3, 0, 2)$. It is evident that $(p_1, p_2) = (0, 0)$ if $p_1 = 0$, and $(p_1, p_2) \neq (x, y)$ for $1 \leq x \leq 4$, $1 \leq y \leq x$. Since consecutive zeros do not occur in our encoding rules, (p_1, p_2) cannot be $(x, x+1)$ for $1 \leq x \leq 3$.

We assume that beacon packet loss occurs during the reception. Now, the recovery procedure is as follows.

1) *Case 1:* $(p_1, p_2) = (0, 0)$. Then, the received bits are $\cdots 1111LU \cdots$ Therefore, LU must be 01 by our encoding rules.
2) *Case 2:* $(p_1, p_2) = (1, 0)$. It means that the received bits are $\cdots 0111LU \cdots$ Hence, LU must be 10 by our encoding rules.
3) *Case 3:* $(p_1, p_2) = (2, 0)$. Then, the received bits are $\cdots 1011LU \cdots$, so LU must be 11.
4) *Case 4:* p_1 or p_2 is equal to 3. Then, the received bits are $\cdots 01LU \cdots$ In this case, the possibility of p_3 is 2 or 4, by our encoding rules. If $p_3 = 2$, then LU is determined by 11, since the received bits are $\cdots 01LU10 \cdots$ When $p_3 = 4$, it is evident that LU is 01, since the received bits are $\cdots 01LU1110 \cdots$

Algorithm 2 Recovery Process of the PPCTC

Input ← $(\mathbf{p_1}, \mathbf{p_2}, \mathbf{p_3})$
Output ← **LU**
while input date received **do**
  if (p_1, p_2) is $(0, 0)$ **then**
    LU is 01
    break
  else if (p_1, p_2) **is** $(1, 0)$ **then**
    LU is 10
    break
  else if (p_1, p_2) **is** $(2, 0)$ **then**
    LU is 11
    break
  else if p_1 *or* p_2 **is** 3 **then**
    if p_3 **is** 2 **then**
      LU is 11
      break
    else if p_3 **is** 4 **then**
      LU is 01
      break
    end if
  else if p_1 *or* p_2 **is** 4 **then**
    if p_3 **is** 2 **then**
      LU is 10
      break
    else if p_3 **is** 3 **then**
      LU is 11
      break
    end if
  end if
end while

5) *Case 5:* p_1 or p_2 is equal to 4. It means that there is a zero just before L and so $L = 1$. According to our encoding rules, p_3 must be 2 or 3. If $p_3 = 2$, then U must be 0 since the received bits are $\cdots 01U10 \cdots$, and when $p_3 = 3$, the received bits are $\cdots 01U110 \cdots$ Therefore, U should be 1.

The detailed algorithm for this recovery process is described in Algorithm 2.

In addition, when two beacon packet losses occur consecutively, if the receiver knows a bit value of a sufficient length before and after the beacon packet loss, then the receiver can recover the loss of three transmitted bits according to the encoding rule. Here, a bit value of sufficient length means more than 3 bits before and after BI loss each. However, in this study, we do not cover the three-bit recovery processes.

C. Covert Frame

In this section, we present the covert frame, considering the confidentiality and integrity aspects of the PPCTC. The PPCTC was designed with a focus on complementarity and recovery. However, all WCC methods as well as the PPCTC always have a problem of exposing data to unintended receivers or attackers. There is a possibility that the confidentiality of the covert channel is broken immediately upon exposure and the data can be decoded. To overcome this problem, we propose a covert frame applicable to the PPCTC. The purpose of the covert frame is to prevent data leakage to an attacker by encrypting the data, and to provide integrity so that only the promised covert channel receiver can decode the

covert data without error. We describe the way of constructing the covert frame that provides confidentiality and integrity.

1) Hash-Based XOR *Cipher:* Even using the covert channel, sending data in a plain text has a risk of data leakage. In this study, XOR cipher is used for transmitted data to prevent data exposure. The XOR cipher is a simple encryption technique that exploits exclusive OR calculation for the key and data. The XOR cipher was used to minimize the delay that occurs during cryptographic operations in a delay-sensitive CTC environment, and the hash value of SHA-1 was used as a key to compensate for the weakness of the XOR cipher.

We designed the XOR cipher key to have three characteristics. First, because the reuse of the key increases the probability of exposing the key, and the entire data can be leaked, the hash value is dynamically changed whenever a covert frame is created. Second, since a preshared key (PSK) is used as a part of the SHA-1 input values; attackers cannot create the same XOR key even if they know the key generation algorithm. Finally, the XOR key was used to verify the integrity of the covert frame as well as the encryption. Therefore, a part of the hash value, which is the key of XOR, is used as the integrity check field of the covert frame. The next section describes how to calculate the SHA-1 hash value and the process of applying the SHA-1 hash value as an XOR encryption key.

2) SHA-1 Hash Value for Integrity Verification and XOR *Cipher Key:* This section describes the components of input data for SHA-1 and how the hash value of SHA-1 is used as an XOR cipher key. The input data of SHA-1 is composed of the SFD field, the nonce field of the covert frame, and the PSK promised in advance by the PPCTC transceiver. The SFD field and PSK are fixed values, and the nonce field is a value that varies for each frame generation. Because of the nonce field, the hash value is different each time a frame is created. Furthermore, the PSK is shared differently depending on the receiver group, so that the covert AP can select the receiver group to which the data is sent. More details of the covert frame field will be covered in the next session. The output of SHA-1 always has a length of 20-bytes hash values regardless of the length of the input. Of the 20-byte hash value, the upper 2 bytes are used for integrity, and the remaining 18 bytes are used for the XOR cipher.

In 802.11 WLAN, AES is usually used for encryption, but AES requires larger computing power compared to SHA-1, and the hardware performance of the AP causes an additional delay in the frame creation process. Because the PPCTC is designed as a practical CTC that uses only a delay of several tens of μs, it is necessary to minimize the delay that occurs during the encryption process. For this reason, SHA-1 and XOR cipher, which require relatively small computational power, are used to provide integrity and confidentiality.

3) Covert Frame Structure: Since PPCTC is unidirectional communication, the receiver cannot send ACK/NACK to the sender. Thus, it is important to send data to the receiver as reliably and robustly as possible. As mentioned in Section III-B, we designed the covert frame structure to be similar to the existing communication frame structure. A frame is largely composed of three parts: 1) synchronization; 2) integrity; and 3) encrypted data. It has reliability even in broadcast transmission without ACK/NACK protocol. As shown in Fig. 11, the covert frame consists of eight fields. In Fig. 11, the function of the field is divided into three types with different colors. A gray field (Preamble) indicates synchronization, a yellow field (SFD, Nonce, and covert SFD) indicates integrity, and a black field [header, payload, and cyclic redundancy check (CRC)] indicates confidentiality using encryption.

