수동적 및 능동적 탐지 불확실성이 존재하는 중계기 네트워크에서의 은닉 통신

문지환*
*국립한밭대학교

*anschino@staff.hanbat.ac.kr

Covert Communications In Relay Networks With Passive and Proactive Detection Uncertainty

Jihwan Moon*
*Hanbat National University.

요 약

은닉 통신은 중요한 통신 링크의 은폐를 요구하는 높은 수준의 보안 네트워크에서 큰 주목을 받고 있다. 은닉 통신의 성공 여부는 원치 않는 노드의 탐지 오류 확률을 얼마나 낮출 수 있는지에 따라 평가된다. 이러한 탐지 오류는 예를 들어 잡음 수준의 변화와 같은 수동적 불확실성에서 발생할 수 있으며, 전송 패턴 변경과 같이 능동적으로 유도될 수도 있다. 본 논문에서는 이 두 가지 유형의 탐지 불확실성이 존재하는 중계기 네트워크에서의 은닉 통신을 살펴본다. 구체적으로, 소스 노드는 중계기를 거쳐 먼 목적지 노드로 일반 메시지와 은닉 메시지를 함께 전송한다. 이러한 환경에서 중계기에 탑재된 은닉 메시지 탐지기가 잡음 불확실성을 겪는 경우와, 소스 노드가 인위적인 잡음을 변동적으로 발생시키는 경우를 모두 고려해 본다. 시뮬레이션 결과를 통해 일반 및 은닉 메시지 간 최적 전송 전력 할당에 따른 달성 가능한 은닉 전송률을 평가한다.

Ⅰ. 서 론

무선 기술이 지난 수십 년 동안 크게 발전함에 따라, 안전하고 신뢰성 있는 통신에 대한 수요는 그 어느 때보다도 중요해졌다. 근래 각광을 받고 있는 사물인터넷(Internet of Things, IoT), 차량-사물 간 통신(Vehicular-to-Everything, V2X), 다중접속 엣지 컴퓨팅(Multiaccess Edge Computing, MEC), 저궤도(Low Earth Orbit, LEO) 위성 통신과 같은 정교한 시스템에서는 수백 개의 장치를 동시에 관리하는 것이 어렵기 때문에 도청이나 악의적인 공격에 대한 취약성이 더욱 심화되고 있다 [1].

보다 강력한 보안 조치를 추구하는 과정에서, 통신의 존재 자체를 숨기는 것이 필요할 수 있다. 이는 암호화나 물리 계층 보안이 비인가 노드가 실제 정보를 획득하는 것을 막는 데에는 효과적이지만, 여전히 패킷의 IP 주소나 전송 행태와 같은 메타데이터를 기반으로 트래픽 분석을 통해 사용자 활동을 유추할 수 있기 때문이다 [2]. 이에 따라 외부로부터의 탐지 가능성을 최소화하는 것이 최우선인 상황에서는 은닉 통신, 또는 저피탐 통신이 큰 주목을 받고 있다. 이러한 은닉 통신은 사설 IoT 네트워크, 군 특수부대의 전술 작전, 대테러 합법 감시 활동, 주요 인프라 내 기밀 정보 보호와 같은 분야에서 활용될 수 있다 [3].

은닉 통신은 중요한 통신 링크의 은폐를 요구하는 높은 수준의 보안 네트워크에서 큰 주목을 받고 있다. 은닉 통신의 성공 여부는 원치 않는 노드의 탐지 오류 확률을 얼마나 낮출 수 있는지에 따라 평가된다. 이러한 탐지 오류는 예를 들어 잡음 수준의 변화와 같은 수동적 불확실성에서 발생할 수 있으며, 전송 패턴 변경과 같이 능동적으로 유도될 수도 있다. 본 논문에서는 이 두 가지 유형의 탐지 불확실성이 존재하는 중계기 네트워크에서의 은닉 통신을 살펴본다. 구체적으로, 소스 노드는 중계기를 거쳐 먼 목적지 노드로 일반 메시지와 은닉 메시지를 함께 전송한다. 이러한 환경에서 중계기에 탑재된 은닉 메시지 탐지기가 잡음 불확실성을 겪는 경우와 [4], 소스 노드가 인위적인 잡음을 변동적으로 발생시키는 경우를 모두 고려해 본다. 시뮬레이션 결과를 통해 일반 및 은닉 메시지 간 최적 전송 전력 할당에 따른 달성 가능한 은닉 전송률을 평가한다.

