이 일 구 교수 지도
석사학위 청구논문

모바일 보안 구역을 위한 협력 친화적 방해 전파 기술

2023

성신여자대학교 대학원
미래융합기술공학과
전 가 혜

모바일 보안 구역을 위한
협력 친화적 방해 전파 기술

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2023년 5월

성신여자대학교 대학원

미래융합기술공학과

전 가 혜

인 준 서

전가혜의 석사학위 논문으로 인준함

2023년 5월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 김 경 진 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

성신여자대학교 일반대학원

논 문 개 요

무선 통신 기술이 발전함에 따라 시공간의 제약 없이 고용량 데이터를 고속으로 송수신할 수 있게 되면서, 사이버 위협에 따른 도청과 정보 유출의 피해가 증가하고 있다. 특히, 전 산업 분야에서 활용되고 있는 사물인터넷은 일반적으로 개방형 네트워크 환경에서 불특정 다수에게 동시에 데이터를 보내는 브로드캐스트 통신을 하기 때문에 스니핑이나 재밍 공격에 취약하다. 종래 연구에서는 무선 통신 기술의 안전한 통신 채널 확보를 위해 시간, 주파수, 공간 영역에서 보안성을 개선한 프로토콜을 제안해왔다. 하지만 복잡한 하드웨어가 필요하기 때문에 이동 통신 네트워크와 사물인터넷에 적용하기 어렵다. 이에 종래 무선 통신 네트워크의 기술적 한계를 극복하기 위해 경량성과 이동성을 개선한 새로운 보안 모델이 요구된다. 본 논문에서는 자율 이동체인 드론을 대상으로 인공 노이즈와 기기의 이동성을 활용하여 협력적 우호 재밍을 수행하는 보안 모델을 제안하고, 시뮬레이션과 필드 테스트를 통해 도청 위협 방지 효과와 보안성 향상 효과를 입증하였다. 드론 기반의 모바일 보안 구역 기법(CFJ-DMZ)은 우호적 재머를 통해 보호 대상 위치에 따른 보안 구역을 설정하여 안전한 무선 이동 통신 네트워크를 지원할 수 있으며, 도청 위협을 효과적으로 경감할 수 있다. 본 연구의 실험 결과에 따르면, CFJ-DMZ가 적용된 시나리오에서 도청자들의 평균 Information Leakage Rate (ILR)은 3% 이하로 종래의 방식대비 평균적으로 92% 개선되었다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

무선 네트워크 기술은 고속 고용량 멀티미디어 콘텐츠를 장소와 시간의 제약없이 이용하고 싶은 사용자의 요구를 충족시키기 위해 진화하고 있다. 하지만 도청에 취약한 무선 통신이 갖는 근본적인 한계로 인해 정보가 유출되는 사례가 계속되고 있다[1]. 도청으로 인한 정보 유출 문제를 해결하기 위해 시간, 주파수, 공간 영역에서 안전한 통신채널을 확보하거나 보안성을 개선한 프로토콜과 매커니즘이 제안되었다[2]. 그러나 종래 무선 통신 보안 방법들은 복잡한 하드웨어가 필요하고, 에너지 효율과 데이터 전송 성능을 저하시키기 때문에 기밀 정보를 교환하는 경량의 고신뢰 무선 자율이동체에 적용하는데 한계가 있다[3, 24].

무선 네트워크 기술 중 사물 인터넷(Internet of Things, IoT)이 전 산업과 일상생활의 필수 요소가 됨에 따라 사물 인터넷들을 연결해주는 무선 네트워크의 보안 취약점이 더 큰 이슈가 되고 있다[4]. 기존 무선 통신 체계는 물리계층에서 발생하는 물리적 정보와 헤더 정보를 활용하는 공격, 부채널 공격(side-channel attack) 등의 공격들에 취약하기 때문에 통신 과정 중 보안 프로토콜 키가 유출되어 암호화가 무력화될 수 있다. 하지만 대다수의 사물인터넷은 일반적인 PC나 모바일 기기에서 활용하는 보안 매커니즘을 적용하기에는 부족한 사양을 가진 경량의 기기들이며, 공개된 네트워크 환경에서 통신하기 때문에 도청과 같은 보안 위협에 노출되기 쉽다. 이러한 취약점을 이용해 사용자 기밀 정보를 쉽게 수집할 수 있다[5].

이와 같은 보안 위협에 노출되기 쉬운 사물인터넷 환경에서 보안성을 향상시키기 위해서는 모바일 사물 인터넷 장치의 경량성과 이동성을 고려하여 보안아키텍처를 설계해야 한다[6]. 본 논문에서는 무선 통신 환경에서 보안성을 향상시키기 위해 협력적 우호 재밍 신호를 송출하는 드론을 이용한 모바일

보안 구역 기법(CFJ-DMZ, Cooperative Friendly Jamming Techniques for Drone-based Mo-bile Secure Zone)을 제안한다. 도청은 공격 증거를 남기지 않는 수동적인 공격이기 때문에 무선 통신 환경에서 도청자를 탐지하는 것은 매우 어렵다. 따라서, 본 연구에서는 불특정한 잠재적 도청자의 도청 확률을 줄이는 사전 예방 방법을 제안했다. CFJ-DMZ 기법은 자율이동체의 이동성(Mobility)과 인공잡음(Artificial Interference)을 활용해 보안 구역(Secure Zone)을 형성하여 모바일 사물인터넷 무선 통신 환경에서도 안전한 데이터 통신을 보장하고, 보호하고자 하는 구역을 유연하게 제어하여 도청 위협을 효과적으로 경감할 수 있다.

제안하는 CFJ-DMZ 기법을 평가하기 위해 네트워크 시뮬레이션 모델을 구현하여 성능을 검증했다. 이 네트워크 시뮬레이션 모델은 송신 노드가 수신 노드의 주변으로 이동한 후, 협력적 재머 드론이 형성한 보안 구역 내에서 안전한 근거리 Device to Device (D2D) 통신을 수행한다. 이 때, 3개의 드론이 서로 통신하며 인공 잡음 신호 도달 범위 경계를 기반으로 보안 구역을 생성하여 노드 간 통신의 기밀성을 보호한다. 또한, 현장 실험을 통해 CFJ-DMZ 기법의 효과성을 분석했다.

이 문서의 주요 기여점은 다음과 같다.

- 모바일 사물인터넷 장치의 경량성과 이동성을 고려하여 인접한 드론들이 기밀통신을 위한 Secure Zone을 유연하게 형성하는 협력적 재밍 기법을 제안했다.
- 제안된 CFJ-DMZ의 효과를 시뮬레이션과 현장 실험을 통해 분석, 입증했다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 기존 무선 통신 보안 기술과 자율 이동체의 무선 통신 보안에 대한 주요 연구를 소개한다. Ⅲ장에서는 Friendly jamming 보안 성능 기준과 Friendly jamming모델에 대해 서술한

다. Ⅳ장에서는 CFJ-DMZ모델을 제안하며, Ⅴ장에서는 제안 모델의 보안 성능을 시뮬레이션과 현장 실험을 통해 입증한다. 마지막으로, Ⅵ장에서는 결론과 향후 연구방향에 대해 서술한다.

Ⅱ. 관련 연구

Wyner은 도청 채널 연구에서 보안 채널 용량이라는 개념을 정의하고, 정보 이론 관점에 따라 도청자의 도청 채널이 합법적인 리시버에 비해 품질이 저하 될 경우 기밀 보안 달성이 가능함을 증명했다[7]. 보안 채널 용량(Secrecy Capacity)은 합법적인 송신자와 합법적인 수신자간의 채널 용량과 합법적인 송신자와 도청자간의 채널 용량의 차이로 정의된다. 만약 합법적인 송신자와 도청자간의 채널 용량이 합법적인 송신자와 합법적인 수신자간의 채널 용량보다 커서 보안 채널 용량이 음수이면 보안 채널 용량은 0이다. 이는 합법적인 송신자가 합법적인 수신자에게 안전하게 보낼 수 있는 정보가 없음을 의미한다. 이 때, 합법적인 수신자의 채널 품질은 좋게 하고, 도청자의 채널 품질을 나쁘게 하여 안전한 통신을 수행하기 위해 신호와 인공적인 잡음을 이용할 수 있다. 무선 통신의 보안성 향상을 위한 빔 형성 재밍기법, 릴레이 재밍기법, 우호적 재밍 기법 등 다양한 재밍 기법 연구가 진행되었다. 최근에는 악의적인 도청자의 도청 성능을 저하시킬 수 있는 재밍 신호를 다중 안테나와 결합하여 빔을 형성하면 합법적인 통신자들 간의 통신 보안성과 신뢰성을 크게 향상시킬 수 있음이 입증됐다. 하지만, 다중 안테나 혹은 massive antenna를 활용한 빔포밍 기술은 복잡하고 파워 소모량이 커서 사물인터넷이나 모바일 장치에 활용하기 어렵다[8,9].

재밍 신호를 보안 목적으로 활용하기 위한 우호적 재밍 보안 기법에 대한 여러 연구가 진행되고 있다[10-17]. 우호적 재밍 기법은 송신자가 합법적인 수신자와 통신하는 동안 악의적인 도청자가 엿듣는 것을 방해하기 위해 우호적인 인공잡음 신호를 방출하는 방법이다. 재머를 이용하여 무선 통신 네트워크를 보호하고 메시지를 기밀하게 전송하여 합법적인 송수신자가 안전하게 통신할 수 있도록 한다. 우호적 재밍 보안 기법 중 무선 통신 네트워크에서

이동체 간에 안전하게 정보를 전달하기 위해 다수의 우호적 재머를 자동으로 배열하는 간섭취소기법(Anti-Jamming)을 활용하는 방법도 제안되었다 [15-17].