Fig. 11. Covert frame.

The details of the covert frame field are listed as follows:

1) *Preamble:* The preamble field does not contain data and only repeatedly transmits the BI_o. In this study, we set to repeat 16 times the BI_o (transmitted bit "1") into the preamble field. When the receiver starts receiving in the middle of a transmission, it waits only for the preamble until the preamble is completely received.
2) *SFD:* The SFD field indicates that a frame starts. In this study, we set it as 0xA5. SFD is also used as input data for SHA-1 hash and the length of the SFD is 1 byte.
3) *Nonce:* The nonce field is used as the input data of the SHA-1 hash and is 2-bytes long.
4) *Covert SFD:* The Covert SFD field is the integrity check field of a covert frame. Covert SFD uses the upper 2-bytes of the SHA-1 hash.
5) *Header:* The header field contains a sequence number and data length information and is encrypted. The upper 3 bits are used as bits for the sequence number and indicate the number of repetitions. The sequence number indicates the number of repeated transmissions of the frame and is decremented by 1 for each transmission. When it becomes 0, it resets to the first set sequence number and sends the next frame. The lower 5 bits indicate the length of data including payload and CRC. The length of the header field is 1 byte.
6) *Payload:* The payload field contains information and is encrypted. The length of the payload is 1 to 16 bytes and the maximum amount of transmission per covert frame is 16 bytes.
7) *CRC:* The CRC field confirms the errors for the received data, and was encrypted. The length of CTC is 1 byte.
8) *End of Frame (EOF):* The EOF field indicates the end of a frame. In this study, it was set to 0x5A.

Fig. 12 specifically shows how the hash value is used in the covert frame for integrity and encryption. The Covert SFD field uses the upper 2 bytes of the hash value of SHA-1 for integrity. Here, the input data of SHA-1 is *SFD||NONCE||PSK*. The lower 18 bytes of the hash value for encryption are sequentially XORed with the header, payload, and CRC fields. Here, the maximum payload size is 16 bytes.

At the receiver end, if the received value matches the preamble, they store the SFD and NONCE. Subsequently, they take the form of *SFD||NONCE||PSK* as input data. The SHA1 results are then calculated using the input data.

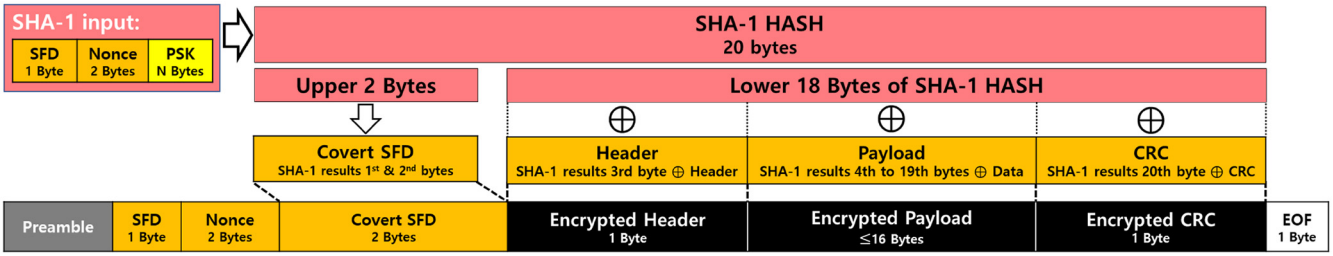

Fig. 12. SHA-1 hash used covert SFD and XOR cipher KEY.

TABLE IV
ACHIEVING REQUIREMENT OF COVERT COMMUNICATION

Environment	CTC Scheme	Covertness			Robustness		Transparency	Concealment	Throughput (bit/s)
		$^{**}J$	$^{\dagger}\epsilon$	$^{\ddagger}K$	Recovery	BER (%)			
IEEE 802.11	On-offCTC [9]	0.3333	39.92 %	-	-	-	-	-	6.55 bps
	Binary [18]	0.3333	-	-	-	-	-	-	9.77 bps
	DPOI [8]	0.4999	-	-	-	-	-	-	6.55 bps
	Our PPCTC	0.5549	97.07 %	0	two bit	0.01 - 0.76 %	◯	◯	2.79 bps
	*SFO [17]	-	-	-	-	2.19 - 2.45 %	-	-	9.76 bps
* LTE	SPCC [16]	-	-	-	-	0.01 - 1 %	-	-	0.8 - 3 bps
	NoP-GCTC [15]	-	-	0.01 - 0.1	-	0.1 - 1 %	-	-	1 - 8 bps
	VRCTC [14]	-	-	0.01 - 0.1	-	0.1 - 1 %	-	-	10 - 85 bps
	RPDCTC [13]	-	-	-	-	0.01 - 1 %	-	-	1 - 2 bps
	MSVCTC [12]	-	-	0	error correction	0.001 - 0.85 %	-	◯	0.05 - 0.49 bps
	ZMCTC [11]	-	-	0	-	1.5 %	-	-	0.27 - 2.73 bps

*The results of [11]–[17] referred to the mentioned in their paper.
*The results of LTE environment CTCs are provided informatively to compare with IEEE 802.11 environment.
** J: Jaccard Similarity, $^{\dagger}\epsilon$: ϵ-similarity ($\epsilon \leq 0.005$), $^{\ddagger}K$: Kullback–Leibler divergence

V. EXPERIMENTAL EVALUATIONS

In this section, we describe the experimental results and verify whether our proposed scheme is achieved or not for the four types of requirements through comparison to other covert communication schemes. In Table IV, we summarized whether the requirements are satisfied according to each CTC scheme. First, we analyze the covertness of the PPCTC with respect to its three aspects: 1) BI distribution; 2) the relative difference between the delay sizes of covert bits; and 3) the difference in distribution between legitimate BI and PPCTC. Second, robustness represents how we can have reliable communication in wireless covert unidirectional communication. Third, transparency means how little the effect is on legitimate users when covert data is transmitted. Finally, concealment indicates the difficulty in decoding the covert data, even if the covert signal is detected. In the case of concealment, it is considered only our proposed schemes. This is because we designed it for a practical covert communication environment. To achieve the concealment of our covert communication, we proposed the covert frame, which encrypts the data using SHA-1 and XOR cipher. Even though a simple encryption method, the covert data can be protected from the adversary warden.

Before performing the verification for the requirements in more detail, we compare the BI distribution and delay size of the PPCTC and conventional CTC algorithms in the practical IEE 802.11 environment using covert AP. This is because, in the CTC, the distribution of time intervals and the size of delay are closely related to covertness. Here, covertness indicates the similarity between the signal of the covert channel and the legitimate signal. That is, high covertness means it is difficult to distinguish between a covert signal and a legitimate signal.

