이 일 구 교수 지도

석사학위 청구논문

iBeacon covert 채널의 구현 및 보안성 분석

2024

성신여자대학교 대학원

미래융합기술공학과

오 예 솔

iBeacon covert 채널의
구현 및 보안성 분석

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2023년 11월

성신여자대학교 대학원

미래융합기술공학과

오 예 솔

인 준 서

오예솔의 석사학위 논문으로 인준함

2023년 11월

심사위원장 이 주 희 (서명 또는 인)

심 사 위 원 김 성 민 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

성신여자대학교 대학원

논 문 개 요

Covert 채널은 일반적으로 통신이 탐지되지 않도록 보안 정책을 우회하여 정보를 비밀스럽게 전송하는 데 사용된다. 종래에는 네트워크 기반의 covert 채널뿐만 아니라 빛, 온도와 같은 요소를 활용하는 등 covert 채널을 구축하기 위한 다양한 기술이 제안되었다. 블루투스(Bluetooth)를 활용한 covert 채널도 연구되었으나, 비콘(Beacon)을 활용한 covert 채널은 활발히 논의되지 못하였다. 또한, 종래의 covert 채널은 은밀성과 대역폭 간의 트레이드 오프(trade-off) 문제가 존재하였다. 따라서 본 논문에서는 covert 채널 구축에 초점을 맞춰 Apple의 iBeacon 브로드캐스트 메시지의 보안성을 검토하고, 취약점을 분석해 두 가지 유형의 BLE(Bluetooth Low Energy) covert 채널을 구현하고 성능을 평가한다. 하나는 advertising 페이로드를 활용한 CSC(Covert Storage Channel)이고, 다른 하나는 advertising 인터벌을 활용한 CTC(Covert Timing Channel)이다. 본 논문은 CSC를 통해 대역폭을 높이고, CTC를 통해 은밀성을 향상시켜서 상호 보완적인 방식으로 사용 가능함을 증명하였다. 실험 결과에 따르면 CSC는 PDR(Packet Delivery Rate)이 75%를 초과하는 최대 911,600Bps(Bytes per second)의 처리량을 달성하며 iBeacon을 통해 상당한 데이터를 은밀하게 전송할 수 있음을 보여주었다. 또한, CTC를 활용할 경우 비밀 메시지를 반복적으로 전송했을 때 수신자가 88%의 정확도로 비밀 메시지를 식별할 수 있었다. 이는 합리적인 사용자에게 서비스를 제공하는 동시에 악의적인 사용자가 이를 활용하여 정보를 유출할 수 있음을 시사한다. 본 연구는 비콘 covert 채널을 활용한 블루투스 릴레이 공격의 가능성을 제시하며, BLE 비콘 보안 강화의 중요성을 강조한다.

목 차

표 차 례

그 림 차 례

Ⅰ. 서 론

Covert 채널은 컴퓨터 시스템이나 네트워크 내에서 은폐되거나 허가되지 않은 통신 채널을 의미한다. covert 채널은 일반적으로 보안 정책 및 제어를 우회하거나 위반하는 방식으로 정보나 데이터를 전송하여 통신 내용이 탐지되지 않도록 한다. 지난 수십 년 동안 네트워크 기반의 covert 채널을 설정하기 위해 수많은 기술이 제안되었으며[1-4], 블루투스(Bluetooth)[5], 전압[6], 소리[7], 빛[8]과 같은 다양한 구성요소를 이용하여 covert 채널을 설정할 수 있음을 보여주었다. 그중에서도 특히 사물인터넷(Internet of Things, IoT) 기기가 증가하면서 블루투스 기반 covert 채널에 대한 주의가 요구되고 있다. 글로벌 기술 시장 자문 회사인 ABI Research에 따르면, 현재 블루투스 지원 제품은 8억 1,500만 개 이상인 것으로 보고되었다[9]. 아마존, 알리바바, 구글, 바이두, 샤오미와 같은 대규모 인터넷 기업은 음성 인식과 같은 블루투스 기반 서비스를 제공할 뿐만 아니라 스마트 조명, 스마트 가전, 도어락, 센서 및 기타 다양한 유형의 기기에 블루투스를 활용하고 있다.

기기 간 근거리 통신을 위해 설계된 BLE(Bluetooth Low Energy) 기술은 특히 IoT 환경에서 통신 및 위치 기반 서비스를 위한 기술로써 폭발적인 성장을 이루어왔다. BLE는 높은 가용성, 저비용, 낮은 전력 소모 및 구축 용이성으로 인해 일상생활과 다양한 산업 환경에서 사용되고 있다. 일반적으로 배터리로 작동하지만 배터리 없이도 작동할 수 있으며[10], 현재 BLE는 스마트폰 대부분에 기본적으로 내장되어 있고, iOS, Android, Linux, Windows[11]와 같은 주요 운영체제에서 지원되고 있다.

Apple iBeacon[12]이나 Google Eddystone[13] 프로토콜의 BLE 장치는 작은 데이터 패킷인 비콘(Beacon) 메시지를 전송한다. 이 메시지는 일반

적으로 일정한 간격으로 인근 장치나 애플리케이션에 정보를 브로드캐스트하는 데 사용된다. 그러나 기존 비콘 시스템의 대부분은 전송되는 BLE 비콘 메시지나 프로토콜의 고유 파라미터에 대한 보안이 미흡하여 정보 유출 공격에 활용될 수 있다. 즉, 보안 취약점을 이용해 비인가 장치가 데이터를 도청하거나 스푸핑, 중간자 공격(Man In The Middle attack, MITM)을하는 등 비콘은 악용 가능성이 충분하다[14]. 또한, 장치가 특정 위치에서 자신의 존재를 알리기 위해 고유 식별자를 지속적으로 브로드캐스트하는 비콘의 고유한 특성 때문에 BLE를 사용하는 종단 장치 간 연결 없이도 advertising을 통해 비밀 통신을 설립할 가능성이 있다[15, 16]. 따라서 사용자의 프라이버시를 보호하고, 비인가 접근을 방지하며, 전송된 데이터의 무결성을 유지하기 위해서는 비콘 배포의 보안을 보장하는 것이 필수적이다.

본 논문에서는 Apple의 iBeacon을 중심으로 비콘 advertising의 보안 영향을 조사하고자 한다. iBeacon 분석을 기반으로 두 개의 BLE covert 채널인 CSC(Covert Storage Channel)와 CTC(Covert Timing Channel)를 구현하고 보안성을 분석한다. 페이로드 수정을 기반으로 하는 CSC는 모니터링이나 로깅이 없고 채널 용량을 최대화해야 할 때 데이터를 전송하는 데 효과적이다. 그리고 인터벌(Interval) 수정을 기반으로 하는 CTC는 CSC에 비해 은폐력이 강해서 안전하지만, 패킷의 전송 시간이 불확실하기 때문에 네트워크 통신 품질에 영향을 받을 수 있다[17]. 본 논문은 페이로드 기반의 covert 채널을 구현하고 PDR(Packet Delivery Rate)과 처리량을 평가한다. 실험 결과에 따르면 제안된 채널의 최대 처리량은 초당 911,600Bps로 효율적인 covert 채널임을 보였다. 또한, 인터벌 기반 covert 채널을 구현하고 메시지 해독 가능 여부를 평가한 결과, 비밀 메시지를 50번 반복하여 전송했을 때 수신자가 88%의 정확도로 비밀 메시지를 식별할 수 있음을 보였다.

본 논문의 주요 기여점은 다음과 같다.

- iBeacon을 활용한 브로드캐스트 메시지의 보안 취약점을 분석하고 BLE covert 채널의 공격 가능성을 입증했다.
- BLE covert 채널을 구현하고 처리량, 패킷 수신 정확도 등을 평가할 수 있는 프레임워크를 설계하였다.
- BLE covert 채널을 활용한 공격 시나리오를 제시하고 이에 대응하는 방법을 제안하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 covert 채널과 iBeacon에 대한 배경 기술을 서술하고, Ⅲ장에서는 covert 채널 선행연구를 분석한다. Ⅳ장에서는 iBeacon을 활용한 두 가지 유형의 covert 채널 모델을 설계하고 구현하는 방법을 설명한다. Ⅳ장 실험 환경에서 제안하는 방법의 실험 조건과 평가 방법에 관하여 서술하고, Ⅴ장에서 페이로드 기반 covert 채널과 인터벌 기반 covert 채널의 성능을 평가하고 실험 결과를 분석한다. Ⅵ장에서는 비콘 covert 채널을 활용한 공격 방법에 대해 논의하며, 마지막으로 Ⅶ장에서 결론을 맺는다.

Ⅱ. Background

본 장에서는 종래 covert 채널의 유형과 구조를 분석하고, iBeacon에 대한 개념을 서술한다.

2.1 Covert 채널

1973년 Lampson의 연구에서 처음으로 발신자와 수신자만이 통신 행위를 알고 비밀 메시지를 주고받을 수 있다는 covert 채널의 개념이 제안되었다[18]. 공격자는 정보를 훔치고, 세션 비밀번호나 권한 정보 등의 개인 정보를 전달하기 위해 covert 채널을 사용할 수 있다[17]. 종래의 네트워크 covert 채널은 CSC와 CTC 두 가지 유형으로 분류된다.