이동 통신 네트워크에서 다중 무인 항공기(Unmanned Aerial Vehicle, UAV)를 활용한 Friendly-Jamming 보안 모델 연구가 진행되고 있다. Friendly UAV Jamming (Fri-UJ) 기법은 다중 무인 항공기 재머가 방해 전파를 송출해 도청 장치의 신호 대 간섭 및 노이즈 비율(Signal-to-Interference-plus-Noise Ratio, SINR)을 저하시켜 도청 확률을 낮추는 기법이다. 이때, 보안 영역 인근에 배치된 재머의 수가 많을수록 도청 확률이 낮아진다[18]. 또한 의료 분야에서 사용하는 사물인터넷에 적용하여 Fri-UJ의 효과성을 입증한 연구가 있다[25]. 그러나 현실적으로 무한 대의 다중 무인 항공기 재머 설치는 어렵고, 다중 무인 항공기 재머의 수가 많을수록 손실 비용이 크다. 또한, 재머의 개수가 늘어날수록 섬세한 보안 영역을 생성할 수 있지만 여러 대의 재머를 사용할수록 재밍 신호가 중첩되는 영역이 증가하여 보안 영역을 생성하는데 비용 대비 효율성이 떨어진다. 그러므로 보안 영역의 크기와 재머의 수, 비용 대비 보안 효율성을 기준으로 이동 통신 환경에서의 효과적인 Friendly-jamming 모델을 비교, 분석하고 제안하는 연구가 필요하다.

재머 역할인 무인 항공기 위치 관련 연구도 진행되고 있다. 드론의 위치는 사용자에게 제공하는 서비스의 질이나 사용자 대기 시간 및 지연과 관련있는 중요한 요소이다[26]. 또한, 우호적 재밍 신호를 이용하여 지상에 위치한 합법적 노드를 보호하기 위한 방해 전력 세기, 전력 궤적 경로에 대해 연구가 있다[27]. [27]의 제안 모델은 도청자의 위치를 계산하여 추정하는데, 실제 상황에서는 도청자의 위치를 파악하기는 매우 어려우므로 현실 적용 가능성이 낮다. 이에 [28]에서는 도청자의 특정 위치를 파악하는 것이 아닌 무작위성을

모델링한다. 이때, 합법적인 여러 수신기의 기밀 비율을 최대화하기 위해 신호 대 간섭비를 이용하여 영역을 결정한다. 하지만 보안 영역 내 수신기의 기밀성이 동일하게 보장되지 않아 일부 기기의 도청가능성은 높은 상태로 남아 있을 수 있다. 또한 무인 항공기의 최적 위치가 결정되면 상황에 따라 일부만 변경되므로 영역이 유연하지 못하고 무인 항공기의 이동성을 활용하지 못했다. 그리고 데이터의 송수신이 진행되지 않을 때에도 항상 재밍 신호를 송출해야 하므로 배터리 사용도 비효율적이다.

Table 1은 friendly jamming과 관련된 선행 연구들을 정리한 표이다. 표의 저자는 선행 연구의 1저자이고, 재머 수는 선행 연구 제안 모델에서 사용한 jammer의 수를 의미한다. Single은 1 대의 jammer를 사용한 모델이고, Multiple은 2대 이상의 jammer를 이용한 모델이다. UAV 이용은 선행 연구 제안 모델에서 무인 항공기(UAV) 이용 여부를 의미하며, X는 무인 항공기를 이용하지 않은 모델이고 O는 무인 항공기(UAV)를 재머로 사용한 모델이다. 기여점은 각 논문에서 제안한 모델의 주요 내용이고 한계점은 각 논문의 한계점에 대한 분석 결과이다. 종래의 연구들은 파워 소모량이 커서 경량 장치에 적용하기 어렵고, 이동성이 없어 안전한 무선 통신을 위한 보안 영역 생성에 비효율적이고 유연하지 않다. 하지만 본 연구에서는 우호적 재밍 신호를 송출하는 3대의 드론만 이용하여 효율적이며 유연한 보안 영역을 생성하는 모델을 제안하며, 시뮬레이션과 현장 실험을 통해 그 모델의 효과성을 입증했다.

TABLE 1. Comparison of Friendly-Jamming prior study

저자	재머 수	UAV 이용	기여점	한계점
Bakr. O.[8]	Single	X	• 도청자의 수신 성능 저하를 위한 재밍 신호 송출 • 다중 안테나 이용 재밍 신호 송출	• 기술복잡성과 파워 소모량 큼 • 사물인터넷 적용 어려움
Cumana. K.[9]		X	• 도청자의 수신 성능 저하를 위한 재밍 신호 송출 • Massive Antenna 빔포밍 이용 재밍 신호 송출	• 기술 복잡성과 파워 소모량 큼 • 사물인터넷 적용 어려움
Vilela[11]		X	• Relay aided single input - single output 네트워크 환경에서 협력적 재밍 신호 이용 • 협력 재머의 표준 운영절차(SOP) 성능 향상을 위한 시뮬레이션 실시	• 합법적 기기의 통신 보호 요청 시 기밀 통신 보장을 위한 연구 필요

Giti[13]	Multiple	X	• Static wiretap fading channel 에서 협력적 재밍 신호 이용	• Mobile 환경에서 재밍 신호 이용 연구 필요
Lohanna. P.[28]		O	• 3D 공간 가정 UAV 배치 • 도청자 위치 파악 없이 합법적 수신기의 비밀 비율 최대화 전략	• 보안 영역 내 합법적 수신기의 기밀성 동일하게 보장 안됨 • 비밀 비율 최대화 상태 결정 후 UAV 위치 변경 없음
Kim[15]		X	• Wi-Fi 환경에서 WPA2 enter-prise mode 통한 협력적 재밍 신호 이용	• Mobile 환경에서 재밍 신호 이용 연구 필요
Yaacoub [16]		X	• MIMO 빔포밍 협력적 재밍 신호 이용 • Cylindrical antenna 정렬	• 재머의 적절한 배치 위치 연구 필요

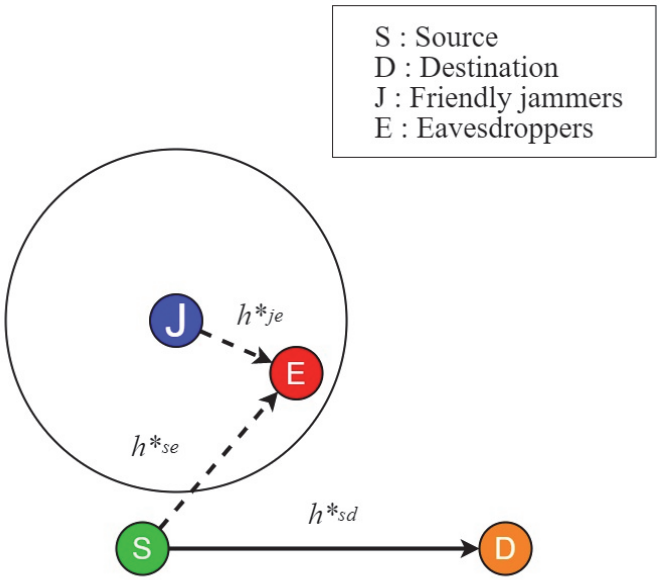
Qubeijian. W. [18]		O	• 도청자의 신호 대 간섭 및 노이즈 비율 (SNIR) 저하시켜 도청 확률을 낮춤 • 사물인터넷 이동 통신 네트워크 환경에서 UAV 이용 재밍 기법(Fri-UJ) 제안	• 재머인 UAV 수에 대한 연구 없음
Xai. L.[25]		O	• 의료 분야 사물인터넷에 Fri-UJ[18] 기법 적용 후 효과성 입증	• 재머인 UAV 수에 대한 연구 없음

Ⅲ. Friendly-Jamming Technique

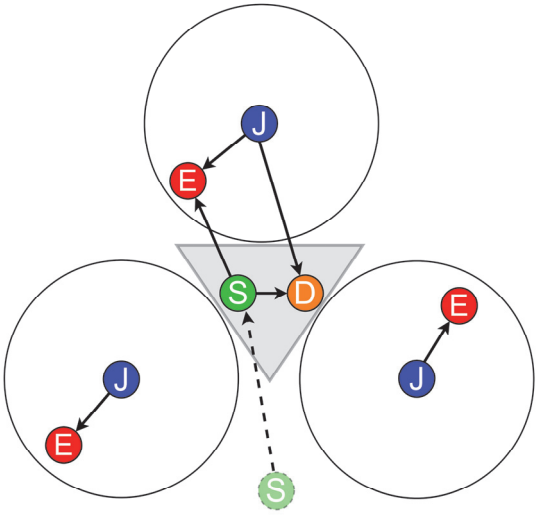
Friendly jamming의 보안 성능 평가 지표로 Information Leakage Rate(ILR) metrics을 수식 (1)과 같이 정의했다. 정보 유출 비율 ILR은 Bit Error Rate (BER)과 Friendly-Jamming 간의 관계로 정의하였다. BER이 0.5를 초과하면 비트 에러율이 높아 정보 추출이 불가능함을 의미하므로 ILR은 0이다[19-21]. 반면, BER이 0.5 이하이면 비트 에러율이 낮아 정보 추출이 가능함을 의미하므로 ILR은 0이상의 값을 가진다. BER 값이 작을수록 ILR은 큰 값을 가지고, ILR 값이 클수록 보안성이 낮아 많은 정보가 추출 가능함을 의미한다.

$$ILR = 0, \ if \ BER > 0.5$$
$$ILR = 1 - \frac{BER}{0.5}, \ if \ BER \leq 0.5 \quad (1)$$

Fig.1 Friendly jamming의 보안 성능을 검증하기 위한 네트워크 구성이다. Fig.1(a)는 드론이 재머의 역할을 하는 우호적 재밍 기법 모델이다. 단일 안테나를 사용하는 송신 노드(Source, S)는 수신 노드(Destination, D)에 공개된 채널을 통해 데이터(h_{sd}^{*})를 전송한다. 이때, 공개된 채널을 통해 데이터를 송신하므로 도청 장치(Eve, E)도 같은 데이터(h_{se}^{*})를 수신한다. 송신 노드 근처에 위치한 드론(Jammer, J)은 friendly jamming 신호(h_{je}^{*})를 송출하여 jamming 영역을 형성한다. 우호적 재밍 영역 내 도청 장치는 재밍 신호의 영향으로 도청 품질이 떨어져 도청 가능성이 낮아진다.



(a)



(b)

FIGURE 1. Network configuration for friendly jamming; (a)friendly jamming model, (b)CFJ-DMZ model

Ⅳ. CFJ-DMZ Model

본 장에서는 기기의 이동성과 friendly-jamming기법을 이용하여 보안구역을 형성하는 CFJ-DMZ모델을 소개한다. 세 대의 드론은 Secure Zone 외부에 재밍 신호를 송출한다. 이러한 협력적 재밍 신호는 도청자의 도청 확률을 줄이고 Secure Zone 에서 합법적인 송수신자간의 보안 통신이 가능해진다.