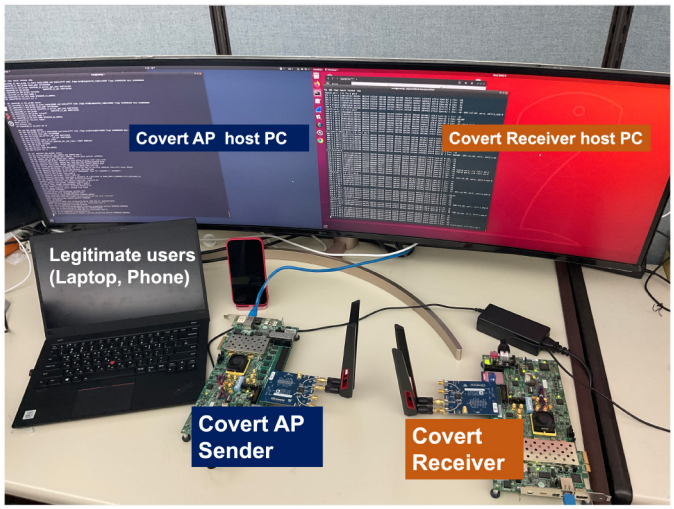

Fig. 13. PPCTC test environment.

If periodic signals lose periodicity or legitimate signals appear in a specific pattern, the adversary warden may suspect a covert channel. In addition, if the delay of a legitimate signal becomes large enough to affect the general user's communication, there is also a risk that the covert channel will be caught. The size of delay is related to covertness as well as transparency.

A. Experimental Testbed

Fig. 13 shows the PPCTC testbed for evaluation. The Zynq boards are used as covert AP and covert receiver and a

laptop that has a wireless LAN card is a covert receiver in this experimental environment. One laptop and one smartphone are prepared as legitimate users to evaluate the practical environment.

We applied several CTC algorithms as a benchmark to the covert AP environment and analyzed in terms of delay applied to BI_o. In general, since BI_o is set to 102.4 ms, we set it to 102.4 ms in our experiment. The benchmark schemes which are to compared with our PPCTC are as follows.

On–OffCTC [9]: On–offCTC sends covert data by skipping sending BI_o. When this method is applied to our experiment, BI_o represents the information bit value "$\hat{1}$" and skipped BI_o represents the information bit value "$\hat{0}$." Thus, the BI_c is double the BI_o and the information bit value "$\hat{0}$." In terms of beacon packets, covert data is transmitted while intentionally causing packet loss.

Binary [18]: Walker and Fairbanks proposed a CTC with a delay time of 5-ms unit in BI_o. To compare with our PPCTC, we modified the delay size to 50 μs and called it Binary. This is because we used the fixed delay to divide information bit value "$\hat{1}$" and "$\hat{0}$."

DPOI [8]: The DPOI was modified on the On–offCTC to have smaller BI_c instead of BI_o skip. As same as On–offCTC, BI_o of DPOI represents the information bit "$\hat{1}$". However, the difference is that the information bit "$\hat{0}$" is represented as an BI_o following BI_c.

Through the implementation of covert AP, we can be controlled by the tens of μs units for the IPD. As a result, we changed the delay size to tens of μs units for each comparison between CTC schemes, and we performed the comparison. Fig. 14 illustrates the BI distribution of CTCs. We set the same size of delay as 40 μs for the binary and DPOI. On–offCTC is set to 204.8 ms for BI_c, and BI_c of our PPCTC is 35 to 45 μs. Each CTC sends information bit "0 × AAAA" repeatedly, and the total number of transmitted beacon packets is 6000. We can see from Fig. 14 that our PPCTC has the most obvious BI, which is what we wanted. Furthermore, our PPCTC has the smallest covet BI bar.

Unlike other CTC methods, our PPCTC can control the peak value of each BI_c bar by adjusting the range of the BI_c. Fig. 15 shows the change of the BI_c peak value according to the covert range. Fig. 15 shows the histogram of the PPCTC BI distribution according to the BI_c range. First, the BI_c range has no effect on BI_o. However, a narrower range of the BI_c leads to a higher BI_c bar, which indicates a higher probability of detecting the BI_c. Thus, it shows the importance of properly controlling the scope of BI_c.

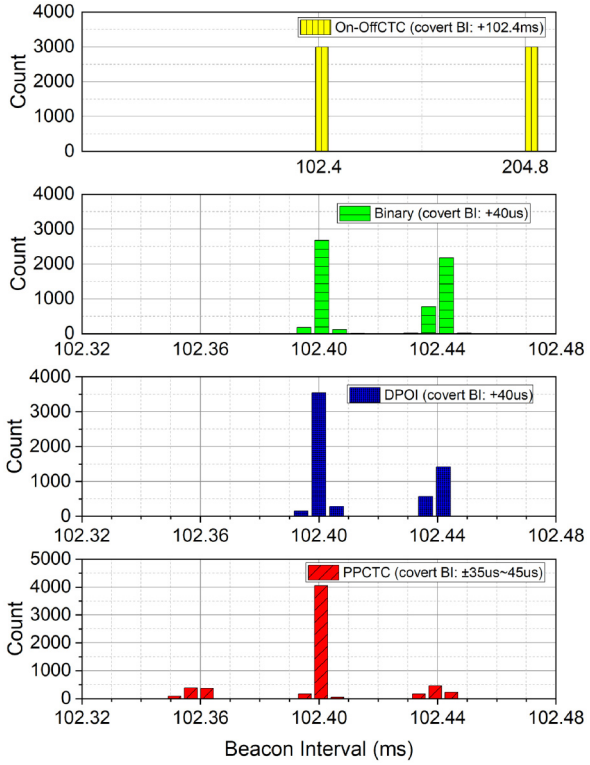

Fig. 14. BI distribution for multiple CTCs in a WLAN environment.

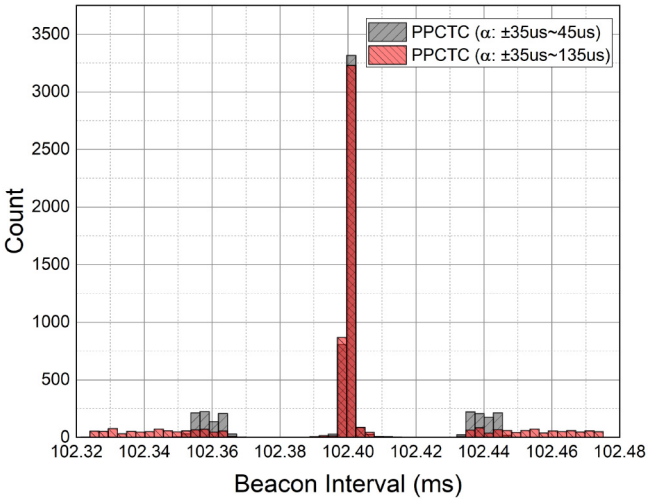

Fig. 15. PPCTC: overall BI distribution according to the BI_c range.