CSC는 합법적인 패킷 필드에서 예약되거나 비어있는 위치를 활용하는 방법이며[1, 19], 현재 네트워크 프로토콜 설계의 불완전성을 활용한다[20]. CSC는 일반적으로 프로토콜 필드에 비밀 메시지를 은닉한다[21]. 헤더나 PDU(Protocol Data Unit)의 크기를 이용해 비밀 메시지를 인코딩하고, 헤더나 PDU의 순서를 변경하는 구성 방법이 이용된다. 예를 들어, 네트워크 프로토콜을 이용한 CSC의 경우 TCP(Transmission Control Protocol)의 ID 필드나 IP의 옵션 비트가 사용되었다. 그러나 CSC는 사용되지 않는 패킷 헤더 필드의 변화를 관찰하여 쉽게 감지될 수 있다는 한계점이 존재한다.

1978년 Padlipsky의 연구를 시작으로, 다양한 CTC 설계 방식이 제안되었다[22]. CTC는 IPD(Inter-Packet Delay)나 패킷 재전송과 같은 전송 시간 간격 간의 차이를 이용한다[1, 19]. 다음의 Fig. 1, Fig. 2, Fig. 3은 각각

CTC 종래 연구인 [23], [24], [25]의 메커니즘을 표현한 것이다. Berk, V. [23]는 전송할 비밀 메시지를 바이너리 형식으로 인코딩하였다. 송신자가 비트 0을 고정된 지연 값으로, 비트 1을 비트 0으로 설정된 값보다 긴 길이의 고정된 지연 값으로 설정하여 전송하면 수신자는 송신자와 동일한 규칙을 이용해 비밀 메시지를 추출할 수 있다[26]. Cabuk, S. [24]는 송신자가 특정 시간 간격 내에 패킷을 전송할 경우 비트 1을, 어떠한 패킷도 보내지 않는 경우를 비트 0으로 표현하여 메시지를 전달하는 방식을 제안하였다. 수신자는 수신한 패킷의 트래픽 스트림을 스캔하여 비트를 디코딩하고 메시지를 읽을 수 있다. Cabuk, S. [25]는 통계분석을 통해 covert 채널이 발각되는 것을 방지하기 위해 TRCTC(Time-Relay Covert Timing Channel)를 제안하였다. 일반적인 통신의 시간 간격을 분석하여 임계값을 설정한 뒤, 임계값보다 큰 시간 간격과 작은 시간 간격 그룹으로 분류하였다. 이후 비트 0은 작은 시간 간격 그룹에서, 비트 1은 큰 시간 간격 그룹에서 무작위로 하나의 값을 선택하여 해당하는 시간 간격으로 비밀 메시지를 전송하였다.

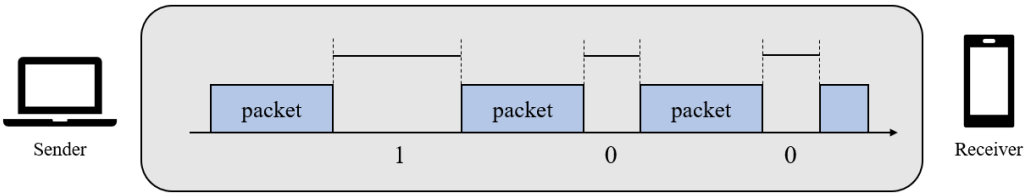

FIGURE 1. Structure of [23]

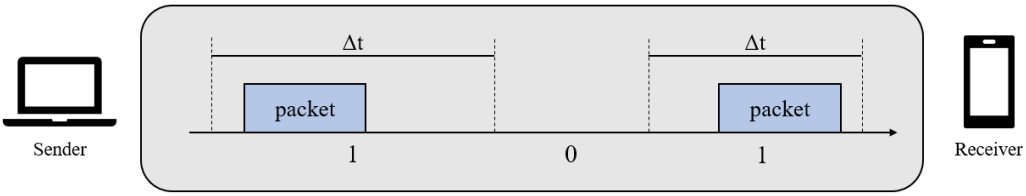

FIGURE 2. Structure of [24]

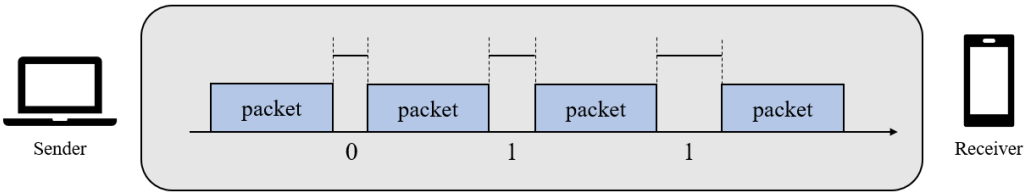

FIGURE 3. Structure of [25]

종래의 covert 통신 방식에서는 통신 과정에서 발신자가 IP주소를 이용해 수신자와 직접 연결하여야 했으며, 특히 CTC 시나리오에서 그 특징이 더욱 두드러졌다. 직접 연결하는 covert 통신 방식은 노출된 IP주소와 covert 통신을 통해 송신자와 수신자의 실제 신원을 추적할 수 있다는 문제점이 있다[18]. 따라서 본 논문에서는 수신자와 직접 연결하지 않고도 비밀 메시지를 교환하는 covert 통신 방식을 설계한다.

2.2 iBeacon

블루투스 비콘은 BLE 프로토콜을 사용하는 저비용, 저전력, 위치 기반 기술이다. 대표적인 비콘의 표준 통신 프로토콜로는 Apple이 개발한 iBeacon과 Google이 개발한 Eddystone이 있다[10, 27]. 비콘은 UUID(Universally Unique Identifier)와 함께 여러 바이트 정보가 포함된 블루투스 신호를 주변 환경에 브로드캐스트한다[27]. BLE는 비면허 주파수 대역인 2.4GHz ISM 대역에서 작동하며 주파수 호핑을 사용하여 동일한 대역에서 작동하는 다른 RF(Radio Frequency) 장치의 간섭을 최소화하므로[11], covert 채널을 구축하는 데 적합하다. 또한, iBeacon 기술은 산업적으로 이용할 수 있으며 실제 사례에서 사용되고 있으므로 연구 대상으로서의 가치가 있다[14]. iBeacon 프로토콜은 2013년에 도입되었으며, 단방향 검색 메커니즘을 사용하고 미리 지정된 간격으로 작은 데이터 패킷을 전송한다. 블루투스는 다양한 advertising 인터벌을 허용하고 있으나, iBeacon은 advertising 인터벌을 100ms로 권장하고 있다[28]. iBeacon 전송의 최대 범위는 위치와 배치에 따라 달라지며, 장거리 비콘의 경우 450m에 도달한다[27]. 다음의 Fig. 4와 TABLE 1은 iBeacon advertising 패킷의 구조와 필드의 구성 요소를 나타낸 것이다[15, 28-30].

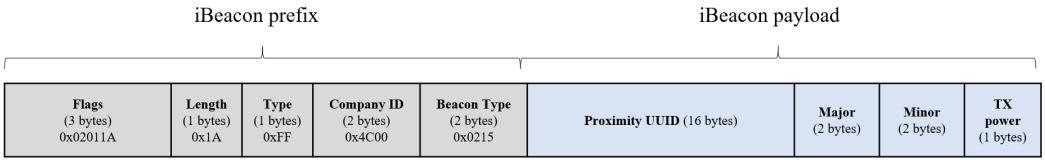

FIGURE 4. iBeacon packet structure

TABLE 1. Information fields of iBeacon packet

Field	Size (Bytes)	Usage
Flags	3	• Length, Type, Value 각 1바이트씩 구성됨. 02는 길이 지시자로 Flags 필드에 2개 바이트가 추가로 있음을 나타내며, 01은 Value 필드에 flag가 포함되었음을 나타내고, 1A는 flag 값을 나타냄
Length	1	• 해당 필드 이후에 오는 프레임 페이로드의 길이를 표시
Type	1	• 프레임의 내용이 제조사별 데이터임을 나타냄
Company ID	2	• 제조사별 advertising 페이로드의 시작으로, 4C는 Apple 회사 ID 번호를 나타냄
Beacon Type	2	• 02는 프로토콜 식별자이며, 15는 이후 페이로드의 길이를 표시
UUID	16	• 개발자는 개발 제품과 관련된 UUID를 정의해야 함
Major	2	• 특정 iBeacon 및 use case를 추가로 지정
Minor	2	• Region이나 use case를 세분화할 수 있음
TX power	1	• 블루투스 장치 제조업체가 1m 떨어진 곳에서 측정한 값

UUID 이전의 필드는 iBeacon prefix로, 해당 부분을 수정할 경우 iBeacon 수신기에서 패킷을 정상적으로 식별할 수 없으므로 탐지 가능성이 높다. 그러나 UUID, Major, Minor 부분을 수정하여도 전송 유효성에 영향을 미치지 않으므로 탐지 가능성이 비교적 낮으며, 20바이트 데이터를 이용할 수 있다.

비콘 장치까지의 거리는 TX power와 수신 신호의 현재 수신 신호 강도(Received Signal Strength Indicator, RSSI)를 통해 추정할 수 있으며[29], Apple API는 개발자에게 immediate, near, far, unknown의 4가지 상태를 제공한다[15, 30]. 따라서 TX power 필드를 수정하였을 때 정상적으로 거리를 추정할 수 없으면 unknown 설명자를 반환하므로, iBeacon 프로토콜을 중단하지 않고도 유효한 covert 채널을 생성할 수 있다[15]. 다음의 TABLE 2는 iBeacon에서 비콘 장치까지의 거리를 나타내는 4가지 상태를 설명한 것이다.