Fig.1(b)는 본 논문에서 제안하는 CFJ-DMZ 모델이다. CFJ-DMZ네트워크는 송신 노드(S)와 수신 노드(D), 임의의 도청자(E)와 세 대의 우호적 재밍 드론(J)으로 구성된다. 드론은 Fig.1(b)와 같이 Secure Zone을 형성한 후 Secure Zone 외부에 재밍 신호를 송출한다. 저전력 경량 드론은 다중 안테나 통신 인터페이스를 이용하기 어렵기 때문에 본 연구에서는 하나의 안테나를 이용하여 무선 통신 한다. 합법적인 송신 노드와 수신 노드는 Secure Zone 내부에서 D2D 통신을 한다. 송신 노드가 수신 노드의 위치로 이동하여 두 기기간 거리가 가까워졌기 때문에 송신 노드의 데이터 전송 신호 세기가 감소한다.

Fig.2는 CFJ-DMZ 모델의 시나리오 흐름도이다. CFJ-DMZ는 보안 영역 형성, 재밍 신호 송출, Secure Zone 내 통신 순의 3단계로 수행된다.

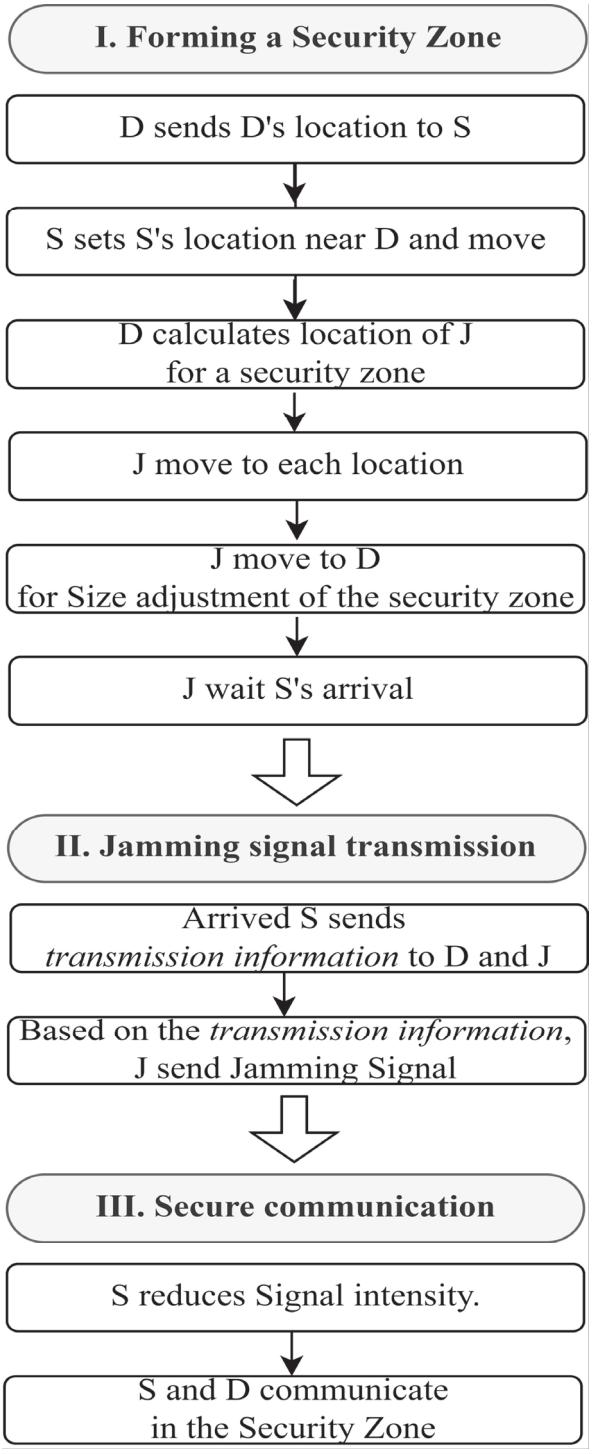
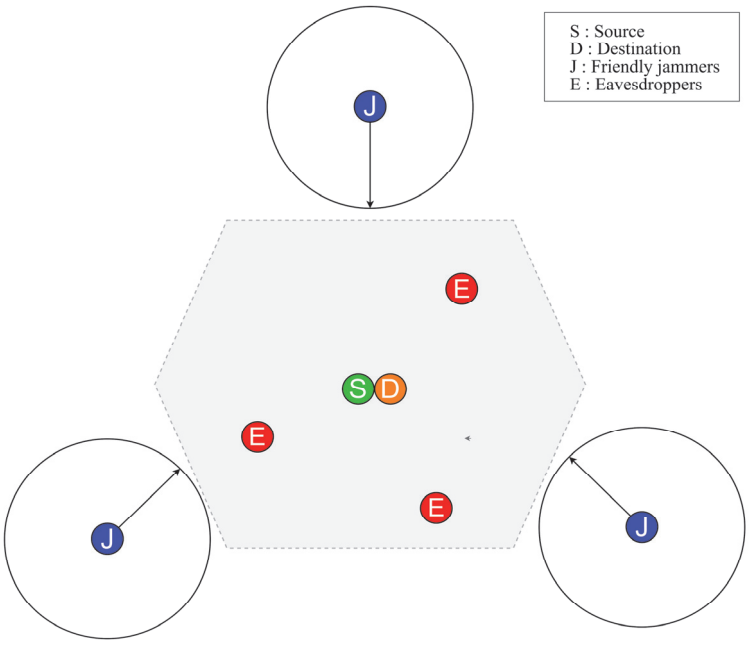


FIGURE2. CFJ-DMZ Flow Chart

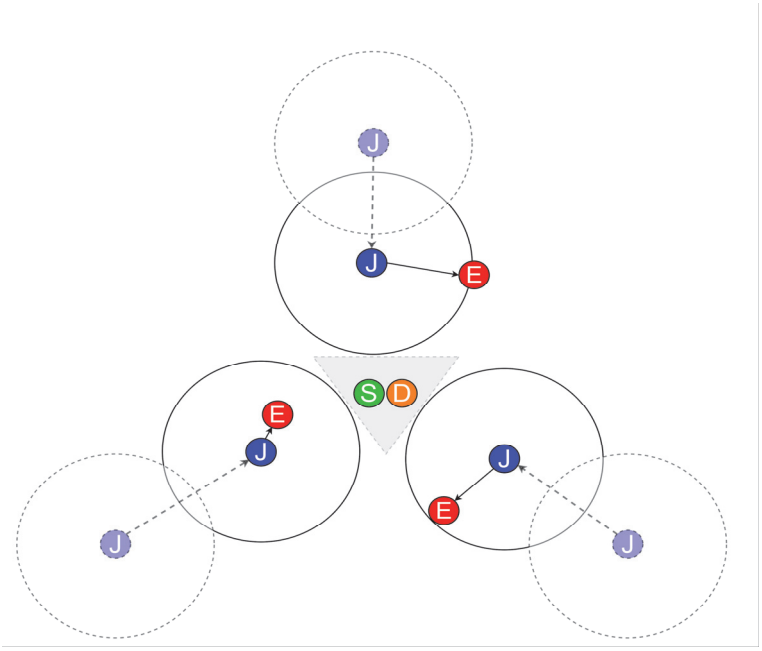
첫 번째 단계는 세 대의 드론을 이용하여 보안구역을 형성하는 단계이다. 기기 간 통신이 결정되면, 수신자(D)는 송신자(S)에 GPS를 이용하여 자신의 위치 좌표 정보를 전달한다. D의 위치좌표를 전달받은 S는 D의 주변으로 자신의 위치좌표를 결정한다. S는 결정한 위치정보를 D에 전달하고, 결정한 위치로 이동한다. D는 S의 도착 좌표 정보와 D의 현재 좌표 정보를 활용하여 드론(J)들의 위치를 계산한다. D는 본인 위치를 중심으로 가상의 원을 생성한다. 이때, J의 재밍 신호 송출 세기에 따라 최대 신호 송출 가능한 거리를 x라 할 때, D가 본인 위치를 중심으로 생성한 가상의 원의 반지름은 수식(2)와 같다.

$$Radius = \frac{2}{3}\sqrt{3}x \tag{2}$$

D는 자신의 위치를 중심으로 생성된 가상의 원 위에 정삼각형을 만드는 임의의 세 점을 선택하고, 선택한 위치를 3대의 J에 각각 전달한다. 각각의 J는 전달받은 각자 위치로 이동한다. 각자 위치에 도착한 J는 Fig.3과 같이 재밍 신호를 송출하여 서로의 재밍 신호가 잡히지 않는 위치까지 D쪽으로 이동하며 Secure Zone 크기를 조정한다. J가 재밍 신호 세기에 따른 최대 신호 송출 가능 거리에서 D쪽으로 이동하였으므로, Fig.3에서 회색 영역인 Secure Zone의 크기가 Fig.3(a)에서 Fig.3(b)로 작아진다. 그 결과, Fig.3(a)의 Secure Zone 내부에 있던 도청자 E가 Fig.3(b)에는 Secure Zone 외부에 있다. 이처럼 Secure Zone의 크기 조정은 Secure Zone 내부에 도청자가 있을 확률을 줄인다. 또한, Fig.3(b)와 같이 합법적 노드 주변 도청 가능성이 높은 도청자에 직접 재밍 신호를 송출하여 도청 품질을 떨어트려 도청 가능성을 줄인다. 서로의 재밍 신호를 수신한 J는 Secure Zone을 만들기 위한 최적의 위치를 결정하고, S가 D 주변 최종 목표 좌표에 도착할 때까지 재밍 신호 송출을 중단하고 대기한다.



