무선통신 환경에서의 데이터 은폐 기법과 은닉 채널 형성 방법 조사

박지훈*, 최상훈[1], 박기웅†

,1세종대학교 SysCore Lab. (대학원생, 연구 교수[1])
† 세종대학교 정보보호학과 (교수†)

A Survey on Data Hiding and Covert Channel Techniques in Wireless Communications

Ji-Hoon Park*, Sang-Hoon Choi[1], Ki-Woong Park†

*,1SysCore Lab., Sejong University
† Dept. of Computer and Information Security, Sejong University
(Graduate Student*, Research Professor[1], Professor†)

요 약

정보통신 기술의 발전으로 다양한 무선통신 기법이 등장했다. 이러한 무선통신은 뛰어난 확장성으로 인해 진화하고 있지만, 더 정교해지는 보안 위협에 직면하고 있다. 특히, 무선 환경에서 도청이나 하이재킹 등에 의해 기밀성을 침해당할 수 있으며, 서로 다른 장치로 구성된 환경에서 각 구성요소가 암호화에 필요한 리소스를 충분히 가지고 있지 않으므로, 메시지 노출을 방지하기 위해 데이터를 은닉하는 스테가노그래피와 공개된 채널에서 당사자만이 송, 수신하도록 은폐 채널을 생성하는 방법에 대한 조사가 필요하다. 본 논문에서는 무선통신 환경을 분류하고 이에 대한 은폐 통신과 스테가노그래피 기법을 조사하였으며, 각 접근법의 도전과제를 도출한다.

I. 서론

무선통신은 스마트폰, 노트북, 사물인터넷, 무인 이동체와 같은 장치를 원격으로 제어하기 위해 광범위하게 사용되며, 일상생활에서도 많은 상업시설에 의해 서비스된다. 이러한 무선통신 환경은 개방적인 특성으로 인해 인가된 사용자와 비 인가된 사용자 모두 접근이 가능하다. 또한, 이와 같은 무선통신 환경에서의 브로드캐스팅은 악의적인 사용자가 데이터를 가로채기 위해 도청을 시도할 수 있으며, 특정 송신기에서 전송된 신호로부터 무선통신의 기밀성을 손상시킨다. 추가로, 이러한 무선통신 환경에서 공격자는 메시지를 가로채어 통신을 지연시키거나 공격자가 원하는 행동을 하도록 유도하기 위해 재전송 공격을 시도할 수 있다. 이외에도, 무선통신 환경에서 노이즈 등을 활용한 은닉 채널 생성과 패킷 또는 프로토콜 내 데이터를 은폐하는 스테가노그래피를 통해 데이터를 유출하는 등의 위협이 존재한다 [1, 2].

이와 같은, 개방된 특성을 가진 무선통신 환경에서 노출되는 패킷은 악의를 가진 사용자에 의해 쉽게 도청되거나 가로챔을 당하는 등 다양한 위협에 취약하여 기밀성을 보장하는 것이 중요하다. 이를 위해 암호 키를 통해 암호화된 통신을 수행하거나 암호 프로토콜이 사용될 수 있으나, 별도의 암호 키 및 암호 프로토콜 사용을 통해 기밀성을 적용하는 방법은 리소스가 제한된 환경에서 전력 효율성 및 전송 효율성 등을 저해하므로, 전반적인 무선통신 성능에 악영향을 미칠 수 있다 [3].

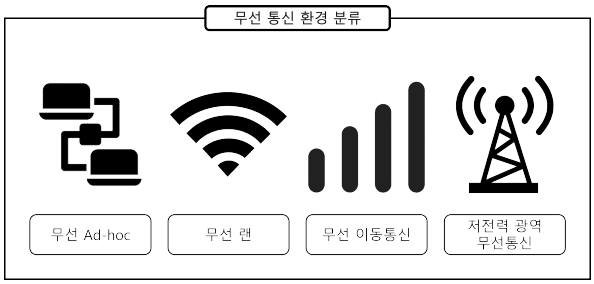
이러한 무선통신 환경에서는 침해를 위해 정보를 은닉하는 은닉 채널 생성 기법이 존재한다 [4]. 하지만 정보를 은닉함으로써 전송되는 데이터의 기밀성을 강화하고, 암호화 또는 암호

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2024-00438551, 50%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 30%), 정보통신방송혁신인재양성사업(Project No.2021-0-01816, 20%)의 지원을 받아 수행된 연구임.

프로토콜을 사용하는 대신, 의도적으로 데이터를 노이즈에 숨겨 전송의 효율성을 높이는 은폐 통신 기법 또한 연구되었다 [5].