TABLE 2. iBeacon proximity status description [30]

Proximity State	Description
Immediate	장치가 비콘에 물리적으로 매우 가까운 상태
Near	장치에서 비콘까지 약 1-3m의 거리가 있음
Far	비콘을 감지할 수 있으나 신뢰도가 너무 낮은 상태로, 반드시 물리적으로 가깝지 않다고 의미하는 것은 아님
Unknown	비콘의 근접성을 확인할 수 없으며 거리 측정이 막 시작되었거나 측정이 충분하지 않은 상태

Ⅲ. 관련 연구

본 장에서는 연구의 배경이 되는 covert 채널을 두 가지 유형으로 분류하여 종래의 covert 채널 연구를 검토하고, 그 기여점과 한계점을 분석한다.

3.1 CSC(Covert Storage Channel)

TABLE 3은 CSC 선행연구를 분석한 표이다. Priest, J. [15]는 Apple이 개발한 iBeacon에 covert 채널이 적용될 가능성을 주장했다. iBeacon prefix는 iBeacon의 정체성을 식별하는 역할을 하므로 이 부분을 수정하면 iBeacon으로 인식되지 않는다. 따라서 합법적인 iBeacon 수신기가 패킷을 iBeacon으로 해석할 수 있도록 prefix를 수정하지 않고 패킷의 수정 가능한 필드를 활용했다. Company ID의 두 번째 바이트, UUID, Major, Minor, TX power 필드를 수정하면 유효한 iBeacon을 생성할 수 있음을 확인하고, macbook pro와 ipad air7로 구성된 환경에서 기본 advertising 인터벌 동안 수신자가 얼마나 많은 advertising 패킷을 수신하는지 확인하였다. Priest, J. [15]는 iBeacon 필드를 분석하여 유효한 covert 채널이 생성될 수 있는 필드를 분석하였으나, 다양한 advertising 인터벌을 분석하지 못하여 iBeacon을 이용한 CTC의 성능을 충분히 평가하지 못했다는 한계점이 있다. Zhang, Q. [20]은 VoLTE(Voice over Long Time Evolution) 채널에서 RTCP(Real-time Transport Control Protocol) 페이로드를 수정하는 CSC를 제안하였다. Android 운영체제를 사용하는 두 개의 스마트 모바일 장치에 TCPdump할 수 있는 환경을 구축하였다. 양쪽 장치는 서로 다른 보안 수준을 가지고 있으며, 엄격하게 모니터링되는 환경과 모니터링되지 않는 환경으로

구분된다. 엄격한 모니터링 환경에서는 엔드포인트에 데이터 패킷이 도착하는 시간과 애플리케이션이 데이터 패킷을 처리하는 시간의 차이를 이용해 RTCP 패킷의 jitter 필드 중 최하위 비트(Least Significant Bit, LSB)만 수정하여 covert 채널을 구축했다. 엄격하지 않은 모니터링 환경에서는 느린 전송 속도를 보완하기 위해 EHSNR(Extended Highest Sequence Number Received) 필드와 BLP(Bitmask of following Lost Packets) 필드를 이용해 전송 대역폭을 증가시켰다. Zhang, Q. [20]은 K-S(Kolmogorov-Smirnov) test를 통해 구축된 CSC에서 엄격한 모니터링 환경에서도 변조된 필드를 감지하기 어려움을 검증하였으나, 전송 대역폭이 작고 수정할 수 있는 필드 비트가 매우 적다는 한계점이 존재한다. Gao, J. [31]은 RTP(Real-time Transport Protocol) 패킷 페이로드를 수정하는 CSC를 제안하고 평가하였다. RTP는 UDP(User Datagram Protocol)을 통해 실행되므로 전송 과정이 네트워크 노이즈에 영향받을 수 있어 신뢰성이 떨어진다. 따라서 재전송이 가능한 전송 제어 메커니즘을 설계하고, 비밀 메시지를 AES(Advanced Encryption Standard) 알고리즘으로 암호화하여 메시지 유출을 방지하고자 하였다. RTP 패킷의 헤더 섹션은 고정되어 수정할 경우에 탐지 가능성이 커져서 데이터 섹션을 수정해 메시지를 삽입했다. 또한, 송·수신자는 무작위로 생성되는 SSRC(Synchronization source)의 첫 8바이트를 결합해 AES 알고리즘의 키 값을 획득하고 공유한다. Gao, J. [31]은 RTP 패킷을 이용해 45KB/s의 전송 속도로 데이터를 은밀하게 전송할 수 있는 채널을 제안하였다. 그러나 송·수신자는 데이터 전송 전 연결을 설정하거나 중지하기 위한 추가적인 메시지 교환 절차가 필요하며, AES 알고리즘을 위한 키 협상이 필요하다는 한계점이 있다.

TABLE 3. Analysis of previous studies on CSC

Ref.	Contribution	Limitation
[15]	• iBeacon 패킷 내 covert 채널로 이용할 수 있는 필드 분석	• 충분한 advertising 인터벌별 처리량을 분석하지 못함
[20]	• 엄격한 모니터링 환경에서도 변조 필드를 탐지하기 어려움	• 전송 대역폭이 낮고 수정할 수 있는 필드 비트가 매우 적음
[31]	• 신뢰도가 낮은 RTP 프로토콜을 극복하기 위한 재전송이 가능한 전송 제어 메커니즘 설계 • AES 알고리즘을 이용해 비밀 메시지를 암호화하여 메시지 유출 방지	• 데이터 전송 전 AES 키 협상 필요 • 송신자와 수신자가 연결을 설정하거나 중지하기 위한 추가적인 메시지 송·수신 절차 필요

3.2 CTC(Covert Timing Channel)

TABLE 4는 CTC 선행연구를 분석한 표이다. Seong, H. [19]는 IEEE 802.11 환경에서 공용 AP(Access Point)의 BI(Beacon Interval)를 활용한 비밀 무선 단방향 통신 메커니즘을 구축하였다. 전송되는 정보의 기밀성과 무결성을 위한 프레임 구조를 제안하였으며, 탐지 가능성을 줄이기 위한 PPCTC(Ping-Pong Covert Timing Channel) 데이터 인코딩 방식을 제안하였다. 제안하는 메커니즘은 단방향 통신이지만, 연속적인 2비트 오류에 대한 복구 특성이 있어서 안정적인 통신을 보장하였다. 802.11 a/b/n 표준을 따르는 Openwifi와 Xilinx Zynq를 이용해 합법적인 사용자에게 합법적인 서비스를 제공하는 동시에 은밀한 수신자에게 신호를 전송하는 AP를 구현하였으며, Linux 커널 타이머를 jiffies 기반에서 hrtimer로 변경하여 수십 마이크로초 이내의 시간 차이를 제어하였다. Seong, H. [19]는 정밀하게 인터벌을 조정함으로써 은밀성을 향상시키고, SHA-1과 XOR 암호를 이용하여 비밀 메시지를 유출하는 covert 채널을 구현하였으나, 하드웨어를 수정해야 하며 제한된 페이로드 길이로 인해 전송 성능을 크게 높일 수 없다는 한계점이 존재한다. Zhang, X. [32]는 VoLTE(Voice over LTE) 환경에서 silence period를 조정하는 covert 채널을 제안하였다. VoLTE 트래픽의 IPD는 고정되어 있어서 애플리케이션에 적용할 수 없으므로, silence period를 조정하여 고유한 기호로 covert 메시지를 인코딩하여 전송한다. 사전에 송신자와 수신자는 사용자 정의 매개변수를 공유하며, 수신자는 covert 메시지를 수신하여 디코딩한다. 채널 노이즈를 완화하기 위해 그레이 코드를 이용해 메시지를 인코딩하며, KS와 KLD(Kullback-Leibler divergence) 테스트를 사용하여 탐지 불가능성을 테스트하였다. Zhang, X. [32]는 IPD 기반 방법보다 견고성을 개선했으며, VoLTE 환경에서의 탐지 불가능성을 입증하였다. 그러나 대량의 데

이터를 전송하는 것이 비효율적이며, silence period가 길어질수록 음성 품질에 영향을 미칠 수 있다는 한계점이 존재한다. Zi, X. [33]은 게이트웨이나 라우터와 같은 중간 노드에 상주하며 통과하는 패킷의 전달 시간을 변조하여 은밀하게 메시지를 전송하는 IP-PCTC(Inter-Packet Passive Covert Timing Channel)를 구현하고 테스트했다. 송신자의 위치에 패킷이 도착하면 일시적으로 패킷을 버퍼링하고 계획된 시간에 전달하며, 메시지는 인접한 패킷 간 전달 간격으로 인코딩된다. 정보를 전송하기 위해 송신자와 수신자는 비트 0과 비트 1의 값을 미리 협상해야 하며, 수신자는 두 패킷 간 도착 간격이 특정 값보다 짧을 때 비트 0으로, 길면 비트 1로 디코딩한다. IP-PCTC는 버퍼를 이용하므로 버퍼 오버플로우나 패킷 고갈과 같은 상황이 나타날 수 있어 채널의 상태를 통신 상태, 일시정지 상태, 빠른 전송의 3가지 상태로 나누어 정의하고 임계값에 따라 채널을 전환하여 메시지를 전송한다. Zi, X. [33]은 패리티 비트를 이용해 1비트의 손실 오류를 정정할 수 있으며, 71 bps(bits per second)의 전송률을 보여주었다. 그러나 채널 상태를 식별하기 위한 추가적인 패킷 전송이 필요하며, 프레임 동기화를 위해 인접한 프레임 사이에 패킷을 전송하지 않는 무음 간격을 도입하여 전송할 수 있는 메시지의 양이 감소한다는 한계점이 있다. Archibald, R. [34]는 파운틴 코드(Fountain code)를 기반으로 한 CTC를 설계하고 분석했다. 인코딩 과정에 CSPRNG(Cryptographically Secure Pseudo-Random Number Generator)를 추가하여 covert 채널이 탐지되더라도 CSPRNG를 초기화하는 데 사용되는 무작위 시드 값을 먼저 발견하지 않고는 비밀 메시지를 해독할 수 없게 하여 보안성을 높였다. 송신자는 일반 트래픽과 통계적으로 구분할 수 없는 IPD를 생성하며, 인코딩된 비밀 메시지는 패킷 스트림의 IPD에 매핑된다. 또한, BP 알고리즘(Belief Propagation)과 보호 대역(Guard Band)을 사용해 비트 오류를 최소화하고 코드와 디코딩 속도를 향상시키고자 했다. Archibald, R.