(a)



(b)

FIGURE 3. Size adjustment of The Security Zone; (a)before, (b)after

두 번째 단계는 재밍신호 송출 단계이다. S가 D 주변 최종 목표 좌표에 도착하면, D와 J에게 재밍 신호 송출 시작 시간과 재밍 신호 송출 유지 시간 정보를 전달한다. 세 대의 J는 시간 정보에 기반하여 동시에 재밍 신호를 송출하고, S와 D는 재밍 신호 송출 유지 시간동안 보안 데이터를 전송할 수 있다. 이처럼 J는 데이터 전송 시간에 맞춰 Secure Zone 내부에서 S와 D의 통신이 이루어질 때만 재밍신호를 송출한다. 데이터 전송과 상관없이 재밍신호를 지속적으로 송출하면, Secure Zone의 내부 보안성은 향상된다. 하지만 지속적인 재밍 신호는 주변의 또 다른 합법적 송수신 개체의 통신을 방해한다[22]. 또한 Secure Zone 내부에서의 통신 여부와 관계없이 지속적으로 재밍 신호를 송출하는 것은 에너지 측면으로도 비효율적이다. 따라서 CFJ-DMZ는 S와 D가 통신할 때만 J가 재밍신호를 송출하여, 주변의 다른 송수신 노드에 끼치는 재밍신호 영향을 최소화하고 배터리를 효율적으로 사용하고자 한다.그리고 Secure Zone 형성만을 위한 목적으로 새로운 UAV를 추가 배치하는 것이 아닌, 기존에 다른 목적으로 사용되는 주변 UAV의 도움을 받아서 기밀 정보를 전송하는 시간에만 Secure Zone을 형성하는 것을 가정한다. 그러므로 본 연구에서는 CFJ-DMZ를 위한 협력적 재밍 드론의 비용을 고려하지 않았다. 물론, 제안하는 CFJ-DMZ 방식을 구현하기 위해 다른 목적으로 사용되고 있던 협력적 재밍 드론들과 사용자 기기에 매우 작은 제어 로직이 추가될 수 있다. 하지만 신호 송출과 기기 이동 기능은 드론의 기본 기능에 포함되어 있는 기능이므로 추가되는 하드웨어 비용은 크지 않다.

마지막으로 S와 D는 J의 재밍신호 송출로 형성된 Secure Zone 내부에서 통신한다. 이때, S와 D의 거리가 가까워졌으므로 S는 송신 신호 세기를 감소한다. 그리고 세 대의 J는 협력적 재밍 신호를 송출한다. 그 결과 도청자의 도청확률을 줄여 Secure Zone에서 기기 간 통신 보안성이 향상된다.

본 논문에서는 CFJ-DMZ 모델의 보안성 입증을 위해 시뮬레이션과 현장 실험을 했다. 시뮬레이션은 Octave를 활용했고, 현장 실험은 raspberry pi 3를 이용했다. Ⅴ장에서는 CFJ-DMZ 모델 보안성 입증 과정과 결과 분석을 다룬다. CFJ-DMZ 모델 보안성 입증은 Secure Zone 내부의 보안성 향상 입증에 초점을 맞췄다. 이에, CFJ-DMZ 시나리오 과정 중 송신 노드의 이동, Secure Zone 형성을 위한 우호적 재밍 드론의 이동 완료를 가정한다.

Ⅴ. Evaluation and Analysis

1. Simulation

1) Effect of Friendly-Jamming

본 논문에서 제안한 CFJ-DMZ 모델은 D2D 무선 통신의 기밀성을 보호하기 위해 세 대의 드론을 우호적 재머로 이용한다. 3대의 드론은 재밍 신호를 외부에 송출하여 2대의 합법적 노드 간의 통신을 보호한다. 본 논문에서는 이론적으로 2차원 영역을 만들 수 있는 가장 적은 수인 3대의 드론을 이용하여 비용-성능 효율적인 Secure Zone을 구성했다. 도청자가 받는 재밍 신호 효과는 송신 노드-도청자간의 거리(Source-Eve distance, dSE)와 재밍 드론-도청자 간의 거리(Drone-Eve distance, dDE)에 영향을 받는다. Fig.4는 시뮬레이션을 이용하여 측정한 dSE와 dDE의 변화에 따른 도청자의 BER이다. 거리를 1m부터 100m 까지 변경하며 도청자의 BER을 측정하였다. 그 결과, 송신노드와 도청자간의 거리(dSE)보다 재밍 드론과 도청자간의 거리(dDE)가 더 가까울 수록, 도청자의 BER이 증가하여 도청자의 통신 품질이 저하됨을 확인하였다.

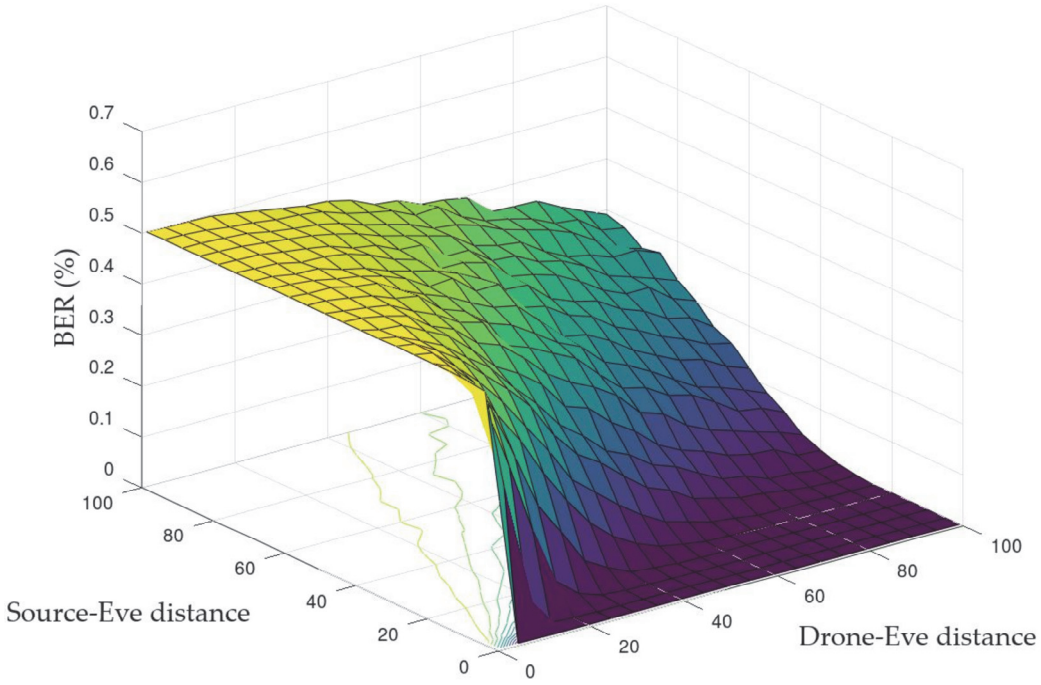


FIGURE 4. BER by each distance of Source-Eve and Drone-Eve

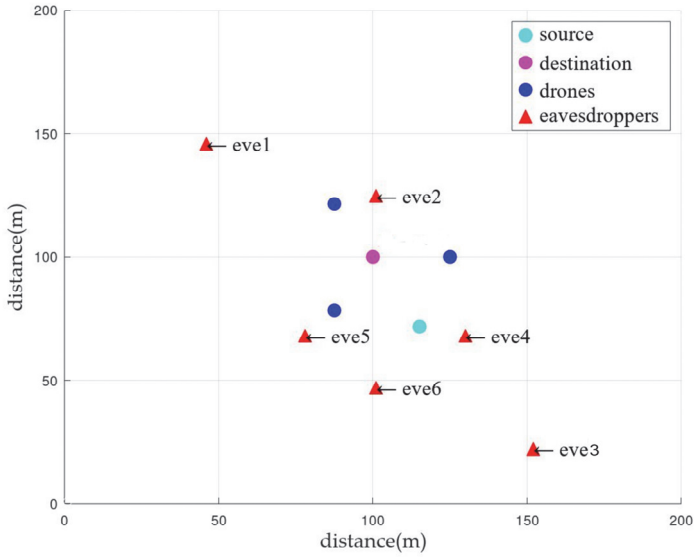
2) Evaluation Environments

Table 2는 Evaluation 환경을 정리한 표이다. 시뮬레이션은 프로그램 Octave를 사용했고, version은 6.1이다. 또한 시뮬레이션 동작에 사용된 CPU는 intel i5-7200U이고, RAM은 8.0GB이다. 시뮬레이션은 200m*200m 규격의 자유공간에 노드를 랜덤하게 배치했다. 실험환경을 자유공간으로 설정하였으므로, 공기나 다른 전파에 의한 영향력은 고려하지 않는다. 또한 시뮬레이션의 송신노드, 수신노드, 우호적 재밍 드론의 최대 전송 전력은 각 24dBm으로 설정했다.

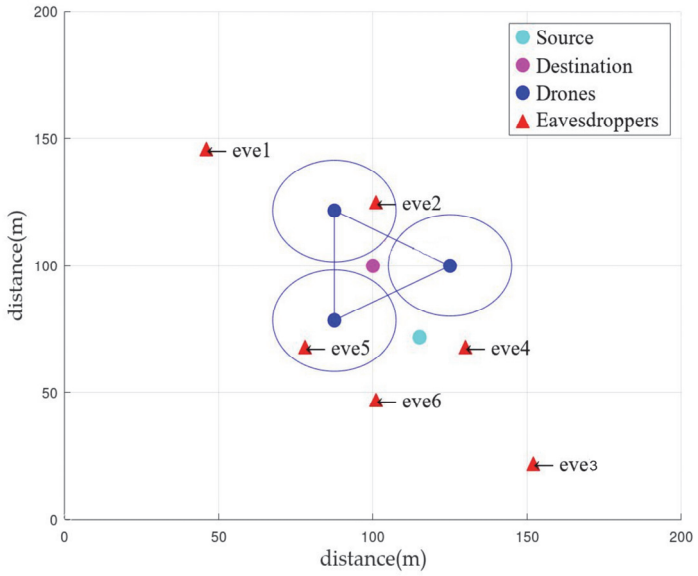
TABLE 2. Evaluation Environments

Simulation		Field Experiment	
Program	Octave 6.1	Device	Raspberry pi 3 Model B+
CPU	intel i5-7200U	CPU	Quad-core 64bit ARMv8
RAM	8.0GB	RAM	1.0GB
공간 규격	200m*200m	공간 규격	50m*50m
최대 전송 전력	24dBm	최대 전송 전력	24dBm