본 연구팀은 무선 환경에서 통신 당사자 간의 안전한 무선통신을 달성하기 위해 은닉 채널을 형성하고, 스테가노그래피를 통해 데이터를 은폐하는 다양한 기법을 조사하였다. 이와 같은 무선 은폐 통신 기법이 활용되는 환경을 무선 Ad-hoc, 무선 랜, 무선 이동통신, 저전력 광역 무선통신 환경으로 분류할 수 있었으며, (그림 1)과 같이 표현한다.

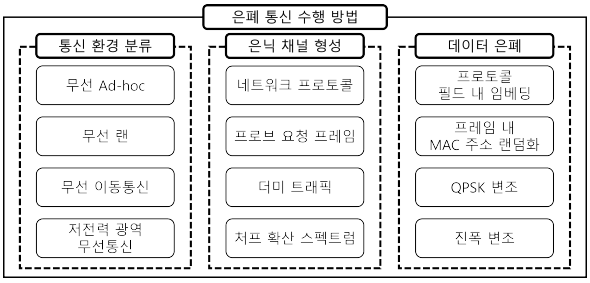


(그림 1) 통신 거리 및 범위에 따른
무선통신 환경 분류

본 논문의 구성은 2장에서 통신 거리 및 범위에 따른 무선통신 환경을 분류하고, 해당 환경에서 사용되는 은폐 통신 기법을 분석하여 각 무선통신 환경에서 구현된 은닉 채널 형성과 데이터 은폐가 어떤 접근법을 통해 무선통신의 기밀성을 달성하는지 소개한다. 3장에서는 각각의 무선통신 환경에서 구현되는 은폐 통신 기법의 도전과제를 분석하고. 4장에서는 결론과 향후 연구 방향을 제시한다.

II. 무선 은폐 통신

무선통신에서 은닉 채널과 스테가노그래피를 사용한 은폐 통신이란, 공개된 채널 내에서 코드를 아는 사람만이 기밀 메시지를 추출할 수 있도록 하는 통신 방식이다. 본 연구팀은 무선 통신 환경을 무선 Ad-hoc, 무선 랜, 무선 이동통신, 저전력 광역 무선통신으로 분류하였으며, 각각의 아키텍처에서 암호화 없이 기밀성을 보장하기 위해 은닉 채널을 생성하고 스테가노그래피를 통해 데이터를 은폐하는 은폐 통신 기법을 조사한다. 또한, 본 연구팀은 각 무선통신 환경에서 은닉 채널을 형성하는 방법과 데이터를 은폐하는 방식을 구분하였으며, (그림 2)와 같이 표현한다.



(그림 2) 은폐 통신 수행 방법 분류

2.1 무선 Ad-hoc

무선 Ad-hoc 환경에서는 중앙화된 인프라가 필요하지 않으므로 MANET(모바일 Ad-hoc), VANET(차량 Ad-hoc), FANET(무인 항공 Ad-hoc) 네트워크에 활용된다 [6]. 하지만 동적이고 분산되어있는 특성으로 인해 데이터 프라이버시와 사이버 보안을 유지하는 데에 많은 문제점을 가진다. 이러한 특징을 가진 무선 Ad-hoc 환경에서 스테가노그래피 기술을 구현하기 위해 TCP, DNS, IP(v4), ICMP, HTTP를 포함한 네트워크 프로토콜에 데이터를 삽입하는 은폐 통신 기법이 연구되었다 [7]. 해당 연구에서는 임베딩을 위한 전송 모듈에서 특정 네트워크 패킷 또는 세그먼트를 선택하고 패킷 구조를 유지함과 동시에 각 프로토콜 내 필드를 변경한다. 이후 수신 모듈에서 스테가노그래피에 사용된 임베딩에 따라 추출 알고리즘을 수행함으로써 은닉 채널 형성과 데이터 은폐를 구현하였다.

2.2 무선 랜

무선 랜 통신 환경에서의 Wi-Fi와 같은 네트워크는 무단 접근, 데이터 가로채기, 네트워크 스푸핑, 라우터와 브릿지 또는 클라이언트 장치의 취약성을 표적으로 하는 다양한 보안 위협에 취약하다. 특히, 이러한 무선 네트워크에서의 통신은 장치 간 전송 채널이 공유되는 특징으로 인해 각 장치에서 동일한 채널이 사용 중이라는 것을 감지할 수 있으므로 기밀성과 처리량을 보장받지 못하게 된다 [8, 9]. 이러한 문제를 해결하기 위해 장치로부터 전송되는 데이터를 숨기는 방법으로 은닉 채널을 구현할 수 있다. 특히, 무선 랜에서 MAC 주소를 랜덤화하여 은닉 채널을 구현한 연구가 진행되었다 [10]. 해당 연구에서는 프로브 요청 프레임 내 출발지 주소 필드에 랜덤한 일회성 MAC 주소로 인

코딩된 비밀메시지를 은폐한다. 또한, 은닉 채널을 형성하기 위해 프로브 요청 프레임 내 순서 제어 필드의 단편화 번호와 순서 번호의 값을 활용한다. 해당 연구에서 제안한 은폐 통신은 은폐된 메시지를 올바르게 해석하기 위해 공유한 사전을 가지며 이는 강력한 보안성을 제공한다. 또한, 일반 전송 채널 내에서 비밀 데이터를 교환함으로써 기존 무선 랜 환경에서의 MAC 주소 기반 은닉 채널보다 높은 처리량을 보인다.