TABLE V
BI_o RATIO OF CTC

CTC Algorithm	avg.	Min.	Max.
On-offCTC [9]	50%	50%	100%
Binary [18]	50%	50%	100%
DPOI [8]	66.66%	50%	100%
Our PPCTC	71.38%	50%	80%

B. Analysis Results

1) Covertness: In this section, we analyze the covertness for various CTCs focused on the WLAN environment. First, Table V lists the ratio of BI_o in covert communication for each CTC on the WLAN environment.

Table V shows our PPCTC guarantees the BI_o of at least 50%, and the maximum ratio is 80%. However, other schemes are shown to have 50% and 80% each for the Min and Max ratios. The reason for the Max ratio of PPCTC being lower than others in our proposed encoding schemes include a repetition mechanism. The percentage of BI_o for the PPCTC depends on the information bit. If the number of information bit value "$\hat{1}$" increases, the ratio of BI_o will increase. However, it is very difficult to maintain a 100% BI_o ratio because there

TABLE VI
JACCARD SIMILARITY

CTC Algorithm	Jaccard similarity.
On-offCTC [9]	0.3333
Binary [18]	0.3333
DPOI [8]	0.4999
Our PPCTC	0.5549

TABLE VII
ϵ-SIMILARITY COMPARED WITH CONVENTION SCHEME

	ϵ-similarity.			
CTC Algorithm	0.005	0.01	0.03	0.1
On-offCTC [9]	39.92	58.58	79.74	91.85
Our PPCTC	97.07	97.07	97.07	97.07

are a few cases where only information bit value "$\hat{1}$" is sent. Consequently, the average BI_o represents the general BI_o ratio in covert communication, and our PPCTC has the highest BI_o ratio on average compared to the other algorithms. To evaluate the covertness, we calculate the similarity using the average ratio of BI_o in Table V.

To analyze the covertness of our PPCTC, we measure the following three metrics.

1) Jaccard similarity [46].
2) ϵ-similarity [9].
3) Kullback–Leibler divergence (K–L divergence) [47].

Jaccard Similarity: The Jaccard similarity shows how much BI_o is occupied in covert communication. In other words, it shows the similarity in terms of the BI distribution. If the BI_o ratio is 100% in the covert communication, the Jaccard similarity value is 1. The equation of the Jaccard index is as follows:

$$(\mathrm{BI}_o, \mathrm{BI}_c) = \left(\frac{\mathrm{BI}_o \cap \mathrm{BI}_c}{\mathrm{BI}_o \cup BI_C}\right) \tag{1}$$

where BI_o denotes the distribution of legitimate AP's BI (BI_o) and BI_c represents BI distribution of covert AP.

Here, we used the average ratio value in Table VI for calculating the Jaccard index, and Table VI represents the Jaccard similarity for the CTCs on WLAN. Our PPCTC has a 0.5549 Jaccard index which shows the highest index among the comparatives. Consequently, in terms of BI_o distributions, our PPCTC has the best covertness.

ϵ-Similarity: ϵ-similarity is the ratio of covert bit signals in which the different values with the size of the previous signal are less than ϵ for a given ϵ, when the given covert bit signals are arranged in the order of the size of the BI interval. Therefore, if for a given small ϵ, ϵ-similarity is close to 100%, then we can conclude that it is difficult to detect these covert signals. Table VII shows the percentage of ϵ-similarity for different ϵ values. As shown in Table VII, our PPCTC has a 97.07% for every ϵ unlike On–offCTC. In other words, Table VII shows that through implementation, we can control the sophisticated timing for the BIs, Consequently, our PPCTC achieves the higher covertness.

Table VIII shows the ϵ-similarity according to our PPCTC delay size. To compute ϵ-similarity, we received 6000 beacon packets for each delay size. ϵ-similarity of our PPCTC remains high at 97.07 for ϵ is 0.001 and delay size, 35 μs.

TABLE VIII
ϵ-SIMILARITY OF THE PPCTC ACCORDING TO THE DELAY SIZE

PPCTC	ϵ-similarity.				
Delay size	0.0001	0.0004	0.001	0.01	0.1
$10ms$	69.57	69.78	69.80	69.80	97.57
$1ms$	70.12	70.33	70.33	98.32	98.32
$100\mu s$	69.50	69.62	76.80	97.42	97.42
$35\mu s$	69.40	83.53	97.07	97.07	97.07

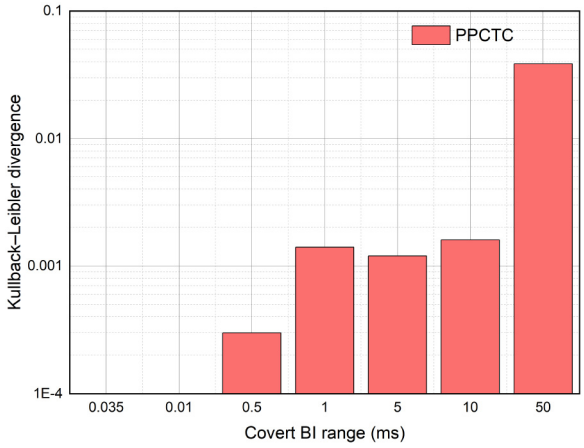

Fig. 16. K–L divergence for PPCTC.

Even when ϵ is extremely small at 0.0001, it can be seen that the ϵ-similarity is maintained somewhat high at 69.4. However, for $\epsilon = 0.1$, the ϵ-similarity of 100% is not achieved. This means that 2.03% packet loss still occurs. Nevertheless, the results of Table VIII show the capability, which can control a smaller delay size in tens of microseconds, leads to high ϵ-similarity for the smaller ϵ.

K–L Divergence: We calculate K–L divergence [47] for the PPCTC to evaluate the undetectability according to the delay size. A number of wireless CTCs have recently been using K–L divergence to verify the undetectability of their CTC [11], [12], [14], [15], [16]. The K–L divergence is a method for quantitatively measuring the difference between two probability distributions that are legitimate AP's BI and Covert AP's BI. If K–L divergence has a low value, then the cross-entropy of the distribution Covert AP's BI based on that of legitimate AP's BI is almost the same as the information entropy of the distribution of legitimate AP's BI. Therefore, it is difficult to distinguish the distributions of legitimate AP's BI and Covert AP's BI. Fig. 16 shows the result of the K–L divergence according to the different delay sizes of BI_c. When the BI_c range is smaller than 0.01 ms, the K–L divergence is 0 which means if the 35 μs of BI_c, the detection rate is 0. Consequently, the delay size is deeply related to the undetectability of the CTC method.