[34]의 최대 처리량은 보호 대역이 0.3일 때 4.25bps 였으며, 제안하는 모델의 견고성과 보안성을 모두 높이고자 하였다. 그러나 메시지 수신 여부를 알리기 위한 역방향 채널이나 대역 외 채널이 필요하며, 보호 대역이 늘어날수록 비트 오류가 감소하나 평균 IPD가 증가한다는 한계점이 존재한다.

종래의 연구는 페이로드 길이가 제한되어 전송 성능을 높이기 어렵거나, 대량의 데이터를 전송하는 데 비효율적인 한계점이 존재하였다. 또한, 802.11 네트워크나 VoLTE에서 covert 채널을 구축한 선행연구는 다수 존재했으나, 블루투스 환경, 특히 비콘을 활용하여 covert 채널을 구축한 연구는 활발히 이루어지지 않았다. 따라서 본 논문에서는 비콘을 활용한 high-throughput covert 채널을 구축하고 평가하고자 한다.

TABLE 4. Analysis of previous studies on CTC

Ref.	Contribution	Limitation
[19]	• 마이크로초 단위의 정밀한 인터벌 조정 • 암호화를 통한 메시지 은폐	• 하드웨어 수정 필요 • 제한된 페이로드 길이로 전송 성능을 크게 높일 수 없음
[32]	• IPD 기반 방법보다 견고성 향상 • 그레이코드로 메시지를 인코딩하여 채널 노이즈 완화	• 대량 데이터 전송에 비효율적 • 메시지가 길어지면 음성 품질에 영향을 미칠 수 있음
[33]	• 패리티 비트를 이용해 1비트의 손실 오류 정정 가능	• 채널 상태를 식별하기 위한 추가적인 패킷 전송이 필요 • 프레임 동기화를 위해 인접한 프레임 사이 무음 간격을 도입해 전송 가능한 메시지의 양 감소
[34]	• 인코딩 프로세스에 CSPRNG를 추가하여 채널이 탐지되어도 제3자가 비밀 메시지 해독 불가능 • 보호 대역을 도입해 네트워크 노이즈로 인한 비트 오류 최소화	• 메시지 수신 여부를 알리기 위한 역방향 채널이나 대역 외 채널이 추가로 필요 • 보호 대역이 늘어날수록 비트 오류가 감소하나 평균 IPD가 증가함

Ⅳ. BLE covert 채널 메커니즘

본 장에서는 iBeacon 기반 covert 채널을 페이로드 기반(CSC)과 인터벌 기반(CTC) 2가지 유형으로 설계한다. 페이로드 기반 채널은 iBeacon 브로드캐스트 메시지 페이로드 내 데이터를 직접 수정하는 반면, 인터벌 기반 채널은 두 iBeacon 패킷 사이의 인터벌로 데이터를 인코딩 함으로써 더욱 은밀한 통신이 가능하다. 서론에서 언급한 것과 같이, 페이로드 기반 covert 채널은 모니터링이나 로깅이 없는 환경에서 채널 용량을 극대화할 수 있으며, 인터벌 기반 covert 채널은 은닉성을 좋게 하거나 채널 용량이 작고 전송 환경에 따라 지연이 증가할 수 있다. 이러한 두 채널의 특징을 이용하여 상호 보완적으로 사용할 수 있다. 예를 들어 인터벌 기반의 covert 채널로 데이터를 전송하는 동시에 페이로드의 일부를 시퀀스 번호로 변경하여 전송하면, 패킷 전송 중 오류가 발생하더라도 수신자는 시퀀스 번호에 따라 패킷 누락을 인지해 재전송을 요청할 수 있다. 또는, 페이로드 기반의 covert 채널에서 송신자가 보낸 패킷임을 수신자에게 증명하기 위해 사전에 합의한 advertising 인터벌로 패킷을 전송할 수 있다. 다음 절에서는 iBeacon을 이용한 covert 채널 모델을 구체적으로 설계하고 설정하는 방법을 다룬다.

4.1 설계 개요

1) iBeacon CSC

3.2에서 언급한 것과 같이, UUID, Major, Minor, TX power 필드를 수정하여 iBeacon CSC를 설계할 수 있다. 필드 전체를 수정하여 비밀 메시지를 포함할 수 있지만, 필드 일부분만 수정해도 비밀 메시지를 전달할 수 있다. 예를 들어 TX power 필드 전체인 1바이트를 수정할 수 있지만, 1바이트 중 일부 비트만 수정해도 메시지를 전달할 수 있다. iOS 장치는 비콘의 신호를 감지했을 때 수신 신호 강도를 사용하여 비콘 송신기와의 거리를 추정한다[30]. 1바이트를 수정하면 1비트를 수정할 때보다 신호 강도의 변화 폭이 커져서 감지될 위험성이 커진다. 이처럼 비트 단위로 수정할수록 은밀성이 보장되지만, 전송할 수 있는 메시지의 양이 감소한다는 단점이 있다. 다음의 Fig. 5와 Fig. 6은 각각 TX power 필드를 비트 단위와 바이트 단위로 수정한 예시이다.

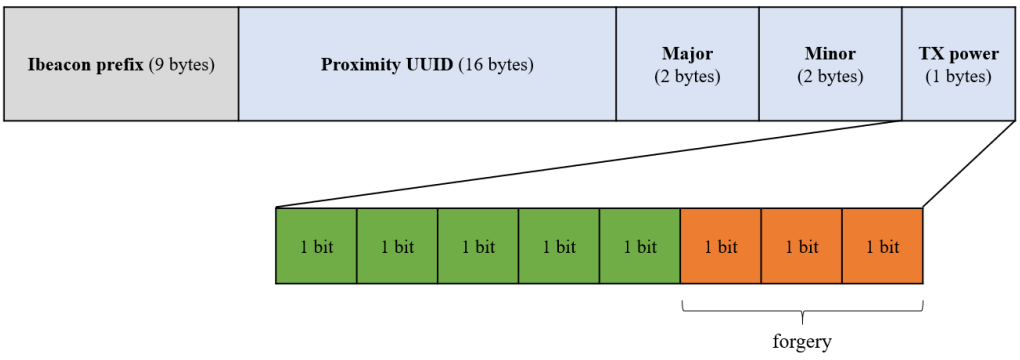

FIGURE 5. Bit-level forgery of the TX power field

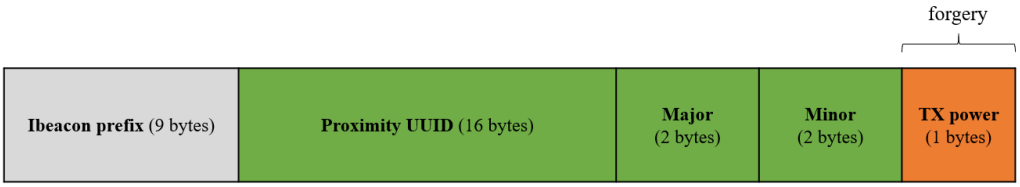

FIGURE 6. Byte-level forgery of the TX power field

Fig. 7은 페이로드 기반 iBeacon covert 채널 모델의 예시이다. 해당 모델은 CSC지만 단순히 페이로드만 수정하지 않고 advertising 인터벌을 변경하여 탐지 가능성을 낮출 수 있다. 송신자와 수신자는 사전에 특정 인터벌로 수신되는 advertising 패킷에 비밀 메시지가 포함되어 있다고 가정한다. 송신자는 합의된 규칙에 따라 페이로드를 수정하여 iBeacon 패킷을 advertising한다. 예를 들어 500ms 인터벌로 수신되는 패킷에 비밀 메시지가 포함되어 있다고 합의했다면 송신자는 UUID, Major, Minor 필드에 비밀 메시지를 은닉하고, TX power 필드를 시퀀스 번호 필드로 이용해 페이로드를 수정한다. 송신자는 정상적인 패킷을 200ms로 advertising하고, 페이로드가 변조된 패킷은 500ms로 advertising하여 수신자가 비밀 메시지를 수신할 수 있도록 한다. 송신자와 수신자는 직접적인 연결이나 하드웨어 수정을 하지 않고도 메시지를 교환할 수 있다.