Ⅱ. 본론

먼저 II. A 절에서 기존 연구 [4]에서의 결과를 바탕으로 중계기에 잡음 불확실성이 존재할 때를 가정한 시스템 모델과 달성 가능한 은닉 통신 속도를 소개한 후 다음 II. B 절에서 인공 잡음 변동을 활용한 은닉 통신에 대해 설명한다.

A. 잡음 불확실성 하에서의 은닉 통신

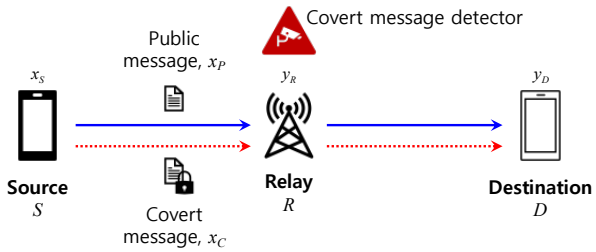

그림 1. 잡음 불확실성 하에서의 시스템 모델

그림 1 은 소스 노드 S와 목적지 노드 D가 중계기 R을 통해 통신하는 구조를 나타낸다. 소스 송신 전력 P_S 중 α는 일반 메시지 x_P에, 나머지 $1-\alpha$는 은닉 메시지 x_C에 할당된다. 한편 중계기의 잡음 $\sigma^2_{R,\mathrm{dB}}$가 불확실하게 변동한다고 가정하며, 이는 데시벨 (decibel, dB) 범위에서 $\sigma^2_{R,\mathrm{dB}} \sim U\left(\bar{\sigma}^2_{R,\mathrm{dB}} - \zeta_{\mathrm{dB}}, \bar{\sigma}^2_{R,\mathrm{dB}} + \zeta_{\mathrm{dB}}\right)$를 따른다고 모델링한다. 여기에서 $\bar{\sigma}^2_{R,\mathrm{dB}}$는 변동의 평균값을, $\zeta_{\mathrm{dB}} \geq 0$는 변동 범위의 상한을 의미한다.

B. 인공 잡음 변동을 활용한 은닉 통신

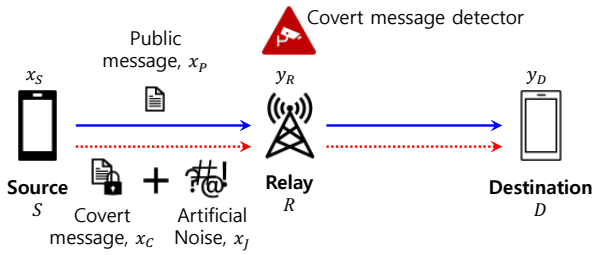

그림 2. 인공 잡음 변동 하에서의 시스템 모델

그림 2 은 소스 노드가 은닉 메시지 x_C를 은닉 송신 확률 $p \in [0,1]$에 따라 확률적으로 전송할 뿐만 아니라 x_C 가 탐지되더라도 이를 은폐하고 기밀성을 유지하기 위해 균일하게 변동하는 전력을 가진 인위적 잡음 $x_J \sim CN(0,1)$ 도 함께 방출하는 구조를 나타낸다. 일반 메시지와 은닉 메시지에 할당한 후 남은 송신 전력 α_J을 x_J 에 할당하며, $\alpha_{J,\mathrm{dB}} \sim U\left(\bar{\alpha}_{J,\mathrm{dB}} - \zeta_{\mathrm{dB}}, \bar{\alpha}_{J,\mathrm{dB}} + \zeta_{\mathrm{dB}}\right)$ 분포를 따라 변동을 준다. 여기에서 $\bar{\alpha}_{J,\mathrm{dB}}$ 는 변동의 평균값을, $\zeta_{\mathrm{dB}} \geq 0$는 변동 범위의 상한을 의미한다.