2) Robustness: Through practical experiments, we show the robustness of our proposed covert communication. Robustness in this context refers to "how much reliable communication is possible when bit error occurs in covert unidirectional communication." Thus, we regard the decoding success rate as robustness in the covert recipient aspect.

TABLE IX
DECODING RATE

Case	# of Covert frame	Error (%)	Recovery (%)	Success (%)
Case 1	195	27.18%	8.2%	81.02%
Case 2	195	76.93%	33.85%	56.92%

The results of practical experiments for our entire covert communication scheme, which is PPCTC with the covert frame, show the reliability depends on with or without the recovery process. In other words, the decoding success rate is deeply related to the recovery process. To compare the robustness of our proposed scheme, we composed the two cases in the real environment. Case 1 is that the beacon packets are rarely skipped. Case 2 is a more realistic case where the beacon packets loss occurs frequently. Table IX shows the results of the covert recipient decoding success rate for the covert data in the two cases.

1) *Case 1:* When the covert AP is idle.
2) *Case 2:* When devices connected to the covert AP actively use the Internet streaming services.

To build case 1, the covert AP only transmits the covert data using a beacon packet without any Internet service provided. In other words, the state of covert AP is idle. To experiment with case 2, we used one smartphone and one laptop as legitimate users. Two devices are connected to the covert AP, and they were watched by a live video streaming service to make the covert AP busy. At the same time, the covert recipient received covert data from the covert AP through BI. Table IX represents the results of the covert recipient decoding success rate for the proposed covert unidirectional communication environment from the two cases.

The covert AP transmits 195 covert frames. Here, one transmitted covert frame is about 25-bytes long, which means that the covert AP has to transmit approximately 700 BIs per 1 covert frame. Thus, to successfully receive the covert data without error, the channel must be very good or the recovery process is needed in the unidirectional communication environment. Once, case 1 has a lower error rate than case 2 due to good channel conditions (covert AP state is idle). Thus, the recovery ratio is only 8.2% and the recipient can decode about 81% of the entire covert frame in case 1. But, in case 2, the error rate is over 76% for the entire covert frame. This means if covert AP is busy, the beacon packets are skipped frequently and the recipient finds it difficult to receive the covert frame successfully. However, Table IX shows a 56.92% success rate for case 2. This numerical value represents our PPCTC recovery process increasing the success rate twice compared to the absence of recovery. Thus, the results show that the worse the channel environment in unidirectional communication is, the more important our recovery process is for reliable communication.

Table X shows the BER of PPCTC according to the various BI_c ranges. Here, the bit represents the transmission bit and the transmit bit rate is approximately 9.7 bps. The maximum BER is about 0.76% at 50 ms. In other words, the covert AP maintains a low BER regardless of the BI_c range. Further, through the recovery process, the BER decreased by about 50% from the original BER. This is because the recovery process is activated immediately when the transmission bits are received.

TABLE X
BER OF PPCTC ACCORDING TO THE BI_c RANGE

BI_c range	Received bit	BER (%)	BER after recovery (%)
35 μs	15175	0.11 %	0.07 %
100 μs	15673	0.05 %	0.01 %
0.5 ms	15049	0.15 %	0.07 %
1 ms	15446	0.72 %	0.3%
5 ms	15356	0.41 %	0.23%
10 ms	15479	0.19 %	0.06%
50 ms	14959	2.4 %	0.76%

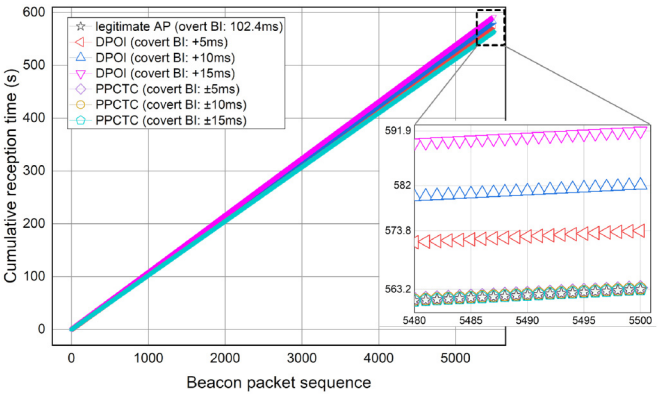

Fig. 17. Timing gap for synchronization according to the accumulated delay.

3) Transparency: When using BI as the covert communication medium, to reduce the effect of the covert communication on legitimate users, BI_c has to follow the legitimate BI continuously. In other words, BI_c always has to follow the average and accumulated time of BI_o. In Fig. 17, we plot the accumulated delay for the DPOI algorithm and our PPCTC. In terms of BI_o distribution, the DPIO has the most BI_os among comparative schemes. The accumulated plot represents how different from the timeline of legitimate AP's accumulated BIs it is in terms of synchronization. As we mentioned previously in Section III, the role of the beacon packet is to provide synchronization to legitimate users for smooth communication. Thus, if the additional covert delay does not have complementary features, then accumulated delay times lead to a disconnect between legitimate users and the AP. This is because covert communication starts generation beacon packets at the same time, but the gap of accumulated time is increasingly far from the legitimate AP's BI timeline. For this reason, the accumulated BI_cs have to follow the BI_os. We compared the cumulative reception time of 5500 beacon packets for dpoi and PPCTC algorithms when the delay size is 5%, 10%, and 15% of BI_o.

DPOI shows that the graph of BI_o gradually spreads in proportion to the size of the delay. Thus, the beacon packet of the last received DPOI differs from the beacon of the legitimate AP by more than 10 ms. This is because the BI_c of the DPOI has no complementarity and accumulates delays according to transmission bits. In contrast, our PPCTC method follows the reception time of the BI_o regardless of the delay size because

TABLE XI
THROUGHPUT COMPARISON FOR THE PPCTC AND WIRELESS CTCS

Scheme	Throughput	BER	CTC media
our PPCTC	2.79 bps	0.07 %	Beacon interval
SFO [17]	9.76 bps	2.19 - 2.45 %	# of IEEE 802.11 stations
SPCC [16]	3 bps	0.9 %	SID frame
NoP-GCTC [15]	8 bps	0.1 - 1 %	# of packets between RTCP
VRCTC [14]	10 - 85.6 bps	0.1 - 1 %	RTP packet
RPDCTC [13]	1 - 2 bps	0.01 - 1 %	video packet drop
MSVCTC [12]	0.49 bps	0.08 %	RTP packet
ZMCTC [11]	0.88 bps	1.5 %	any packet of VoLTE

the BI_c has complementarity. Therefore, it is shown that the CTC algorithm should be designed considering functions such as synchronization for the covert AP to transmit with minimal impact to legitimate users.