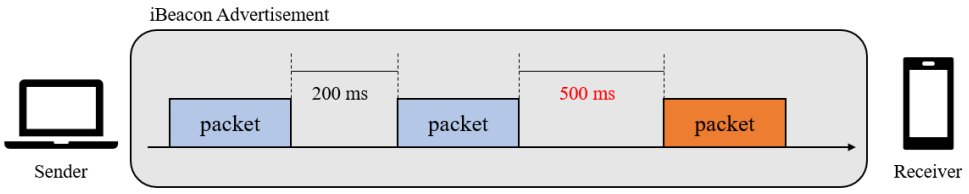

FIGURE 7. Payload-based covert channel using iBeacon

2) iBeacon CTC

iBeacon CTC는 advertising 인터벌을 조정하는 방식으로 covert 채널을 구현한다. iBeacon 규격 내에서 advertising 인터벌은 100ms로 권장되지만, 인터벌을 수정할 수 있다. 비밀 메시지를 전송하려는 송신자가 advertising 인터벌을 100ms 내외로 설정한다면 일반적인 advertising 패킷과 구분하기 어려워서 은밀성이 향상되지만, 네트워크 환경에 따른 패킷 지연의 영향을 크게 받아 수신자가 메시지를 해석하기 어렵다. 만약 advertising 인터벌을 100ms보다 크게 설정한다면 은밀성은 감소할 수 있으나, 패킷 지연의 영향이 적어서 수신자가 더 명확하게 메시지를 해석할 수 있다.

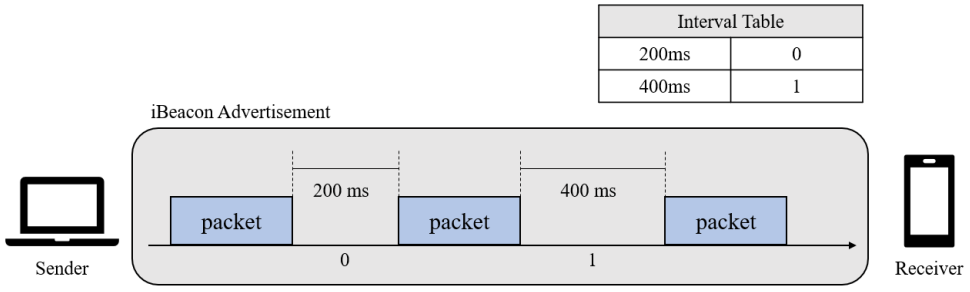

FIGURE 8. Interval-based covert channel using iBeacon

Fig. 8은 인터벌 기반 iBeacon covert 채널 모델의 예시이다. 사전에 송신자와 수신자가 advertising 인터벌 규칙을 합의하면 송신자는 메시지를 암호화하고 합의된 규칙에 따라 iBeacon 패킷을 advertising한다. 예를 들어 비밀 메시지를 모스부호로 암호화하여 전송할 경우 '·'을 0, '-'를 1로 변환할 수 있다. 송신자와 수신자는 사전에 패킷이 200ms 인터벌로 도착하면 0, 400ms 인터벌로 도착하면 1로 해석하는 규칙을 합의했다고 가정한다. 송신자가 'A'를 전송하려는 경우, 'A'를 '01'

로 변환한 뒤 200ms 인터벌로 한 번, 400ms 인터벌로 한 번 총 패킷을 3번 전송하여 ‘A’를 전송할 수 있다. 그러나 ‘S’를 전송하고자 한다면 ‘000’이므로 ‘E’의 ‘0’이나 ‘I’의 ‘00’과 같이 동일한 기호로 변환되는 문자와 혼동될 수 있다. 따라서 송신자는 advertising 인터벌 뿐만 아니라 패킷의 페이로드를 변조해 시퀀스 번호를 추가함으로써 동일한 기호가 연속되어 전송되어도 수신자가 구분할 수 있게 할 수 있다.

Fig. 9는 모스부호를 이용한 iBeacon CTC의 동작 구조를 나타낸 것이다. 모스부호를 이용하면 두 가지 경우의 수가 있으므로 두 개의 advertising 인터벌 값을 선정해야 한다. 비밀 메시지를 송·수신하기에 앞서, 송신자는 여러 개의 비콘 패킷을 advertising하고 지연값의 평균을 구한다. 지연값의 평균을 기반으로 송신에 사용할 advertising 인터벌 값과 메시지 판단을 위한 임계값을 결정한다. 인터벌 값과 임계값이 결정되면 송신자는 비밀 메시지를 모스 부호로 인코딩하고, ‘·’을 0, ‘–’를 1로 변환한다. ‘0’과 ‘1’을 앞서 구했던 advertising 인터벌 값에 각각 매핑한 뒤, 송신자는 패킷을 advertising한다. 수신자는 송신자가 보낸 패킷을 수신하고 시퀀스 번호 별로 인터벌의 평균값을 구한다. 처음에 합의했던 임계값에 따라 평균값을 ‘0’과 ‘1’로 변환하고, 이를 다시 모스부호로 디코딩하여 비밀 메시지를 수신할 수 있다.

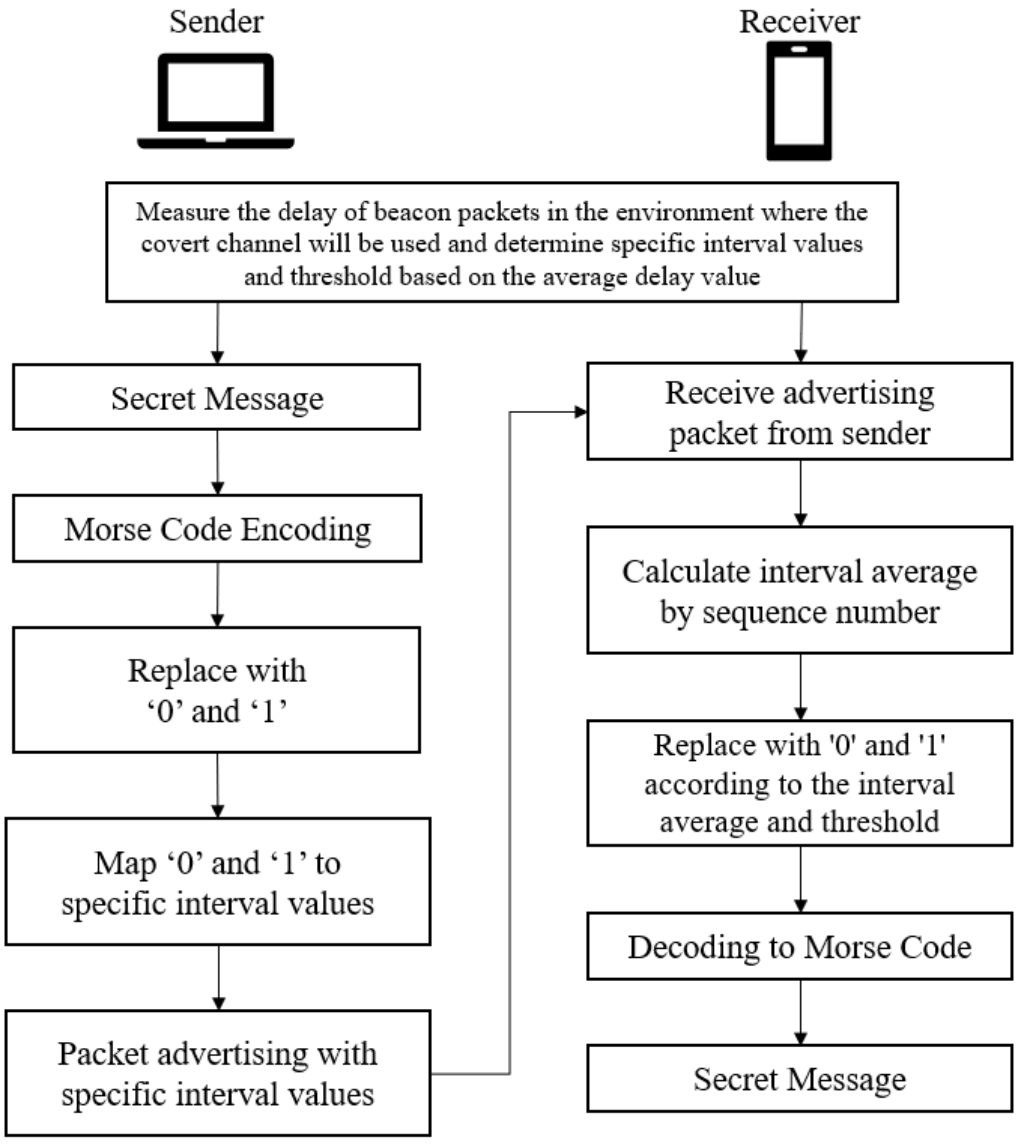

FIGURE 9. iBeacon CTC flowchart

4.2 iBeacon covert 채널 설계

1) iBeacon CSC

본 절에서는 페이로드 기반의 iBeacon CSC를 구현하기 위해 UUID, Major, Minor, TX power를 수정한다. Fig. 10은 UUID, Major, Minor를 임의로 설정하고 TX power를 시퀀스 숫자 필드로 사용하는 페이로드의 예시이다.

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

FIGURE 10. Example of forging payload

Fig. 11은 블루투스 인터페이스에 Fig. 10에서 설정한 대로 실제 페이로드를 구성하도록 하는 명령어이다.

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

FIGURE 11. Advertising payload configuration command

LE Controller Commands의 OGF(Opcode Group Field) 코드는 0x08로 정의된다. 0x0008은 LE Set Advertising Data Command로, 데이터 필드를 갖는 advertising 패킷에 사용되는 데이터를 설정할 수 있다[35]. 1E는 본인을 제외한 전체 페이로드의 길이를 나타낸다[15, 35]. 02 01 1A 1A FF 4C

00 02 15는 iBeacon의 prefix로 고정된 값이며, 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 12 00 00 00 00은 순서대로 Fig. 9에서 임의로 설정한 UUID, Major, Minor 값이다. 01은 TX power 값으로 시퀀스 번호로 설정하였으며, 패킷을 전송할 때마다 값이 1씩 증가한다.