Ⅲ. 결론

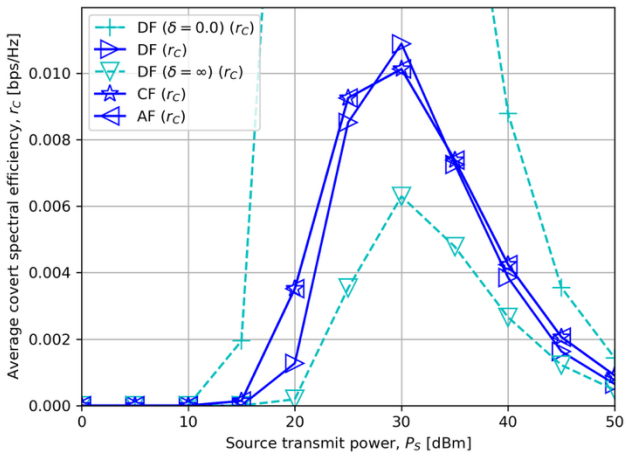

그림 3. 잡음 불확실성 하에서의 은닉 통신 속도

그림 3 는 소스 송신 전력 P_S에 따른 평균 은닉 속도 r_C 를 나타낸다. 모든 증폭-후-전달 (Amplify-and-Forward, AF), 압축-후-전달 (Compress-and-Forward, CF), 복호-후-전달 (Decode-and-Forward, DF) 중계기 종류에서 은닉 속도가 먼저 특정 P_S까지 증가한 후 다시 감소하는 경향을 보이는 것을 확인할 수 있다 [4].

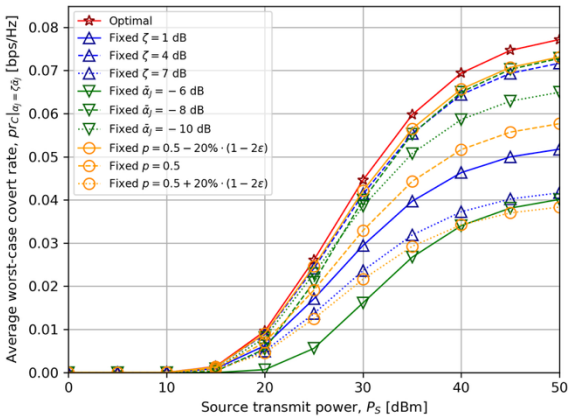

그림 4. 인공 잡음 변동 하에서의 은닉 통신 속도

그림 4 는 소스 송신 전력 P_S에 따른 평균 최악의 경우 은닉 통신 속도 $pr_C|_{\alpha_J = \zeta\bar{\alpha}_J}$를 나타낸다. 최적 해 (optimal)의 성능은 다른 고정된 인공 잡음 변동 범위, 인공 잡음 평균, 은닉 전송 확률 전략 대비 높은 성능을 보인다. 또한 은닉 통신 속도가 P_S에 따라 증가하는데, 이는 II. A 절의 잡음 불확실성이 있는 상황을 고려했을 때 은닉 통신 속도의 경향과 다름을 알 수 있다.

ACKNOWLEDGMENT

이 논문은 2021 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2021R1I1A3050126).

이 논문은 2022 년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-22-047, 우주계층 지능통신망 특화연구실).

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 학·석사연계 ICT 핵심인재양성사업의 연구결과로 수행되었음 (IITP-2025-RS-2022-00156212)

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원을 받아 수행된 연구임(IITP-2025-RS-2024-00437886, 25%)

참 고 문 헌

[1] S. Qazi, B. A. Khawaja, and Q. U. Farooq, "IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends," IEEE Access, vol. 10, pp. 21219–21235, 2022.

[2] B. A. Forouzan, Cryptography and Network Security. New York, NY,USA: McGraw-Hill, 2007.

[3] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert Communications: A Comprehensive Survey," IEEE Commun. Surveys Tuts., vol. 25, no. 2, pp. 1173–1198, Secondquarter 2023.

[4] J. Moon, "Performance Comparison of Relay-Based Covert Communications: DF, CF and AF," Sensors, vol. 23, no. 21, p. 8747, October 2023.