Another aspect of transparency is maintaining the connection between covert AP and legitimate users. Through the experiment of Section V-B2, we could show transparency in terms of legitimate users. While the covert recipient received 195 covert frames, two legitimate devices (one smartphone and one laptop) were never disconnected and provided video streaming services from covert AP. Our PPCTC has a complementary feature and does not disturb legitimate users' Internet services.

4) Transmission Performance: In this section, we compares the throughput with other WCC schemes on 802.11 WLAN, and LTE environment, such as SFO [17], SPCC [16], NoP-GCTC [15], RPDCTC [13], VRCTC [14], MSVCTC [12], and ZMCTC [11]. The throughput represents the data transmission of a given CTC.

Typically, the large throughput represents better transmission efficiency in terms of data transmission. The throughput of the PPCTC is calculated as follows:

$$\text{throughput} = \text{capacity} * 9.77\text{bps} \tag{2}$$

where 9.77 is the transmission rate when using a beacon packet as the transmission media. Since the capacity of our PPCTC is 0.286 (see Appendix in detail), the throughput of our PPCTC is 2.79 bps with 0.07% in terms of BER at 35 μs. Table XI shows the throughput for our PPCTC and wireless CTCs regardless of the communication environment. The throughput of PPCTC is fixed regardless of the BI_c range if beacon packets are used as the transmission media. This is because the capacity of PPCTC is 0.286 and the transmission rate is always 9.77 bps by IEEE 802.11 specification.

We address the throughput and BER for various WCCs including our PPCTC in Table XI. Though most WCCs of Table XI are LTE-based CTCs, all throughput results except for three show that WCC schemes have similar performance compared to our PPCTC. This is because, in an LTE environment, the changeable parameters are strongly limited to constructing covert channels, and the covert channels have to achieve covertness, robustness, and transmission performance at the same time.

The throughput of SFO is much higher than ours, since SFO is used, as covert signals, sending orders for the multiple senders between beacon packets. For a fair comparison, in Table XI, we compared the throughput with our PPCTC when assuming the capacity of SFO is 1, that is, two stations are involved to send covert signals.

NoP-GCTC also shows higher performance than our PPCTC. This is because they used the number of packets (NOPs) between RTCP packets, here the NoP is hundreds of packets. Through modulation which is a variable length of code length, they can get a higher throughput than ours. And furthermore, unlike other CTCs, VRCTC shows the highest throughput. The reason is that VRCTC used data packets for CTC construction which is advantageous in transmission speed.

VI. DISCUSSION

When we designed the PPCTC, we considered two situations that occur during constructing CTC and sending covert data through 802.11 AP. One is that covert messages should be preserved in confidential status even though the covertness is broken, and the other is how to handle the packet loss in unidirectional communication. Therefore, we proposed and implemented our PPCTC with the following design approaches.

1) We focused on the method for concealment in terms of covert data even though the covertness of the covert channel is broken. To overcome broken covertness, we proposed a covert frame to protect the covert data. The cover frame prevents data exposure through key sharing.
2) In unidirectional communication, the receiver can not send the ACK/NACK. Thus, when we design an encoding scheme we consider the self-recovery method without ACK/NACK.

However, our PPCTC has the potential threat that the covertness might be broken by some pattern of time intervals, and even though the covert frame provides confidentiality for the covert data, our PPCTC cannot permit long messages as the payload field of the covert frame, and therefore the high transmission performance cannot be achieved.

To improve in terms of the above constraints, the time interval patterns have to be more complicated to make it hard to detect, and the covert frame structure has to be more improved focusing on the payload field to achieve better transmission performances.

The covert communication is an offensive technology. Therefore, mechanisms to detect and prevent the presence of the covert communication channel are the main countermeasures, which may be open challenges for our PPCTC as well.

VII. CONCLUSION

In this study, we establish a covert wireless unidirectional communication mechanism. Our mechanism is composed of three parts. First, we implement a covert AP that can generate covert signals based on time interval differences. Second, the PPCTC, which is a CTC encoding scheme, is proposed. Finally, we present the covert frame to provide confidentiality and integrity in terms of covert data. In terms of covertness, our PPCTC shows the highest Jaccard similarity 0.55 which is related to the BI distribution. Further, ϵ-similarity

of the PPCTC, which is related to intentional delay size, preserves more than 97% for $0.001 \leq \epsilon \leq 0.1$. In addition, we proved that it is difficult to distinguish between the probability distributions of BI for our covert AP and legitimate AP by measuring K–L divergence. In terms of robustness, when covert AP is busy such as it provides Internet service to legitimate devices, our PPCTC recovered 33.85% for the total frame. In the transparency aspect, our PPCTC encoding always follows the BI_o. Finally, using SHA-1 and XOR cipher, we achieved the concealment for the information transmitted through the PPCTC. Furthermore, when the BI_c is set as 35 μs, our PPCTC exhibits 2.79 bps and 0.07% in terms of throughput and bit error rate, respectively.

For further study, we will try to design a covert channel using periodic signals such as the PPCTC in various communication environments and implement it in the real environment. Furthermore, finding and designing some detection systems of covert channels including the PPCTC system, can be a good research subject. It is because the covert channel can be exploited by a malicious user.

APPENDIX
CAPACITY OF PPCTC

We calculate the capacity of our PPCTC as two parts, one is code rate another is throughput in terms of communication.

Code Rate: The PPCTC algorithm has different transmitted bit lengths according to information bits. For example, the information bit value of "$\hat{1}$" is encoded as five transmitted bits ("01111"), and the information bit value of "$\hat{0}$" is encoded as two transmitted bits ("01"). The coding rate of the PPCTC according to the information bit lengths, for example one bit, two bits, and three bits, is calculated as follows:

$$\text{one}-\text{bit} = \frac{1}{2}\left(\frac{1}{5}+\frac{1}{2}\right) = 0.35$$

$$\text{two}-\text{bit} = \frac{1}{4}\left(\frac{2}{10}+\frac{2}{7}+\frac{2}{7}+\frac{2}{4}\right) = 0.318$$

$$\text{three}-\text{bit} = \frac{1}{8}\left(\frac{9}{15}+\frac{3}{12}+\frac{3}{12}+\frac{3}{12}+\frac{3}{12}+\frac{3}{9}+\frac{3}{9}+\frac{3}{6}\right) = 0.306.$$

The coding rate of the PPCTC algorithm according to the information bit length follows in (3).