2) iBeacon CTC

본 절에서는 인터벌 기반의 iBeacon CTC를 구현하기 위해 advertising 인터벌을 수정한다. BLE의 advertising 인터벌의 범위는 20ms-10.24s 사이 범위 내에서 0.625ms의 정수 배수여야 한다[35, 36]. 아래의 Fig. 12는 최소 100ms에서 최대 200ms 인터벌로 advertising을 시작하도록 하는 명령어이다.

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

FIGURE 12. Advertising interval configuration command

0x0006은 LE Set Advertising Parameters Command로, advertising parameter를 설정할 수 있도록 한다. Advertising_Interval_Min은 최소 advertising 인터벌로 최대 advertising 인터벌인 Advertising_Interval_Max보다 작거나 같은 값이어야 하며, 최적의 advertising 인터벌을 결정할 수 있도록 동일한 값으로 설정하는 것을 지양해야 한다. A0 00은 Advertising_Interval_Min이며, 40 01은 Advertising_Interval_Max이다. 16진수 0x00A0에 0.625ms를 곱하면 100ms, 0x0140에 0.625ms를 곱하

면 200ms로 Fig. 12는 100ms부터 200ms 사이의 인터벌로 패킷을 advertising하도록 설정되었음을 알 수 있다. 03은 Advertising_Type으로, 연결할 수 없음을 나타낸다. Advertising_Type이 0x03(ADV_NONCONN_IND)일 경우 최소 advertising 인터벌과 최대 advertising 인터벌이 0x00A0(100ms) 미만으로 설정되지 않아야 한다 [35]. 따라서 본 논문에서는 advertising 인터벌 범위를 100ms부터 2000ms까지 100ms 단위로 증가시켜 성능을 측정한다. 0x000A는 LE Set Advertise Enable Command로, Advertising_Enable 명령을 0x01(Advertising is enabled)로 설정하여 advertising을 시작할 수 있다.

Ⅴ. 실험 및 결과 분석

5.1 실험 환경

본 장에서는 Ⅱ장에서 설계한 모델을 토대로 iBeacon을 활용한 covert 채널을 구현하기 위한 실험 환경을 서술한다. 본 실험은 raspberry pi 3 b+ 환경에서 Python 3으로 Ⅳ장의 명령어를 hcitool을 이용해 터미널에 입력하는 송신기와 수신기 코드를 구현하였다. Bluez는 Linux 시스템에서 효율적인 Bluetooth 모듈식 구현을 가능하게 하는 라이브러리로[37], 5.55버전을 이용하였다. 송신 raspberry pi는 Ⅳ장에 기술된대로 패킷의 페이로드를 구성하여 iBeacon 패킷을 advertising하며, 수신 raspberry pi는 송신 raspberry pi가 advertising한 iBeacon 패킷을 수신하여 수신 시간, raw data, raw data를 16진수로 변환한 데이터를 출력하도록 하였다.

페이로드 기반의 covert 채널 구현에 있어 정상 수신된 패킷과 누락된 패킷의 수를 파악하기 위해 페이로드의 TX power 필드에 시퀀스 번호를 부여하여 1씩 증가하도록 하였다. Advertising 인터벌 별 PDR은 아래의 수식 (1)로 산출했으며, 소수점 셋째자리에서 반올림하였다.

$$PDR(\%) = (Received\ Packets) / (Entire\ Packets) \times 100 \quad (1)$$

2.2의 Fig. 4에서 언급한 것과 같이, iBeacon 페이로드에서 UUID, Major, Minor를 covert 채널 필드로 활용할 수 있으므로, 패킷 1개 당 20바이트의 정보를 송신할 수 있다. 따라서 advertising 인터벌 별 최대 처리량(Max Throughput) 수식과 최소 처리량(Min Throughput) 수식은 아래의 (2),

(3)과 같고[38], 소수점 첫째자리에서 반올림하였다.

$$\max throughput\,(Bps) = (Received\ Packets) \times 20(Bytes)/\min advertisinginterval \quad (2)$$

$$\min throughput\,(Bps) = (Received\ Packets) \times 20(Bytes)/\max advertisinginterval \quad (3)$$

또한, 인터벌 기반의 covert 채널 성능 평가를 위해 알파벳 메시지를 모스 부호로 변환하여 정수 값으로 치환한 뒤, 특정 인터벌 값에 매핑하여 전송하였다. 본 실험에서는 0을 100ms, 1을 600ms로 가정하였으며, 송신자는 advertising 인터벌과 함께 패킷 별로 시퀀스 번호를 부여하여 전송한다. 수신 raspberry pi는 시퀀스 번호별로 advertising 인터벌의 평균값을 계산하여 중간 값인 350ms를 기준으로 350ms보다 작을 경우 0으로, 클 경우 1로 판단한다. TABLE 5는 모스 부호 치환 값 별 advertising 인터벌을 나타낸 것이다.

TABLE 5. Morse code replacement value

Morse code	Replacement value	Advertising Interval (ms)
·	0	100
-	1	600

5.2 실험 및 결과 분석

1) iBeacon CSC

본 절에서는 제안하는 iBeacon을 활용한 페이로드 기반의 covert 채널의 성능을 검증하기 위한 평가지표로 PDR과 처리량을 이용하였다. 송신기는 advertising 인터벌 별로 60개의 패킷을 100회 반복 전송하였다. 수신기는 송신기가 전송한 모든 advertising 패킷을 수집하여 기록하였으며 이를 토대로 정상 수신 패킷과 누락 패킷의 평균을 계산하였다. TABLE 6은 advertising 인터벌 별 PDR을 나타내며, TABLE 7은 최소 advertising 인터벌과 최대 advertising 인터벌의 차이를 100ms로 하여 100ms부터 2000ms까지의 최소 처리량과 최대 처리량을 계산한 것이다. Fig. 13은 Advertising 인터벌 별 PDR과 처리량을 나타낸 그래프이다.

TABLE 6. PDR per advertising interval

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

TABLE 7. Throughput per advertising interval

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

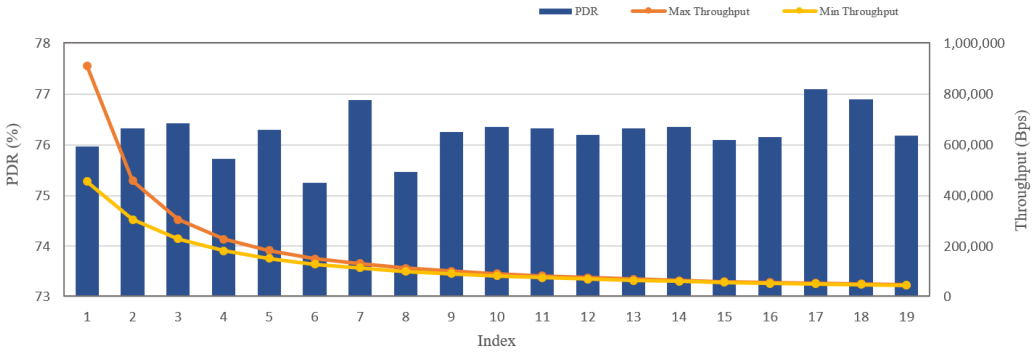

FIGURE 13. PDR and throughput per advertising interval

실험 결과, 가장 높은 PDR은 1700-1800ms의 77.1%, 가장 낮은 PDR은 600-700ms의 75.25%로 1.85%p 차이를 보여 전체적으로 유사한 PDR임을 확인할 수 있다. 처리량은 advertising 인터벌이 짧을수록 큰 결과를 보였으며, 100-200ms의 처리량이 가장 높았다. 따라서 advertising 인터벌 별 PDR 차이가 근소하였을 때, 100-200ms의 advertising 인터벌로 전송할 때 가장 효율적임을 알 수 있었다.

본 실험 결과는 어떤 advertising 인터벌을 선택하여 전송하여도 일정 수준 이상의 PDR을 보장할 수 있으며, 송신자와 수신자의 상황에 따라 적절한 advertising 인터벌을 선택하여 정보를 교환할 수 있음을 시사한다. 예를 들어 복잡한 네트워크 환경에서 정보를 교환하고자 하는 경우 긴 advertising 인터벌을 선택할 수 있다. 또 다른 예로 단기간에 많은 정보를 교환해야 할 때 짧은 advertising 인터벌을 선택하여 전송할 수 있다.

2) iBeacon CTC

본 절에서는 제안하는 iBeacon을 활용한 iBeacon CTC의 성능을 검증하기 위해 인터벌의 평균을 계산하였다. 먼저 송신자는 비밀 메시지를 전송하기 위해 문장이나 단어를 모스 부호로 변환한다. 본 논문에서는 'test'라는 메시지를 전송하였으며, 이를 모스 부호로 변환하면 '- · · · · -' 이다. 해당 모스 부호 값을 TABLE 5에 따라 정수 값으로 치환하면 '1 0 000 1'이다. 0은 100ms, 1은 600ms로 전송되도록 설정했으며, 최소 advertising 인터벌 값과 최대 advertising 인터벌 값은 동일하게 설정하였다. 또한, 하나의 정수 값 당 하나의 시퀀스 번호를 매핑하여 총 6개의 시퀀스 번호를 부여했다. 송신기는 하나의 시퀀스 번호 당 2초 동안 전송하였으며 메시지를 50번 반복하여 전송했다. 수신기는 송신기가 전송한 모든 advertising 패킷을 수집하여 기록하고 시퀀스 번호 별 평균 인터벌 값을 계산, 소수 첫째자리에서 반올림하여 송신기가 의도한 값으로 도착하였는지 확인했다. 6개의 시퀀스 번호를 순차적으로 판단하여 하나라도 잘못 판단될 경우 해당 메시지는 전송이 실패한 것으로 간주했다. TABLE 8은 시퀀스 번호 별 인터벌 평균을 나타낸다.