2.3 무선 이동통신

5G와 같은 무선 이동통신의 적용 범위가 확장됨에 따라 새로운 아이디어, 기술이 계속해서 구현되고 있다. 하지만 이러한 확장성은 새로운 취약점이나 위험을 불러오게 된다. 이와 같은 환경에서 기밀성을 보장하기 위해 데이터 통신을 탐지 불가능하도록 은닉하는 방법이 사용된다. 특히, 5G 환경에서 무선 접속 네트워크(RAN)의 소프트웨어와 가상 네트워크 슬라이싱을 활용하여 개인에게 서비스되는 셀룰러 통신(Private Cellular Connectivity as a Service, PCCaaS)을 구축하고, 은폐 통신이 가능하도록 은닉 패킷을 생성하여 스테가노그래피를 구현한 SteaLTE가 연구되었다 [11]. SteaLTE는 올바른 대상과 기밀 데이터를 교환하기 전 서로 인증하는 과정과 은닉 패킷을 생성하여 전송 시 더미 트래픽에 임베딩하는 과정으로 구성된다. 또한, QPSK 변조를 통해 데이터를 은폐 전송하는 스테가노그래피 시스템을 설계하였다.

2.4 저전력 광역 무선통신

저전력 광역 무선통신은 저전력, 안정적인 범위, 대규모 단말기 접속이 가능하므로, 사물인터넷 또는 스마트시티와 같은 분야에서 사용된다. 이러한 저전력 광역 무선통신 환경에서 LoRa 패킷을 전송할 때 처프의 진폭을 변조하고 기밀 데이터를 임베딩하여 은폐 통신이 가능한 LoRa PHY가 연구되었다 [12]. 은닉 LoRa 패킷은 CloakLoRa을 통해 주파수를 유지한 상태로 처프의 진폭이 변경되고, 은닉 정보가 임베딩된다. 이러한 은닉 패킷은 COTS LoRa 노드를 통해 전송되며, 소프트웨어 정의 라디오에 의해 수신된다. 해당 논문에서 설계한 시스템에서는 기존 처프 확산 스펙트럼이 처프의 초기 주파수만 사용하여 복조하는 반면, 제안한 방법은 은폐 통신을 수행하기 위해 진폭 변조를 이용하여 기밀 메시지를 복조한다.

III. 무선 은폐 통신의 도전과제

3.1 무선 Ad-hoc 통신의 도전과제

본 연구팀이 조사한 Ad-hoc 환경에서의 은폐 통신은 네트워크 프로토콜의 패킷 구조를 유지하면서 프로토콜 내 특정 필드에 패턴 추가, 비트 변조 및 기밀 데이터를 임베딩한다 [13]. 이러한 네트워크 프로토콜 변조를 통해 데이터를 은폐하여 전송하는 은폐 통신 기술은 서로 다른 디바이스로 구성된 Ad-hoc 아키텍처에서 리소스가 제한되는 상황을 고려하여 계산 집약적이지 않아야 한다.

3.2 무선 랜 통신의 도전과제

무선 랜 환경에서 은닉 채널을 생성하고 스테가노그래피를 구현하기 위해, 프로브 요청 시 MAC 주소를 랜덤화하는 기법이 활용된다. 이와 같은 방식은 MAC 주소의 랜덤화가 쉽게 감지되는 문제와 글로벌 MAC 주소의 검색을 통해 탐지될 수 있는 한계를 가지고 있다 [10]. 따라서, 순서 번호와 같은 추가 필드를 랜덤화하거나 핑거프린트를 변경하는 등의 추가적인 방법을 통해 탐지 가능성을 낮추는 방안이 필요하다.

3.3 무선 이동통신의 도전과제

무선 이동통신 환경에서는 무선 접속망 소프트웨어가 광범위하게 사용되고 있으며, 특히 셀룰러에서 가상 네트워크 슬라이싱을 통해 연결성을 제공하고, 프라이빗 네트워크의 형태로 개인에게 서비스될 수 있다 [14]. 또한, 이동통신 환경 내 스테가노그래피와 은폐 통신을 적용하기 위해 기밀 데이터를 변조된 심볼에 임베딩하여 도청을 방지하도록 설계할 수 있다 [11]. 이러한 무선 이동통신 환경에서의 스테가노그래피는 복조 시 오류 발생 문제와 장거리 통신 및 수신기와 송신기의 유동성 문제를 해결하여야 한다.