Consequently

$$\lim_{n\to\infty}\frac{1}{2^n}\left(\sum_{k=0}^{n}\frac{\binom{n}{k}\times n}{5k+2(n-k)}\right) \tag{3}$$

where n denotes the length of the actual data bit, and k is the number of 1 bit in the n.

Throughput: The throughput is calculated as the code rate multiplied by the transmission rate. Here, the transmission rate means the number of transmitted bits per second, and the transmission rate of the BI is calculated as 1/BI. In this study, the overt BI is set to 102.4 ms. Thus, the transmission rate is almost 9.766 bps. That is, when the coding rate is 1, the data rate of BI is 9.766 bps. However, the code rate of our PPCTC is less than 0.3 and the average throughput of PPCTC is calculated as follows:

$$\frac{1}{\text{BI}_o}\times\lim_{n\to\infty}\frac{1}{2^n}\left(\sum_{k=0}^{n}\frac{\binom{n}{k}\times n}{5k+2(n-k)}\right)\text{bps} \tag{4}$$

where BI_o denoted the overt BI.

Because transmit seven bits contain two information bits "10," the arithmetic code rate of our PPCTC is 0.286. In this way, the arithmetic code rates of other CTCs are 1(Binary), 0.67(On–offCTC, DPOI).

The throughput depends on the encoding scheme. Table XII compares the throughput of PPCTC with those of the binary encoding schemes. The binary encoding throughput is always 9.77 bps. The covert rate of binary encoding is 1. However, the throughput of the PPCTC affects the content of actual data because the PPCTC has a different encoding length to bit "1" and "0." The average throughput of PPCTC is approximately 2.79 bps owing to the effect of repeated transmission. The PPCTC seems to have low throughput. However, the PPCTC scheme is perfectly capable of recovering the one packet loss without discarding any received data. This indicates that the encoding scheme complements the low throughput.

TABLE XII
THROUGHPUT ACCORDING TO THE ENCODING SCHEME

Encoding scheme	avg.	Min.	Max.
On-offCTC [9]	6.55 bps	4.89 bps	9.77 bps
Binary [18]	9.77 bps	9.77 bps	9.77 bps
DPOI [8]	6.55 bps	4.883 bps	9.77 bps
PPCTC	2.79 bps	1.953 bps	4.89 bps

REFERENCES

[1] B. W. Lampson, "A note on the confinement problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, 1973.

[2] P. Szary, W. Mazurczyk, S. Wendzel, and L. Caviglione, "Design and performance evaluation of reversible network covert channels," in *Proc. 15th Int. Conf. Availability Rel. Security*, 2020, pp. 1–8.

[3] W. Mazurczyk, P. Szary, S. Wendzel, and L. Caviglione, "Towards reversible storage network covert channels," in *Proc. 14th Int. Conf. Availability Rel. Security*, 2019, pp. 1–8.

[4] W. Mazurczyk, K. Powójski, and L. Caviglione, "IPv6 covert channels in the wild," in *Proc. 3rd Central Eur. Cybersecurity Conf.*, 2019, pp. 1–6.

[5] J. Saenger, W. Mazurczyk, J. Keller, and L. Caviglione, "VoIP network covert channels to enhance privacy and information sharing," *Future Gener. Comput. Syst.*, vol. 111, pp. 96–106, Oct. 2020.

[6] H. Tian, J. Sun, C.-C. Chang, J. Qin, and Y. Chen, "Hiding information into voice-over-IP streams using adaptive bitrate modulation," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 749–752, Apr. 2017.

[7] H. Hovhannisyan, K. Lu, and J. Wang, "A novel high-speed IP-timing covert channel: Design and evaluation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 7198–7203.

[8] F. Rezaei, M. Hempel, P. L. Shrestha, and H. Sharif, "Achieving robustness and capacity gains in covert timing channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 969–974.

[9] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: Design and detection," in *Proc. ACM Conf. Comput. Commun. Security*, 2004, pp. 178–187.

[10] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert channel detection," *ACM Trans. Inf. Syst. Security*, vol. 12, no. 4, pp. 1–29, 2009.

[11] J. Zheng, S. Li, S. Hao, Y. Li, and Y. Zhang, "ZM-CTC: Covert timing channel construction method based on zigzag matrix," *Comput. Commun.*, vol. 182, pp. 212–222, Jan. 2022.

[12] C. Liang, T. Baker, Y. Li, R. Nawaz, and Y.-A. Tan, "Building covert timing channel of the IoT-enabled MTS based on multi-stage verification," *IEEE Trans. Intell. Transp. Syst.*, early access, Oct. 19, 2021, doi: 10.1109/TITS.2021.3118853.