TABLE 8. Interval average per sequence number

Message	Replacement Value	Sequence number	Interval average (ms)
t	1	1	588
e	0	2	164
s	0	3	162
	0	4	153
	0	5	161
t	1	6	605

총 3651개의 패킷을 수신하였으며, 그 중 109개의 패킷이 지연되어 인터벌 값이 1000ms 이상으로 기록되어 해당 값을 제거하고 평균을 계산하였다. 50번 전송한 'test' 에서 6개의 시퀀스 번호를 연속적으로 모두 성공적으로 판단한 경우는 44번으로 88%의 정확도를 보여주었다.

본 실험에서는 100ms와 600ms의 중간값인 350ms를 기준으로 판단하였으나, 네트워크 환경에 따라 다르게 적용할 수 있다. 동일한 환경에서 0을 100ms, 1을 300ms로 전송하고 중간값인 200ms를 기준으로 판단하였을 때 50개의 'test' 메시지 중 30개 만을 정상적으로 판별할 수 있었다. 이처럼 네트워크 환경의 복잡도는 항상 일정하지 않으므로, 비밀 메시지를 송·수신하고자 하는 환경에서 사전에 테스트 패킷을 전송하여 인터벌 지연의 평균을 구하고 그를 기준으로 임계값을 정할 수 있다.

Ⅵ. 논의

본 논문에서는 iBeacon을 이용한 covert 채널을 설계하고 그 성능을 평가하였다. 블루투스는 일상생활에 매우 밀접한 기술이므로, 블루투스를 이용하여 정보를 유출하였을 때 그 파급력이 매우 크다.

BLE의 일반적인 범위는 수십 미터(m)로[30], Wi-Fi에 비해 비교적 범위가 좁다. 그러나 블루투스 기기 간에 수신한 패킷의 인터벌을 그대로 다른 기기에 릴레이로 전송할 경우, 그 범위는 크게 늘어날 수 있다. Fig. 14는 블루투스 기기를 이용해 송신자의 범위 밖에 있는 수신자에게 릴레이로 정보를 전송하는 예시이다.

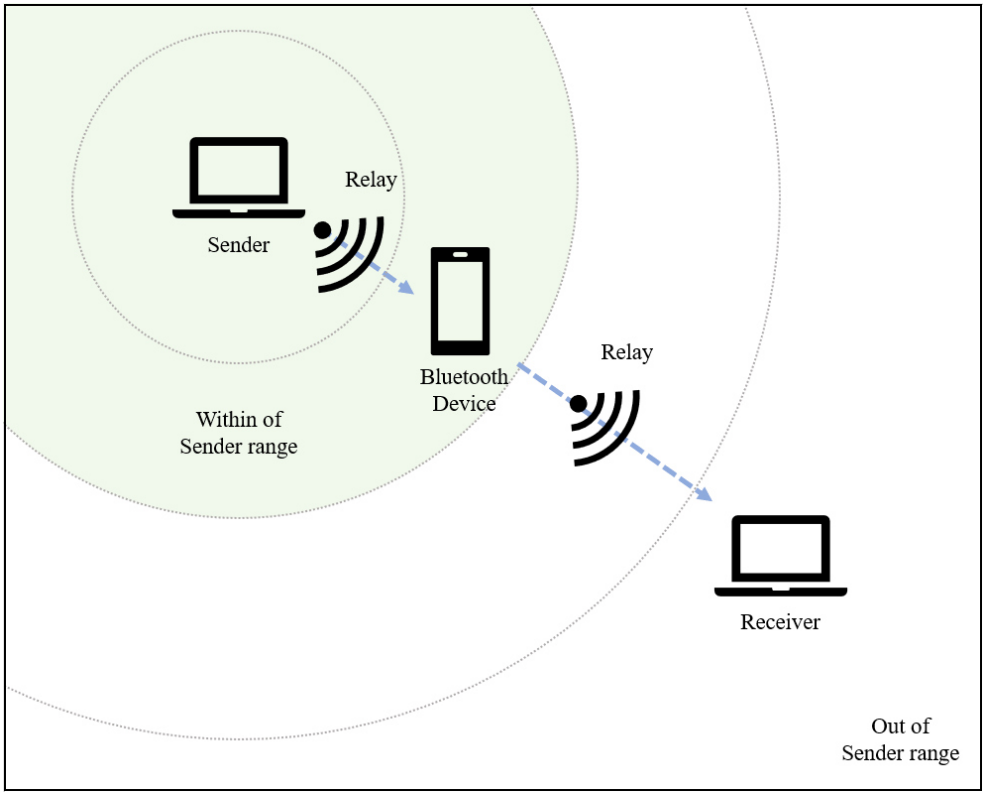

FIGURE 14. Example of relay transmission using a bluetooth device

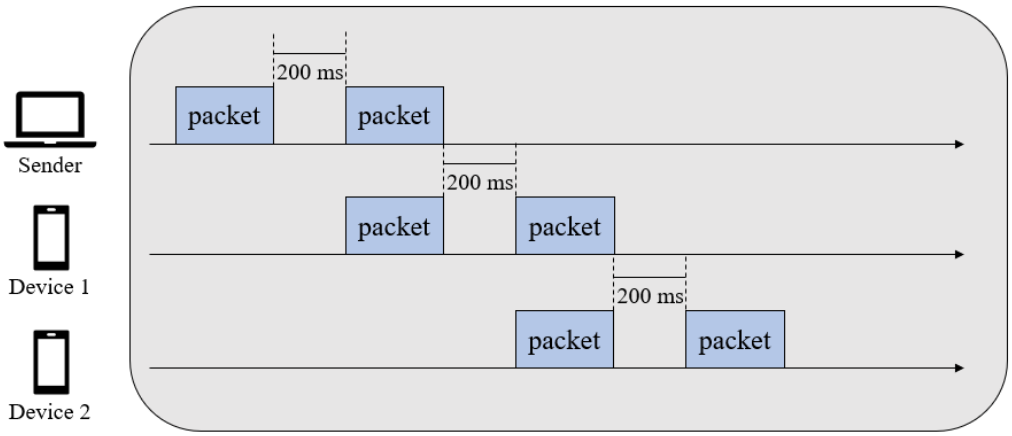

FIGURE 15. Example of relay transmitting interval between bluetooth devices

Fig. 15는 2개의 기기를 거쳐 정보를 전송하는 예시이다. 송신자가 200ms 인터벌로 패킷을 advertising하여 advertising 범위 밖에 존재하는 수신자에게 메시지를 전달하고자 했을 경우, 송신자와 수신자 사이에 위치하는 Device 1과 Device 2가 중계기 역할을 하여 메시지를 전송할 수 있다. iBeacon advertising 인터벌을 권장 설정인 100ms로 설정하고 송신 전력을 -12dBm으로 하였을 때, 예상 범위는 35m이다[39]. 공격자가 블루투스 기기의 advertising 인터벌이나 advertising 패킷 페이로드를 조작할 수 있다면, 비콘을 이용한 covert 채널의 한계이던 좁은 범위를 극복할 수 있다.

비콘은 단순한 브로드캐스팅 구조로 확장성이 매우 뛰어나지만 BLE 비콘 인프라는 승인되지 않은 제3자에 의해 쉽게 남용되고 공격받을 수 있다[40]. 인프라 소유자의 동의 없이 제3자가 비콘 인프라를 사용하거나, 비콘의 advertising 패킷을 복제하여 원본 비콘을 가장할 수 있다. 이러한 취약점을 이용해 공격자는 비콘을 이용해 단순하면서도 확장성이 뛰어난 covert 통신이 가능하다. 최근 IoT 생태계에 BLE 비콘을 도입하고자 하는 연구는 많은 관심을 얻었으나, 비콘 보안 강화 연구도 함께 이루어져야 할 것이다.

Ⅶ. 결론 및 향후 연구

Covert 채널은 다수 연구되고 있으나, 블루투스를 활용한 covert 채널 연구는 활성화되지 않았다. 그러나 블루투스는 우리 실생활에 밀접하게 연관되어 있으며 covert 채널의 악용 가능성을 부정할 수 없다. 본 논문에서는 iBeacon의 페이로드와 advertising 인터벌을 활용한 covert 채널의 가능성을 입증하고 평가하였다. 설계된 CSC를 PDR과 처리량 측면에서 평가한 결과, 전체적으로 PDR은 75% 이상으로 일관되게 유지되었으며 PDR 대비 가장 높은 처리량을 가지는 advertising 인터벌은 기본 advertising 인터벌인 100ms와 유사하였다. 설계된 CTC는 메시지를 모스 부호로 인코딩하여 특정 인터벌 값으로 치환한 뒤, 50번 반복하여 전송하였을 때 44번 식별 가능해 88%의 정확도로 메시지를 송·수신할 수 있음을 보여주었다.