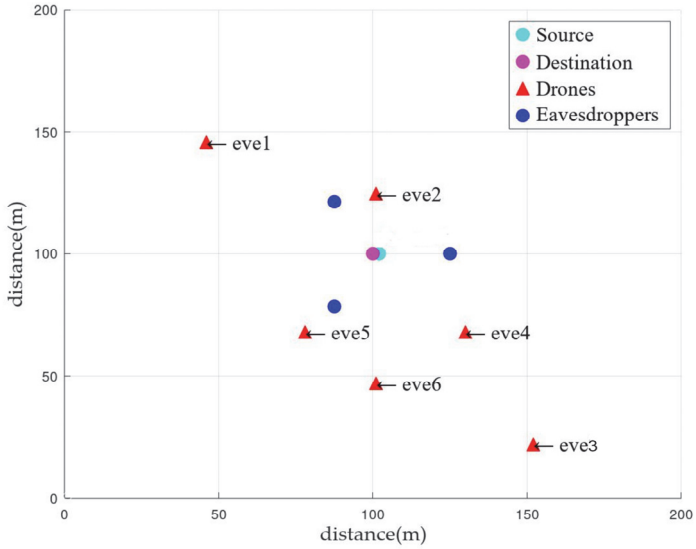
기기의 이동성과 friendly-jamming 기법에 따른 정보 유출량(ILR)을 측정하기 위해 Fig.5와 같이 4가지의 실험 환경을 구성하였다. 송신 노드 (S)와 수신 노드 (D)의 위치를 측정한 후, 세 대의 드론 (J)의 위치를 계산하였다. Fig.5 Case(b)와 Case(d)에서 드론 주변 파란색 원은 협력적 재밍 신호 송출 범위이다. 총 6개의 도청 노드(eve1~6)를 생성하였으며, 도청 노드(E)는 임의의 좌표에 위치한다. 실험 환경 별 효과적인 비교를 위해 도청자의 위치는 모든 실험에서 동일하다. Table 3은 각 노드의 좌표를 정리한 표이다. 본 시뮬레이션 실험에서 Case(a)와 Case(b)의 송신 노드에서 수신 노드까지의 거리는 48.413m이고, 송신 노드(S)가 수신 노드(D) 주변으로 이동한 Case(c)와 Case(d)의 송신 노드에서 수신 노드까지의 거리는 2m 로 설정했다.


source
destination
drones
eavesdroppers
eve1
eve2
eve3
eve4
eve5
eve6
distance(m)
distance(m)
0
50
100
150
200

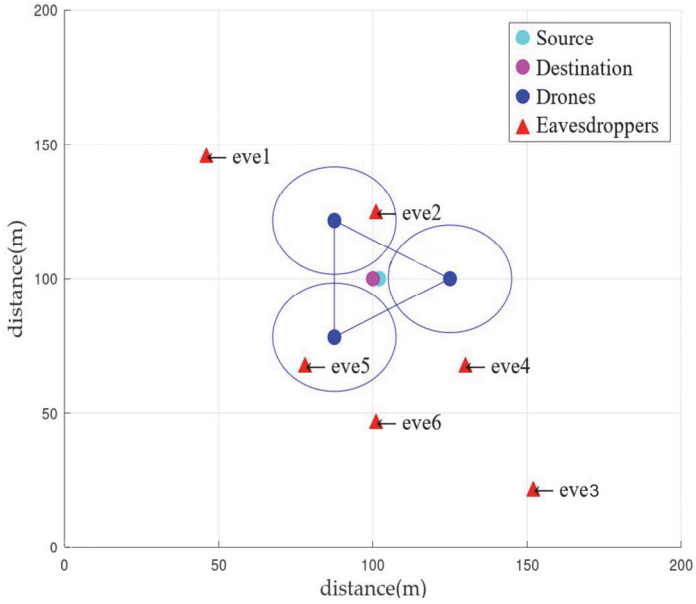
(a)


Source
Destination
Drones
Eavesdroppers
eve1
eve2
eve3
eve4
eve5
eve6
distance(m)
distance(m)
0
50
100
150
200

(b)



(c)



(d)

FIGURE 5. Network configuration for CFJ-DMZ simulation; (a)None mobility and None friendly jamming, (b)None mobility and Friendly jamming, (c)Mobility and None friendly jamming, and proposed scheme (d)Mobility and Friendly jamming

TABLE 3. Location of each Node in simulation

Node	Location
Source in case (a), (b)	(127.42, 60.1)
Source in case (c), (d)	(102, 100)
Destiantion	(100, 100)
eve1	(23, 146)
eve2	(101, 125)
eve3	(155, 22)
eve4	(149, 89)
eve5	(73,71)
eve6	(101, 47)

Fig.5의 실험 환경의 테스트 케이스는 Table 4와 같이 정리 할 수 있다. Mobility는 송신 노드의 움직임 유무이다. Mobility가 O이면 송신 노드가 수신 노드 주변으로 이동한 후 정보를 전달하는 경우이고, X이면 송신 노드가 수신 노드 주변으로 이동하지 않고 정보를 전달하는 경우이다. 송신 노드의 이동성이 있으면 송신 노드와 수신 노드의 거리가 가까워졌으므로 송신 노드의 송신 신호 세기를 감소한다. 즉, Mobility가 O이면 송신 노드의 신호 세기가 감소한 경우이다. 그리고 Friendly jamming은 드론의 friendly-jamming 기법의 이용 유무이다. Friendly jamming에 O이면 정보를 전달할 때 드론이 협력적 재밍 신호를 송출 하는 경우이고, X이면 협력적 재밍 신호를 송출하지 않는 경우이다. Source-Destination distances는 송신 노드와 수신 노드 사이의 거리로, Mobility가 있는 경우 송신 노드가 수신 노드 주변으로 이동해 송신 노드와 수신 노드 간의 거리는 2m이다. 본 논문에서 제안하는 CFJ-DMZ 모델은 Mobility와 Friendly jamming이 모두 존재하는 Case(d)이다.

TABLE 4. Environment Setting of Fig.5.

Case	(a)	(b)	(c)	(d)
Mobility	X	X	O	O
Friendly jamming	X	O	X	O
Source-Destination distance (m)	48,413	48,413	2	2

시뮬레이션 설계 과정은 다음과 같다. 우선, 송신 노드와 수신 노드 사이에는 켤레 복소수 형태의 채널 h_{sd}^{*}가 있다고 가정한다. 또한, 송신단과 수신단에서의 P_s, 우호적 재밍 드론의 P_j의 최대 전송 전력은 각각 24(dBm)로 가정한다. 이러한 가정아래 각 개체별 BER 측정을 위한 수식은 다음과 같이 정의된다.

첫 째, 수식 (3)의 수신 노드가 송신 노드로부터 수신하는 신호는 수신 노드와 송신 노드 사이의 거리(h_{sd}^{*}) 와 재머 드론과 수신 노드 사이의 거리(h_{jd}^{*}), 수신단의 최대 전송 전력(P_s), 재머 드론의 최대 전송 전력(P_j) 그리고 잡음(n_d)으로 나타낼 수 있다[23].

$$y_e = G\sqrt{P_s}h^*_{sd}s + \sqrt{P_j}h^*_{jd}q + n_d \qquad (3)$$

이 때, 채널 계수 h는 아래 수식 (4)와 같다. d는 두 통신 노드 사이의 거리, e는 균일하게 분포된 난수 $a+bi$이고, c는 경로 손실 지수이다.

$$h = (d)^{\frac{-c}{2}} e \tag{4}$$

또한, G는 증폭 스케일 벡터로 수식 (5)와 같이 나타낼 수 있다. N은 가우시안 잡음이다.

$$G = \frac{1}{\sqrt{P_s |h^*_{sd}|^2 + N}} \tag{5}$$

마지막으로, 수식 (6)의 도청자가 수신하는 신호는 송신 노드와 도청자 사이의 거리(h^*_{se})와 재머 드론과 도청자 사이의 거리(h^*_{je}), 수신단의 최대 전송 전력(P_s), 재머 드론의 최대 전송 전력(P_j) 그리고 잡음(n_d)으로 나타낼 수 있다.

$$y_e = G\sqrt{P_s} h^*_{se} + \sqrt{P_j} h^*_{je} q + n_e \tag{6}$$

또한, 각 실험의 도청 노드의 BER은 수식 (7)와 같이 나타낼 수 있다. 재밍 신호가 없는 Fig.5의 Case(a)와 Case(c)의 경우 $G\sqrt{P_j} h^*_{je} JamSymbols$은 0으로 계산된다.

$$y_e = G\sqrt{P_s} h^*_{se}\ \ TrustSymbols + G\sqrt{P_j} h^*_{je}\ \ JamSymbols \tag{7}$$

Table 5는 시뮬레이션 의사 코드에 쓰이는 변수를 정의한 표이며, Table 6은 시뮬레이션 의사 코드이다. Table 6의 세부 설명은 다음과 같다. line 1-5는 재밍드론과 eve사이의 거리를 측정하고, 이렇게 측정된 거리는 재머가

eve에 주는 영향력에 이용된다. line 6은 시뮬레이션 반복 횟수로 1000회 반복하여 평균 BER을 구한다. line 7의 c는 경로손실지수로 채널계수를 구하는데 사용한다. line 8-24는 도청자의 평균 BER을 구하는 반복하는 함수이다. 이 함수는 line6에서 정해진 횟수만큼 반복하고, 매개변수로 전송할 데이터의 size, 경로손실지수, 송신노드와 도청자와의 거리, 송신노드와 수신노드와의 거리, 재머와 도청자와의 거리, 송수신단의 최대전송전력, 재머의 최대전송전력을 받는다. line10의 e는 복소수형태의 난수로 채널계수를 구하는데 사용한다. line11-13은 c와 e를 이용하여 채널계수를 구한다. line14의 G는 송신노드와 수신노드의 거리에 따라 증폭되는 스케일링 계수이다. line15-16은 전송할 데이터의 size만큼 0과 1로 무작위 생성한 후 복소수 형태로 매핑하는 것이며, line 17-18은 재밍신호로 사용될 데이터를 무작위로 생성한 후 복소수 형태로 매핑한 것이다. line19은 도청자가 수신한 신호이고, line20은 신호로 형성된 비트이다. line21은 송신 노드가 보낸 비트와 이브가 수신한 비트를 이용하여 BER을 계산한다. 그리고 line22에서 평균 BER을 구한다.