3.4 저전력 광역 무선통신의 도전과제

저전력 광역 네트워크에서 LoRaWAN과 같

은 프로토콜은 대칭 암호를 사용하여 애플리케이션 계층과 네트워크 계층을 보호한다. 하지만, 네트워크 트래픽 수신 및 분석을 통해 도청될 수 있으므로 은폐 통신을 구현함으로써 데이터의 기밀성을 보장하여야 한다 [15]. 저전력 광역 무선통신은 다양한 디바이스가 활용되며 낮은 배터리 수명, 벽이나 장애물과 같은 환경으로 구성되어있으므로 진폭이나 위상, 비트 전송률 변조 등의 계산 효율성과 올바른 신호를 수신하기 위한 신호 강도를 고려하여야 한다.

IV. 결론 및 향후 연구

본 논문에서는 무선통신 환경에서 통신 거리와 범위에 따른 통신 방식을 무선 Ad-Hoc, 무선 랜, 무선 이동통신, 저전력 광역 무선통신으로 구분하였으며, 공기를 매체로 브로드캐스팅되는 무선 채널의 특성에서 메시지 노출을 방지하기 위해 공개된 채널로 은닉 메시지를 전송하는 은닉 채널과 데이터를 숨기기 위한 스테가노그래피 기법을 조사하였다. 또한, 조사를 통해 각 무선통신 환경에서 암호화 없이 스테가노그래피를 적용하기 위해 어떤 도전과제가 있는지 식별하였다. 향후 저전력 광역 무선통신 환경에서 스테가노그래피를 통해 장거리에 있는 디바이스와 단방향 상호 인증이 가능한 통신체계를 연구하고자 한다.

[참고문헌]

[1] Wu, Huihui, et al. "Achieving Covertness and Secrecy in Wireless Communications with Active Attackers." 2024 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2024.

[2] Caviglione, Luca. "Privacy-Leaking and Steganographic Threats in Wireless Connected Environments." Towards a Wireless Connected World: Achievements and New Technologies. Cham: Springer International Publishing, 2022. 17-34.

[3] Zhang, X., Heys, H. M., & Li, C. (2012). Energy efficiency of encryption schemes applied to wireless sensor networks. Security and Communication Networks, 5(7), 789-808.

[4] Singh, A., & Dhir, V. (2017). An Analytical Survey on Covert Channels in Ad-hoc Wireless Network. International Journal of Advanced Research in Computer Science, 8(4).

[5] Physical Layer Covert Communication in B5G Wireless Networks—its Research, Applications, and Challenges

[6] Al-Emadi, Sara, and Aisha Al-Mohannadi. "Towards enhancement of network communication architectures and routing protocols for FANETs: A survey." 2020 3rd international conference on advanced communication technologies and networking (CommNet). IEEE, 2020.

[7] Mukhedkar, Moresh M., et al. "An Innovative Approach Using Cyber Security for Steganography for Wireless Adhoc Mobile Network Application." 2024 International Conference on Science Technology Engineering and Management (ICSTEM). IEEE, 2024.

[8] Natkaniec, M., & Bieryt, N. (2022). An analysis of BSS coloring mechanism in IEEE 802.11 ax dense networks. International Journal of Electronics and Telecommunications, 68(4).

[9] Natkaniec, M., & Bieryt, N. (2023). An Analysis of the Mixed IEEE 802.11 ax Wireless Networks in the 5 GHz Band. Sensors, 23(10), 4964.

[10] Teca, G., & Natkaniec, M. (2023). A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization. Applied Sciences, 13(14), 8000.

[11] Bonati, Leonardo, et al. "SteaLTE: Private 5G cellular connectivity as a service with full-stack wireless steganography." IEEE INFOCOM 2021-IEEE Conference on Computer Communications. IEEE, 2021.

[12] Hou, N., Xia, X., & Zheng, Y. (2022). Cloaklora: A covert channel over lora phy. IEEE/ACM Transactions on Networking, 31(3), 1159-1172.

[13] Mallikarachchi, Dilshani, KokSheik Wong, and Joanne Mun-Yee Lim. "An authentication scheme for FANET packet payload using data hiding." Journal of Information Security and Applications 77 (2023): 103559.

[14] https://www.fierce-network.com/wireless/5g-private-network-or-network-slice

[15] Qadir, Junaid, et al. "Analysis of LPWAN: Cyber-Security Vulnerabilities and Privacy Issues in LoRaWAN, Sigfox, and NB-IoT." Low-Power Wide-Area Networks: Opportunities, Challenges, Risks and Threats. Cham: Springer International Publishing, 2023. 139-170.