본 논문에서는 iBeacon을 기준으로 실험하였으나, Eddystone을 비롯한 다른 비콘에서도 covert 채널을 구축할 수 있을 것이다. 일상생활뿐만 아니라 산업 환경에서도 수많은 블루투스 기기가 존재하고 있으므로, BLE 비콘 메시지나 프로토콜의 고유 파라미터에 대한 보안을 강화해야 한다. 예를 들어 인증 시스템을 도입해 비인가된 장치로부터 BLE 비콘을 조작할 수 없도록 할 수 있다. 또한, 실험 결과 비콘의 특성을 이용하여 많은 양의 데이터를 은밀하게 송수신할 수 있음을 보여주었다. 향후 연구에서는 비콘 covert 채널을 방지하기 위한 대책을 연구할 예정이다.

참 고 문 헌

[1] Tian, J., Xiong, G., Li, Z., & Gou, G. (2020). A survey of key technologies for constructing network covert channel. Security and Communication Networks, 2020, 1-20.

[2] Saenger, J., Mazurczyk, W., Keller, J., & Caviglione, L. (2020). VoIP network covert channels to enhance privacy and information sharing. Future Generation Computer Systems, 111, 96-106.

[3] Schmidbauer, T., Keller, J., & Wendzel, S. (2022). Challenging channels: Encrypted covert channels within challenge-response authentication. In Proceedings of the 17th International Conference on Availability, Reliability and Security, 1-10.

[4] Li, Y., Zhang, X., Xu, X., & Tan, Y. A. (2020). A robust packet-dropout covert channel over wireless networks. IEEE Wireless Communications, 27(3), 60-65.

[5] Claeys, T., Rousseau, F., Simunovic, B., & Tourancheau, B. (2019). Thermal covert channel in Bluetooth low energy networks. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 267-276.

[6] Gnad, D. R., Nguyen, C. D. K., Gillani, S. H., & Tahoori, M. B. (2021). Voltage-based covert channels using FPGAs. ACM Transactions on Design Automation of Electronic Systems (TODAES), 26(6), 1-25.

[7] Coyac-Torres, J. E., Rivero-Angeles, M. E., & Aguirre-Anaya, E. (2021). Cognitive radio based system for best effort communications in sound-based covert channel for iot environments. Mobile Networks and Applications, 26, 1449-1460.

[8] Maiti, A., & Jadliwala, M. (2019). Light ears: Information leakage via smart lights. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3(3), 1-27.

[9] ABiresearch Hompage, https://www.abiresearch.com/press/bluetooth-iot-market-set-nearly-quadruple-2024-smart-home-exceeds-800-million-device-shipments/, last accessed 2023/10/03

[10] Mackey, A., Spachos, P., Song, L., & Plataniotis, K. N. (2020). Improving BLE beacon proximity estimation accuracy through Bayesian filtering. IEEE Internet of Things Journal, 7(4), 3160-3169.

[11] Hernandez-Rojas, D. L., Fernandez-Carames, T. M., Fraga-Lamas, P., & Escudero, C. J. (2017). Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications. Sensors, 18(1), 57.

[12] https://developer.apple.com/ibeacon/, last accessed 2023/10/03

[13] https://github.com/google/eddystone, last accessed 2023/10/03

[14] Kolias, C., Copi, L., Zhang, F., & Stavrou, A. (2017). Breaking BLE beacons for fun but mostly profit. In Proceedings of the 10th European Workshop on Systems Security, 1-6.

[15] Priest, J., & Johnson, D. (2015). Covert channel over Apple iBeacon. In Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 51

[16] Na, X., Guo, X., He, Y., & Xi, R. (2021). Wi-attack: Cross-technology impersonation attack against iBeacon services. In 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 1-9.

[17] Qian, Y., Sun, T., Li, J., Fan, C., & Song, H. (2016). Design and analysis of the covert channel implemented by behaviors of network users. Security and Communication Networks, 9(14), 2359-2370.

[18] Zhang, C., Zhu, L., Xu, C., Zhang, Z., & Lu, R. (2023). EBDL: Effective blockchain-based covert storage channel with dynamic labels. Journal of Network and Computer Applications, 210, 103541.

[19] Seong, H., Kim, I., Jeon, Y., Oh, M. K., Lee, S., & Choi, D. (2022). Practical covert wireless unidirectional communication in IEEE 802.11 environment. IEEE Internet of Things Journal, 10(2), 1499-1516.

[20] Zhang, Q., Zhang, X., Xue, Y., & Hu, J. (2020). A stealthy covert storage channel for asymmetric surveillance VoLTE endpoints. Future Generation Computer Systems, 102, 472-480.

[21] Zhang, X., Guo, L., Xue, Y., & Zhang, Q. (2019). A two-way VoLTE covert channel with feedback adaptive to mobile network environment. IEEE Access, 7, 122214-122223.

[22] Al-Eidi, S., Darwish, O., & Chen, Y. (2020). Covert timing channel analysis either as cyber attacks or confidential applications. Sensors, 20(8), 2417.

[23] Berk, V., Giani, A., & Cybenko, G. (2005). Detection of covert channel encoding in network packet delays.

[24] Cabuk, S., Brodley, C. E., & Shields, C. (2004). IP covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security, 178-187.

[25] Cabuk, S. (2006). Network covert channels: Design, analysis, detection, and elimination (Doctoral dissertation, Purdue University).

[26] Han, J., Huang, C., Shi, F., & Liu, J. (2020). Covert timing channel detection method based on time interval and payload length analysis. Computers & Security, 97, 101952.

[27] Griffiths, S., Wong, M. S., Kwok, C. Y. T., Kam, R., Lam, S. C., Yang, L., ... & Lu, K. (2019). Exploring bluetooth beacon use cases in teaching and learning: Increasing the sustainability of physical learning spaces. Sustainability, 11(15), 4005.

[28] Gast, M. S. (2014). Building applications with iBeacon: proximity and location services with bluetooth low energy. 1st ed. O'Reilly Media, Inc.;

[29] Dalkilic, F., Cabuk, U. C., Arikan, E., & Gurkan, A. (2017). An analysis of the positioning accuracy of iBeacon technology in indoor environments. In 2017 International Conference on Computer Science and Engineering (UBMK), IEEE, 549-553.

[30] Apple: Getting Started with iBeacon Version 1.0. (2014)

[31] Gao, J., Li, Y., Jiang, H., Liu, L., & Zhang, X. (2019). An RTP extension for reliable user-data transmission over voip traffic. In Security and Privacy in Social Networks and Big Data: 5th International Symposium, SocialSec 2019, Copenhagen, Denmark, July 14-17, 2019, Revised Selected Papers 5, Springer Singapore, 74-86.

[32] Zhang, X., Tan, Y. A., Liang, C., Li, Y., & Li, J. (2018). A covert channel over volte via adjusting silence periods. IEEE Access, 6, 9292-9302.

[33] Zi, X., Yao, L., Pan, L., & Li, J. (2010). Implementing a passive network covert timing channel. Computers & Security, 29(6), 686-696.

[34] Archibald, R., & Ghosal, D. (2012). A covert timing channel based on fountain codes. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 970-977.

[35] Bluetooth SIG Proprietary: Bluetooth Core Specification 5.0. (2016)

[36] Shan, G., & Roh, B. H. (2018). Advertisement interval to minimize discovery time of whole BLE advertisers. IEEE Access, 6, 17817-17825.

[37] Bluez Homepage, http://www.bluez.org/about/, last accessed 2023/10/03

[38] Ameri, A., & Johnson, D. (2017, March). Covert channel over network time protocol. In Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, 62-65.

[39] https://support.kontakt.io/hc/en-gb/articles/4413251557650-Advertising-Interval-best-practices, last accessed 2023/10/03

[40] Jeon, K. E., She, J., Soonsawad, P., & Ng, P. C. (2018). Ble beacons for internet of things applications: Survey, challenges, and opportunities. IEEE Internet of Things Journal, 5(2), 811-828.

ABSTRACT

Implementation and security implication analysis of covert channel using iBeacon

Ye-Sol Oh

Department of Future Convergence
Technology Engineering
Graduate School of
Sungshin Women's University

Covert channels are typically employed to transmit information and bypass security policies and controls simultaneously to maintain undetected communication. Various techniques have been proposed for establishing covert channels, including those at the network level, and for using different components. While Bluetooth-based covert channels have been studied, discussions regarding covert channels utilizing beacons have been limited. Moreover, traditional covert channels have faced a trade-off between secrecy and bandwidth. This study review the security of Apple's iBeacon broadcast messages with a focus on building covert channels, analyze vulnerabilities, implement two types of BLE covert channels, and evaluate their performance. This study introduces two BLE(Bluetooth Low Energy) covert

channels: one using advertising payloads and the other employing advertising intervals. These channels can be used in a complementary manner, balancing covertness and bandwidth. In our evaluation, the payload-based covert channel achieved a maximum throughput of 911,600 Bps(Bytes per second) with a PDR(Packet Delivery Rate) exceeding 75%, demonstrating its capability to transmit substantial data via iBeacon covertly. Additionally, by utilizing CTC, receivers could identify secret messages with an accuracy of 88% when repeatedly transmitted. This indicates the potential for providing services to legitimate users while also highlighting the risk of malicious users exploiting covert channels to leak information. This study presents the possibility of a Bluetooth relay attack using the beacon covert channel and emphasizes the importance of strengthening BLE beacon security.

ACKNOWLEDGEMENTS

본 논문을 지도해주신 이일구 교수님과 최현우 박사님, 연구에 도움을 준 공저자 이연지, 장지원 학생에게 감사드립니다.