TABLE 5. Define Parameters for Pseudo Code

Notation	Remark
c	Channel coefficient for free-space path loss
e	Randomized complex number
h_{se}	Channel coefficient for free-space path loss of Distance between source and eve
h_{sd}	Channel coefficient for free-space path loss of Distance between source and destination
h_{ie}	Channel coefficient for free-space path loss of Distance between jammer and eve
G	Scaling factor of amplification based on the distance source and destination

TABLE 6. Pseudo Code for Eve's BER Measurement

1: $Drone_1 toEveDistacne \leftarrow$ *distance between* $Drone_1$ and *Eve*
2: $Drone_2 toEveDistacne \leftarrow$ *distance between* $Drone_2$ and *Eve*
3: $Drone_3 toEveDistacne \leftarrow$ *distance between* $Drone_3$ and *Eve*
4: *CalculateJEDistance* $\leftarrow$ *Calculate the distance of the cloest drone*
5: *jeDistance* $\leftarrow$ *The distance between one jammer* and *the eavesdropper affected by the jammers*
6: max*Loop* $\leftarrow$ 1000
7: $c \leftarrow$ *path loss* exponent
8: *procedure* $MeasureEveBER(N_{bits}, c, seDistance, sdDistance, jeDistance, P_t, P_{j)}$
9: for 1 *to* max*Loop*
10: $e \leftarrow randomComplexNumber(N_{bits})$
11: $h_{se} \leftarrow seDistance^{-\frac{e}{2}} * e$
12: $h_{sd} \leftarrow sdDistance^{-\frac{e}{2}} * e$
13: $h_{je} \leftarrow seDistance^{-\frac{e}{2}}$
14: $G \leftarrow \frac{1}{\sqrt{(P_t |h_{sd}|^2}}$
15: *SignalBits* $\leftarrow$ *Generate randomly Signal Bits of* N_{bits} *at* 0,1
16: *SignalSymbols* $\leftarrow$ *Mapping SignalBits to SignalSymbol in the form of complex number*
17: *JamBits* $\leftarrow$ *Generate randomly Jamming Symbol of* N_{bits} *at* 0,1
18: *JamlSymbols* $\leftarrow$ *Mapping JamBits to JamSymbol in the form of complex number*
19: $eveRecieveSymbol \leftarrow G\sqrt{P_t} h_{se} SignalSymbols + \sqrt{P_j} h_{je} JamSymbols$
20: *eveRecieveDemappedBits* $\leftarrow$ *Demapping eveRecieve Symbol to Bits*
21: *MeasureBER* $\leftarrow$ *Sum*(*SignalBits* $\neq$ *eveRecieveDemapped Bits*) / N_{bits}, *Calculate BER with comparision between Signal Bits* and *eveRecieve Demapped Bits*
22: *averageBER* $\leftarrow$ *Take average* for *the BER results of each loop so the BER has minimized the bias*
23: *end* for
24: *end procedure*

3) Result of Simulation

송신 노드가 100,000개의 SignalSymbol 데이터를 전송하여 수신 노드와 도청자들의 BER을 측정했다. 시뮬레이션을 1000회 반복하여 평균 BER을 구했다. Fig.5의 모든 Case에서 합법적인 수신 노드의 평균 BER은 0으로 송신 노드가 보낸 데이터를 모두 정상적으로 수신한다. Table 7은 도청자들의 평균 BER 결과를 III장에서 정의한 정보 유출 비율 ILR metrics에 적용한 결과를 정리한 표이고, Fig.6은 Table 7의 그래프이다.

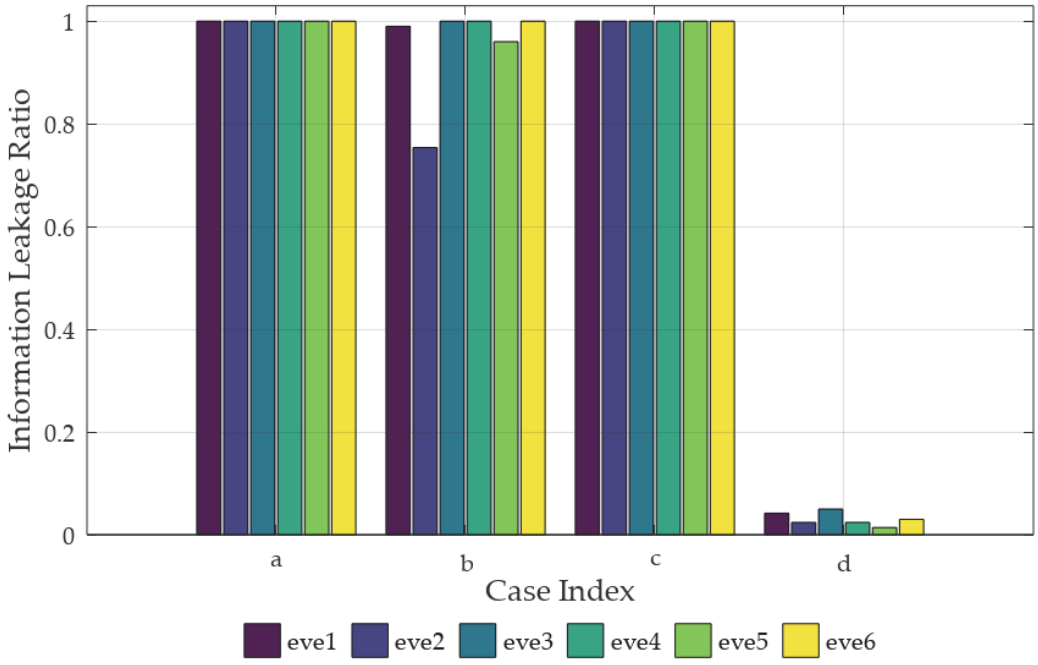


FIGURE 6. Simulation results; conventional schemes (a, b, c) and proposed scheme (d)

TABLE 7. Simulation results; conventional schemes (a, b, c) and proposed scheme (d)

	eve1	eve2	eve3	eve4	eve5	eve6
Case(a)	1	1	1	1	1	1
Case(b)	0.99	0.754	1	1	0.96	1
Case(c)	1	1	1	1	1	1
Case(d)	0.042	0.024	0.05	0.024	0.014	0.03

Case(a)의 경우, 모든 도청자의 ILR은 1이다. 따라서 기기의 이동성이 없고 friendly-jamming기법을 이용하지 않는 경우, 도청자의 도청 확률이 높다.

Case(b)의 경우, Wang의 Friendly UAV Jamming (Fri-UJ)모델[18]의 특징이 반영되어 있다. Fri-UJ는 이동통신 네트워크 환경에서 다중 무인 항공기를 이용하고, UAV가 재머역할을 수행하여 Friendly jamming 신호를 송출한다. 하지만 CFJ-DMZ와 다르게 송신 노드의 이동성이 없다. 이때, 드론의 협력적 재밍 신호 범위 내에 있는 eve2, eve5의 ILR은 각각 0.754, 0.960이고, 드론의 협력적 재밍 신호 범위 밖에 있는 도청자들의 ILR은 1이다. 따라서 기기의 이동성 없이 friendly-jamming기법만 이용하는 경우, 도청자의 도청 확률이 높다.

Case(c)의 경우, 모든 도청자의 ILR은 1이다. 송신 노드와 수신 노드의 거리가 가까워져 송신 노드의 신호 세기가 감소하였다. 하지만 시뮬레이션의 환경은 자유 공간이므로 송신 노드의 신호 세기 감소가 도청자들의 통신 품질에 큰 영향을 주지 못했다. 따라서 기기의 이동성은 있지만 friendly-jamming 기법을 사용하지 않는 경우, 도청자의 도청 확률이 높다.

CFJ-DMZ모델인 Case(d)의 경우, 드론의 협력적 재밍 신호 범위 내에 있는 eve2, eve5의 ILR은 각각 0.024, 0.014이다. 또한 드론의 협력적 재밍 신호 범위 밖에 있는 도청자들의 ILR도 0에 근접하여, 모든 도정자의 평균 ILR은

0.03이다. 따라서 기기의 이동성과 friendly-jamming기법을 이용하는 경우, 도청자의 통신 품질이 저하시켜 Fri-UJ[18]의 특징이 반영 된 Case(b)와 비교할 때 평균적으로 92%의 ILR을 줄일 수 있었고, Case(a) 및 Case(c)와 비교하면 97%의 ILR을 줄인 Secure Zone에서 보안 통신이 가능해졌다.

2. Field Experiment

1) Effect of Friendly-Jamming

본 장에서는 raspberry pi 3를 이용하여 실험을 진행하였다. 우호적 재밍 드론과 도청자도 라즈베리 파이를 이용해 구현하였다. 라즈베리 파이간 통신은 D2D 통신 방식으로 패킷을 전송했다. 송신 노드는 호스트 모드를 이용하여 AP가 되고, 수신 노드는 송신 노드의 AP에 연결하였다. 각 노드들의 최대 전송 전력은 24dBm이다. 재밍 신호는 Ping of Death기법을 이용해서 생성했다.

또한 송신 노드가 수신 노드에게 전송하는 데이터는 총 256비트로 구성된 문자열 '1'이고, 동기화를 위한 프리엠블 비트로 총 128비트로 구성된 문자열 'a'를 이용했다. 프리엠블 비트는 Fig.7과 같이 처리했다. 프리엠블 128개의 비트 중 64비트 미만의 a가 수신되었다면, ILR이 0.5 미만에 해당하는 경우이므로 해당 패킷을 통해 수신받은 데이터를 모두 해석 불가능한 상태로 처리했다. 프리엠블 128개의 비트 중 64비트 이상의 a가 수신되었다면, 프리엠블 비트를 제거한 후 데이터의 에러비트 개수를 구했다. 에러비트 개수는 유실비트 개수와 불일치 비트 개수를 더한 값이다. 유실비트 개수는 송신 비트 수에서 수신 비트 수를 뺀 값이고, 불일치 비트 개수는 수신 비트를 순차적으로 Xor한 후 1의 개수를 센 값이다. 수신 노드와 도청자의 BER은 에러비

트를 이용하여 구한다.