[13] Y. Li, X. Zhang, X. Xu, and Y.-A. Tan, "A robust packet-dropout covert channel over wireless networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 60–65, Jun. 2020.
[14] X. Zhang, L. Zhu, X. Wang, C. Zhang, H. Zhu, and Y.-A. Tan, "A packet-reordering covert channel over VoLTE voice and video traffics," *J. Netw. Comput. Appl.*, vol. 126, pp. 29–38, Jan. 2019.
[15] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-A. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Inf. Sci.*, vols. 445–446, pp. 66–78, Jun. 2018.
[16] X. Zhang, Y.-A. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over volte via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.
[17] K. Sawicki, G. Bieszczad, and Z. Piotrowski, "StegoFrameOrder—MAC layer covert network channel for wireless IEEE 802.11 networks," *Sensors*, vol. 21, p. 6268, Sep. 2021.
[18] T. O. Walker and K. D. Fairbanks, "An off-the-shelf, low detectability, low data rate, timing-based covert channel for IEEE 802.11 wireless networks," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2017, pp. 835–840.
[19] R. Holloway and R. Beyah, "Covert DCF: A DCF-based covert timing channel in 802.11 networks," in *Proc. 8th IEEE Int. Conf. Mobile Ad-Hoc Sens. Syst. (MASS)*, 2011, pp. 570–579.
[20] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "Realizing an 802.11-based covert timing channel using off-the-shelf wireless cards," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2013, pp. 722–728.
[21] K. Sawicki and Z. Piotrowski, "The proposal of IEEE 802.11 network access point authentication mechanism using a covert channel," in *Proc. 19th Int. Conf. Microw. Radar Wireless Commun.*, vol. 2, 2012, pp. 656–659.
[22] L. Frikha, Z. Trabelsi, and W. El-Hajj, "Implementation of a covert channel in the 802.11 header," in *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, 2008, pp. 594–599.
[23] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2015, pp. 209–217.
[24] S. Ma *et al.*, "Covert beamforming design for intelligent-reflecting-surface-assisted IoT networks," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5489–5501, Apr. 2022.
[25] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie, and Y. Wang, "Covert communication with relay selection," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 421–425, Feb. 2021.
[26] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6313–6323, Apr. 2021.
[27] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communications without channel state information at receiver in IoT systems," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11103–11114, Nov. 2020.
[28] Y. Zhao, Z. Li, N. Cheng, W. Wang, C. Li, and X. Shen, "Covert localization in wireless networks: Feasibility and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6549–6563, Oct. 2020.
[29] L. Caviglione, "Trends and challenges in network covert channels countermeasures," *Appl. Sci.*, vol. 11, no. 4, p. 1641, 2021.
[30] S. Huang, W. Liu, G. Liu, Y. Dai, and H. Bai, "A correlation-based approach to detecting wireless physical covert channels," *Comput. Commun.*, vol. 176, pp. 31–39, Aug. 2021.
[31] K. Grzesiak, Z. Piotrowski, and J. M. Kelner, "A wireless covert channel based on dirty constellation with phase drift," *Electronics*, vol. 10, no. 6, p. 647, 2021.
[32] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, "UAV-relayed covert communication towards a flying warden," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7659–7672, Nov. 2021.
[33] S. Qiao, G. Liu, X. Ji, and W. Liu, "The optimal carrier-secret ratio for wireless covert channels based on constellation shaping modulation," *Security Commun. Netw.*, vol. 2021, Dec. 2021, Art. no. 6919530.
[34] K. S. K. Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2787–2801, 2019.
[35] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on constellation shaping modulation," *Security Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 1214681.
[36] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.
[37] N. Hou and Y. Zheng, "Demo abstract: CLoRa-A covert channel over LoRa PHY," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2020, pp. 1288–1289.
[38] L. Qiu, Y. Zhang, F. Wang, M. Kyung, and H. R. Mahajan, *Trusted Computer System Evaluation Criteria*, Nat. Comput. Security Center, Washington, DC, USA, 1985.
[39] V. Petrov, T. Kurner, and I. Hosako, "IEEE 802.15.3D: First standardization efforts for sub-terahertz band communications toward 6G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 28–33, Nov. 2020.
[40] C. Deng *et al.*, "IEEE 802.11be Wi-Fi 7: New challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2136–2166, 4th Quart., 2020.
[41] G. Naik, B. Choudhury, and J.-M. Park, "IEEE 802.11bd & 5G NR V2X: Evolution of radio access technologies for V2X communications," *IEEE Access*, vol. 7, pp. 70169–70184, 2019.
[42] D.-J. Deng *et al.*, "IEEE 802.11ba: Low-power wake-up radio for green IoT," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 106–112, Jul. 2019.
[43] A. Croisier, "Introduction to pseudoternary transmission codes," *IBM J. Res. Develop.*, vol. 14, no. 4, pp. 354–367, 1970.
[44] J. M. Xianjun and M. W. Liu. "Open-source IEEE802.11/Wi-Fi baseband chip/FPGA design." 2019. [Online]. Available: https://github.com/open-sdr/openwifi
[45] T. Gleixner and D. Niehaus, "Hrtimers and beyond: Transforming the Linux time subsystems," in *Proc. Linux Symp.*, vol. 1, 2006, pp. 333–346.
[46] P. Jaccard, "Étude comparative de la distribution florale dans une portion des Alpes et des jura," *Bull. del la Société Vaudoise des Sci. Naturelles*, vol. 37, no. 142, pp. 547–579, 1901.
[47] C. Cachin, "An information-theoretic model for steganography," *Inf. Comput.*, vol. 192, no. 1, pp. 41–56, 2004.

Hayoung Seong (Student Member, IEEE) received the B.S. and M.S, degrees from the Department of Electronic Engineering, Hankyong National University, Anseong, South Korea, in 2017 and 2019, respectively.

He studied with the Information Security Engineering, University of Science and Technology, Daejeon, South Korea. His current research interests include wireless communication security and IoT security technologies.

Ikkyun Kim received the M.S.C.E. and Ph.D. degrees in computer engineering from Kyungpook National University, Daegu, South Korea, in 1996 and 2009, respectively.

Since 1996, he has been working with Electronics and Telecommunications Research Institute, Daejeon, South Korea, where he is currently the Director of Cybersecurity Research Division. And, he worked with Purdue University, Daegu, as a Visiting Scholar. He has developed several network-based intrusion detection systems and is currently working on new anomaly detection method against zero-day attacks for network security. His research interests include DDoS protection mechanism, high-speed network protection system, the design of network processor architecture for network security appliance, and big data security analytics for security intelligence.

Yongsung Jeon received B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University, Daegu, South Korea, in 1986, 1990, and 2010, respectively.

He was with Agency for Defense and Development, Daejeon, South Korea, from 1992 to 1999. He has been with the Electronics and Telecommunications Research Institute, Daejeon, since 1999 and he is currently a Principal Research Engineer. His major interests include digital logic design, information security, and cryptography.

Mi-Kyung Oh received the B.S. degree from the Department of Electrical Engineering, Chung-Ang University, Seoul, South Korea, in 2000, and the M.S. and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology, Deajeon, South Korea, in 2002 and 2006, respectively.

From September 2002 to February 2004, she was a Visiting Researcher with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN, USA. She is currently a Principal Researcher with the Electronics and Telecommunications Research Institute, Daejeon. Her research interests are wireless communication systems, SoC design, and IoT security technologies.

Sangjae Lee received B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in information and communication engineering from Chungbuk National University, Cheongju, South Korea, in 1999, 2001, and 2013, respectively.

He has been a Principal Researcher with Electronics and Telecommunications Research Institute, Daejeon, since 2000. He has been participated in developing the technologies for home gateway, home server, IEEE1394, VoIP, network traffic controller, and wireless PAN MAC and UWB SoC. His current research interests include wireless MAC and SoC design for wireless PAN, and IoT security technologies.

Dooho Choi (Member, IEEE) received the B.S. degree in mathematics from Sungkyunkwan University, Seoul, South Korea, in 1994, and the M.S. and Ph.D. degrees in mathematics from Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1996 and 2002, respectively.

He has been an Associate Professor with Korea University Sejong, Sejong, South Korea, since 2021. He was a Professor with the University of Science and Technology, Daejeon, from 2015 to 2020, and a Visiting Research Fellow with Queen's University Belfast, Belfast, U.K., from 2016 to 2017. He worked with Electronics and Telecommunications Research Institute, Daejeon, as a Principal Researcher from 2002 to 2020. His main research interests include side channel analysis and its countermeasure design, quantum crypto analysis, and security technologies of IoT.