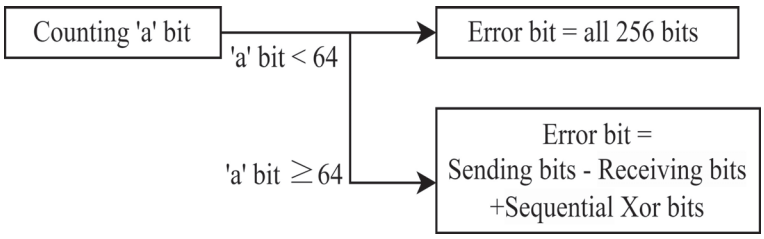


FIGURE 7. Synchronize with Preamble bit

우선 Fig.1(a) friendly jamming모델을 구현하여 재밍 신호의 효과성을 검증했다. 송신 노드와 수신 노드의 위치를 기준으로 우호적인 재밍 드론 노드 한 대를 배치한다.

TABLE 8. Result of Friendly-Jamming (Filed Experiment)

Node	BER metric
Destination Node	0
eve1	0.389
eve2	0.012
eve3	0.975
eve4	0.992
eve5	0.938
eve6	0.562

송신 노드가 데이터를 전송하여 수신노드와 도청자들의 BER을 측정했다. Table 8은 Fig.1(a) 모델 적용을 1000회 반복한 평균 BER이다. 수신 노드의 평균 BER은 0이다. 합법적인 수신 노드는 재밍 신호의 영향을 받지 않으므로 송신 노드와 정상적인 통신이 가능하다. 재머인 드론 주변에 위치하지 않

은 도청자 eve1, eve2, eve6는 평균 BER 이 각각 0.389, 0.012, 0.562으로 상대적으로 낮은 수치의 결과를 보였다. 재머인 드론 노드 주변에 위치한 도청자 eve3, eve4, eve5는 평균 BER이 각각 0.975, 0.992, 0.938으로 1에 근접한 결과를 보였다. 이 실험 결과는 합법적인 송·수신 노드는 협력적 재밍 신호에 의해 주변 도청자들에게 유출되는 정보의 양을 줄이면서 안전하게 정보를 전달할 수 있다는 것을 보여준다. 따라서 friendly-jamming기법을 이용하면 도청자의 도청 확률을 줄여 통신의 보안성을 향상시킬 수 있다.

2)Experimental settings

Evaluation 환경을 정리한 표 Table 2와 같이 현장 실험은 raspberry pi 3 Model B+를 사용했다. 라즈베리파이의 CPU는 Quad-core 64bit ARMv8이고, Ram은 1.0GB이다. 현장실험은 50m*50m 규격의 공터에서 진행했다. 현장 실험은 공터에서 진행하여 다른 전파에 의한 영향력은 최소화하고자 하였다. 라즈베리파이의 최대 전송 전력은 24dBm으로 실험에 사용되는 송신노드, 수신노드, 우호적 재밍 드론의 최대 전송 전력은 각 24dBm이다. Field Experiment는 시뮬레이션과 동일한 실험 환경에서 진행했다. 그러므로 Fig.5의 실험환경대로 기기를 배치하였다. 시뮬레이션과 마찬가지로 실험 별 효과적인 비교를 위해 도청자의 위치는 모든 실험에서 동일하다. 또한 도청자는 송신 노드와 재밍 노드의 신호 범위를 고려하여 시뮬레이션의 도청자가 실험 환경에 따라 받는 신호의 영향과 동일한 위치에 배치했다.

3) Result of Field Experiment

송신 노드가 데이터를 전송하여 수신 노드와 도청자들의 BER을 측정했다.

BER 측정을 1000회 반복하여 평균 BER을 구했다. Fig.5의 모든 Case에서 합법적인 수신 노드의 평균 BER은 0으로 송신 노드가 보낸 데이터를 모두 정상적으로 수신한다. Table 9는 도청자들의 평균 BER 결과를 III장에서 정의한 정보 유출 비율 ILR metrics에 적용한 결과를 정리한 표이고, Fig.8은 Table 9의 그래프이다.

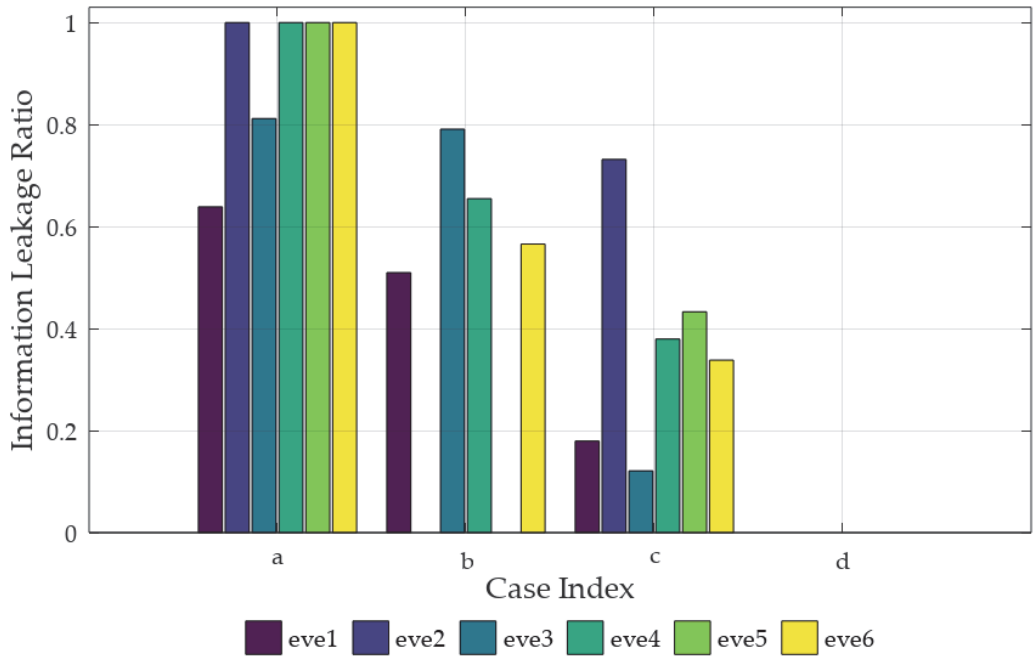


FIGURE 8. Field Experiment Results; conventional schemes (a, b, c) and proposed scheme (d)

TABLE 9. Field Experiment Results; conventional schemes (a, b, c) and proposed scheme (d)

	eve1	eve2	eve3	eve4	eve5	eve6
Case(a)	0.639	1	0.819	1	1	1
Case(b)	0.5098	0	0.791	0.6548	0	0.5658
Case(c)	0.18	0.732	0.121	0.38	0.433	0.338
Case(d)	0	0	0	0	0	0

Case(a)의 경우, eve1과 eve3을 제외한 도청자의 ILR은 모두 1이다. 그리고 eve1과 eve 3의 ILR이 각각 0.639, 0.819이다. 따라서 기기의 이동성 없고 friendly-jamming기법을 이용하지 않는 경우, 도청자의 도청 확률이 높다. 또한, 송신 노드와 상대적으로 거리가 먼 eve1과 eve3만이 ILR이 1이 아닌 것을 통해 도청자와 송신 노드의 거리가 멀수록 도청자의 도청 확률이 감소됨을 알 수 있다.

Fri-UJ[18] 모델의 특징이 반영되어 있는 Case(b)의 경우, 협력적 재밍 신호가 도청자의 통신 품질에 영향을 끼쳐서 모든 도청자의 ILR이 감소했다. 드론의 협력적 재밍범위 내에 있는 eve2, eve5의 ILR은 0이다. 그러나 드론의 협력적 재밍 신호 범위 밖에 있는 도청자들의 ILR은 0.5이상이다. 따라서 기기의 이동성 없이 friendly-jamming기법만 이용하는 경우, 협력적 재밍 신호 범위 밖 도청자의 도청 확률이 높다.

Case(c)의 경우, 송신 노드와 수신 노드의 거리가 가까워졌으므로, 송신 신호 세기를 감소하였다. 그 결과 송신 노드와 상대적으로 거리가 먼 eve1, eve3의 ILR은 0.180, 0.121이다. 그러나 송신 노드와 상대적으로 거리가 가까운 eve2, eve4, eve5, eve6의 ILR이 0.732, 0.380, 0.433, 0.338이다. 모든 도청자들의 ILR이 Case(a)에 비해 감소하였지만 일부 도청자의 ILR은 높다. 따라서 기기의 이동성은 있지만 friendly-jamming 기법을 사용하지 않는 경우,

도청자의 도청 확률이 높다.

CFJ-DMZ 모델인 Case(d)의 경우, 모든 도청자의 ILR은 0이다. 따라서 기기의 이동성과 friendly-jamming기법을 이용하는 경우, 도청자의 통신 품질이 저하시켜 도청 확률을 줄인다. 그러므로 Secure Zone에서 보안 통신이 가능하다.

3. Evaluation Result Analysis

다음은 시뮬레이션과 현장 실험을 통해 얻은 결과이다. 현장 실험 Case(a)에서 eve1과 eve3의 ILR을 통해 송신 노드와 도청자의 거리가 멀수록 도청자의 통신 품질이 저하됨을 알 수 있다.

또한 Case(b)의 eve5와 eve6의 ILR을 통해 도청자가 우호적 재밍 드론과 가까울수록 도청자의 통신 품질이 저하됨을 알 수 있다.

Case(a)와 Case(c), Case(b)와 Case(d)의 도청자들의 평균 ILR비교는 기기 이동성의 효과를 보여준다. 송신 노드가 수신 노드로 이동하여 두 기기 간 거리가 가까워짐에 따라 송신 신호 세기가 감소하면 도청자의 통신 품질이 저하됨을 알 수 있다

기기의 이동성과 friendly-jamming기법을 이용하는 Case(d)에서 도청자들의 평균ILR은 시뮬레이션은 0.03이고 현장 실험은 0이다. 따라서, CFJ-DMZ 모델이 도청자의 통신 품질을 저하시켜 도청 가능성이 높은 영역의 도청 확률을 줄일 수 있다. 그러므로 Secure Zone에서 통신의 보안성이 향상된다.

Ⅵ. 결 론

본 논문은 모바일 사물인터넷 장치의 이동성과 재밍신호를 활용하여 무선 통신의 보안성을 향상시키는 CFJ-DMZ 방법을 제안하고 시뮬레이션과 현장 실험을 통해 그 효과를 입증했다. 협력적 우호 재밍 신호를 송출하는 드론들이 보안 D2D통신을 진행하는 위치로 이동하여 재밍 신호를 송출해 형성된 Secure Zone은 효과적으로 도청을 방지하고 위치와 크기 변경이 쉬워 유연하다. 또한 송수신자가 통신할 때만 재밍 신호를 송출하여 주변의 다른 송수신 노드에 끼치는 재밍 신호의 영향을 최소화하고 배터리를 효율적으로 사용한다. CFJ-DMZ모델을 적용한 Simulation와 Field Experiment를 통해 도청 장치의 BER을 측정하여 도청자의 수신 성능을 악화시켜 정상 패킷 수신율이 감소되는 것을 확인하였다. 그리고 보안 성능 평가를 위한 메트릭으로서 ILR을 정의하여 제안한 방식의 정보 유출량이 줄어드는 것을 실험적으로 확인했다.

본 연구에서 제안한 CFJ-DMZ방법은 군사용 드론 통신 뿐만 아니라 물류 배송과 무인 이동체 등과 같은 미래 사회시스템 전반의 IoT 네트워킹 환경에 접목하여 실제 상용화할 수 있는 모델로서 활용될 수 있을 것이다. 본 연구의 한계점으로 재밍의 영향을 2차원 평면에서 다룬점이 있다. RF 고유한 방출 특성을 고려하기 위해서는 3차원으로도 CFJ-DMZ방법의 효과 검증이 필요하다. 그리고 제안한 방식이 상용 시스템에 적용되려면 낮은 지연이 중요한데, 본 연구에서는 시간 복잡도까지 분석하지 못 했고, 제안한 메트릭 ILR만을 이용해서 제안한 CFJ-DMZ로 기밀 통신을 할 수 있는지에 대해서만 연구가 진행되었다. 또한 드론들로 형성된 Secure Zone 내부에 도청자가 들어간 경우와 같이 다양한 환경에 대한 실험 및 검증이 요구된다. 후속 연구에서는 이러한 한계점을 수학적 모델과 시뮬레이션 모델에 실제 환경 파라

미터를 적용하며 보완해 나갈 것이다. 해당 연구들을 통해 한층 심화된 보안 아키텍처를 설계하고 기밀하고 복잡한 지역에서의 보안성을 높일 수 있을 것이다.

참고문헌

[1] Md. Waliullah, Diane Gan, Wireless LAN Security Threats & Vulnerabilities, January 2014International Journal of Advanced Computer Science and Applications 5(1), 2014.

[2] Jyh-Cheng Chen, Ming-Chia Jiang, & Yi-Wen Liu. Wireless LAN security and IEEE 802.11i. IEEE Wireless Communications, 2005, 27 - 36.

[3] Y. S. Kim, P. Tague, H. Lee and H. Kim, Carving Secure Wi-Fi Zones with Defensive Jamming, Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012.

[4] Yang, Y., Wu, L., Yin, G., Li, L., and Zhao, H., A survey on security and privacy issues in Internet-of-Things, IEEE Internet of Things Journal, vol. 4 no. 5, 1250-1258, 2017.

[5] T. Bose, S. Bandyopadhyay, A. Ukil, A. Bhattacharyya and A. Pal, Why not keep your personal data secure yet private in IoT?: Our lightweight approach, 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015, 1-6.

[6] X Zhang, J. He and Q. Wei, "Security Considerations on Node Mobility in Wireless Sensor Networks," 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009, 1143-1146.

[7] Wyner and D. Aaron, The wire tap channel, Bell system technical journal, vol. 54, no. 8, 1975, 1355-1505.

[8] Bakr, O., and Mudumbai, R., A new jamming technique for secrecy in multi-antenna wireless networks, IEEE International Symposium on Information Theory, IEEE, 2010, 2513-2517.

[9] Cumanan, K., Xing, H., Xu, P., Zheng, G., Dai, X., Nallanathan, A., Ding, Z., and Karagiannidis, G. K., Physical layer security jamming: Theoretical limits and

practical designs in wireless networks, IEEE Access 5, vol. 5, 2016, 3603-3611.

[10] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, Wireless secrecy regions with friendly jamming, IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, 2011, 256 - 266.

[11] J. P. Vilela, M. Bloch, J. Barros and S. W. McLaughlin, Friendly Jamming for Wireless Secrecy, 2010 IEEE International Con-ference on Communications, 2010, 1-6.

[12] B. He, Y. She and V. K. N. Lau, Artificial Noise Injection for Securing Single-Antenna Systems, IEEE Transactions on Vehicular Technology, vol. 66, no. 10, 2017, 9577-9581

[13] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman and R. Gaire, Friendly Jammer against an Adaptive Eavesdropper in a Relay-aided Network, 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 1707-1712, doi: 10.1109/IWCMC48107.2020.9148476.

[14] M. A. Kishk and H. S. Dhillon, Stochastic Geometry-Based Comparison of Secrecy Enhancement Techniques in D2D Networks, IEEE Wireless Communications Letters, vol. 6, no. 3, 2017, 394-397

[15] Kim, Y. S., Tague, P., Lee, H., and Kim, H., A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control, Wireless Networks, vol. 21, no. 8, 2015, 2631-2647.

[16] E. Yaacoub and M. A. Husseini, Achieving Physical Layer Security with Massive MIMO Beamforming, 2017 11th European Conference on Antennas and Propagation (EUCAP), 2017.

[17] Vishal Sharma, Ilsun You, Karl Andersson, Francesco Palmieri, Mubashir Husain Rehmani, Jaedeok Lim, Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey,

[18] Qubeijian Wang, Hong-Ning Dai, Hao Wang, Guangquan Xu, and Arun Kumar Sangaiahs, UAV-enabled friendly jamming scheme to secure industrial

Internet of Things, JOURNAL OF COMMUNICATIONS AND NETWORKS, 2019.
[19] Jehad M. Hamamreh, Haji M. Furqan and Huseyin Arslan, Classifications and Applications of Physical Layer Security Tech-niques for Confidentiality: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, vol. 21, no.2, 2019, 1173-1828
[20] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.
[21] LDPC Codes for the Gaussian Wiretap Channel,2011
[22] Salvatore D'Oro, Eylem Ekici, Sergio Palazzo, Optimal Power Allocation and Scheduling Under Jamming Attacks, IEEE/ACM Transactions on Networking, vol.25, no.3, Jun.2017, 1310-1323
[23] Zaid Abdullah, Gaojie Chen, Mohammed A. M. Abdullah and Jonathon A. Chambers, Enhanced Secrecy Performance of Multihop IoT Networks With Cooperative Hybrid-Duplex Jamming, IEEE Transactions on Information Forensics and Security, vol.16, Jun.2020, 161-172
[24] Allouche, Y., Arkin, E. M., Cassuto, Y., Efrat, A., Grebla, G., Mitchell, J. S., ... & Segal, M., Secure communication through jammers jointly optimized in geography and time, Pervasive and Mobile Computing, 2017, 41, 83-105.
[25] X. Li, H. Dai, Q. Wang, M. Imran, D. Li and M. A. Imran, Securing Internet of Medical Things with Friendly-jamming schemes, ELSEVIER computer communications, vol. 160, July.2020, 431-442.
[26] Shuai Zhang and Nirwan Ansari, Latency Aware 3D Placement and User Association in Drone-Assisted Heterogeneous Networks With FSO-Based Backhaul, IEEE Transactions on Vehicular Technology, vol. 70, Sep.2021, 11991 - 12000.
[27] B. Duo, H. Hua, Y. Li, Y. Hua and X. Zhu, Robust 3D trajectory and power design in probabilistic LoS channel for UAV-enabled cooperative jamming, ELSEVIER vehicular communications, vol. 32, Dec.2021

[28] P. Lohanan, D.Mishrab, J. Nguyen and V. Gupta, Secrecy-aware UAV position-aided jamming for practical eavesdropper localization models, ELSEVIER vehicular communications, vol. 33, Jan.2022

ABSTRACT

Cooperative Friendly Jamming Techniques for Mobile Secure Zone

Ga-Hye Jeon
Department of Future Convergence
Technology Engineering
Graduate School of Sungshin University

Threats of eavesdropping and information leakages have increased sharply owing to advancements in wireless communication technology. In particular, the Internet of Things (IoT) has become vulnerable to sniffing or jamming attacks because broadcast communication is usually conducted in open-network environments. Although improved security protocols have been proposed to overcome the limitations of wireless-communication technology and secure safe communication channels, they are difficult to apply to mobile communication networks and IoT because complex hardware is required. Hence, a novel security model with a lighter weight and greater mobility is needed. This paper proposes a security model applying cooperative friendly jamming using artificial noise and drone mobility, which are autonomous moving objects, and demonstrates the prevention of eavesdropping and improved security through simulations and field tests. The Cooperative Friendly Jamming Techniques for Drone-based Mobile Secure Zone (CFJ-DMZ) can set a secure zone in a target area to support a safe wireless mobile communication network through friendly jamming, which can effectively reduce eavesdropping threats. According to the experiment results, the average information leakage rate of the eavesdroppers in CFJ-DMZ-applied scenarios is less than or equal to 3%, an average improvement of 92% over conventional methods.

ACKNOWLEDGEMENTS

본 석사학위 청구논문은 해외 저널 Sensors에 발표한 Cooperative Friendly Jamming Techniques for Drone-Based Mobile Secure Zone[1]을 기반으로 작성되었습니다. 본 논문을 지도해주신 이일구 교수님과 Cooperative Friendly Jamming Techniques for Drone-Based Mobile Secure Zone을 함께 발표한 이지현, 성연수, 박현주, 이유진, 윤선우 학생에게 진심으로 감사드립니다.

1) G. H. Jeon, J. H. Lee, Y. S. Sung, H. J. Park, Y. J. Lee, S. W. Yun and I. G. Lee, Cooperative Friendly Jamming Techniques for Drone-Based Mobile Secure Zone, Sensors, vol. 22, no. 3, Jan. 2022, 865