패킷 간 지연 기반 은닉 시간 채널 알고리즘 분석

손승환, 권덕규, 오지현, 박영호

경북대학교

sonshawn@knu.ac.kr, kdk145@knu.ac.kr, j2hnoh@knu.ac.kr, parkyh@knu.ac.kr

Analysis of inter-packet delay-based covert timing channel algorithms

Son Seung Hwan, Kwon Deok Kyu, Oh Ji Hyeon, Park Young Ho

Kyungpook National Univ.

요 약

본 논문에서는 패킷 간 지연을 활용한 무선 은닉 시간 채널 알고리즘에 대해서 소개한다. 기존에 제안된 알고리즘으로는 On-off, DPOI, Time-Replay, PPCTC 등이 존재한다. PPCTC를 제외한 대부분의 알고리즘이 예전의 통신환경을 기반으로 제시되었기 때문에 최신 통신환경에서 활용되기 어렵다. 또한, PPCTC의 경우 하나의 패킷 손실에 대해서만 저항성을 가지기 때문에 실제 무선 통신환경에서 활용되기에 견고성 측면에서 문제가 발생할 수 있다. 본 연구자는 기존에 연구된 은닉 시간 채널 알고리즘을 토대로 추후 개선된 알고리즘을 제시할 예정이다.

Ⅰ. 서 론

은닉 채널이란 정보전송을 위해 만들어지지 않은 채널을 통해서 정보를 전송하는 것을 의미한다. 은닉채널의 생성 방법에 따라서 크게 은닉 저장 채널, 은닉 시간 채널 두가지로 분류할 수 있다. 은닉 저장 채널이란 비밀 메시지를 네트워크 패킷에 사용되지 않는 필드에 숨겨서 전송하는 것이다. 예를 들어, 네트워크 패킷의 헤더 필드는 페이로드의 무결성 또는 인증을 달성하기 위해 존재하며 독립적인 데이터는 포함되지 않는다. 이러한 허점을 이용하여 비밀 메시지를 전송할 수 있다. 은닉 시간 채널이란 고의적인 패킷 손실, 패킷 간 시간 간격, 패킷 재정렬 등을 통하여 은닉 메시지를 전송하는 방식이다. 예를 들어, 일반적인 무선 통신환경의 경우 패킷 간 시간 간격이 정해져있다. 하지만 패킷 전송과정에서 백색 소음 등으로 인해 패킷이 조금 더 일찍 도착하거나 더 늦게 도착할 수 있다. 패킷 간 시간 간격을 활용하는 은닉채널의 경우 무선 통신의 이러한 특성을 활용하여 임의로 패킷을 늦게 전송하거나 일찍 전송하는 방식으로 은닉 메시지를 전송할 수 있다. 은닉 채널은 무선 통신 환경에서의 공격 벡터로 간주되어 왔으나, 최근에는 안전하게 메시지를 전송하기 위해 은닉 채널의 활용성 또한 강조되고 있다.. 무선 통신환경에서 공개키 또는 대칭키를 활용하여 메시지를 송수신하는 경우 다양한 공격에 노출될 수 있으나, 은닉 채널을 통해 메시지를 송수신하는 경우 원천적으로 공격이 불가능하다 [1],[2],[3],[4]. 본 논문에서는 다양한 최신 은닉 시간 채널을 소개하고 연구동향을 분석한다.

Ⅱ. 본 론

2-1. On-off

On-off는 2004년 Cabuk 등이 처음으로 제안한 은닉 시간 채널 알고리즘으로 고의적인 패킷 손실을 발생시켜 은닉 메시지를 전송한다 [5]. 수신자와 송신자는 사전에 시간 간격을 합의한다. 이후, 정해진 시간 간격 안에 송신자가 패킷을 전송하면 수신자는 이를 비트 '1'로 해석하고 패킷을 전송하지 않으면 수신자는 이를 비트 '0'로 해석한다. On-off 알고리즘은 초기의 알고리즘으로서 탐지되기가 매우 쉬우며 탐지자가 해당 알고리즘을 인지하고 있는 경우 은닉 메시지도 쉽게 노출될 수 있다.

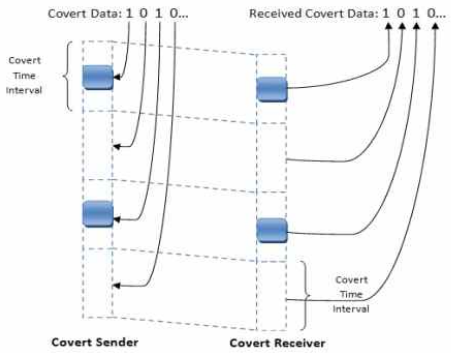

그림 1. On-off 알고리즘.

2-2. DPOI (Delayed Packet One Indicator)

Rezaei 등은 On-off 알고리즘의 낮은 전송 용량을 해결하기 위해 DPOI 알고리즘을 제안하였다 [6]. 무선 통신 채널에서는 표준 패킷 간 지연 값이 존재한다. 송신자는 비트 '0'을 보낼 경우 정상적으로 패킷을 전송하고 비트 '1'을 보낼 경우 정상 보다 조금 지연시켜 패킷을 전송한다.

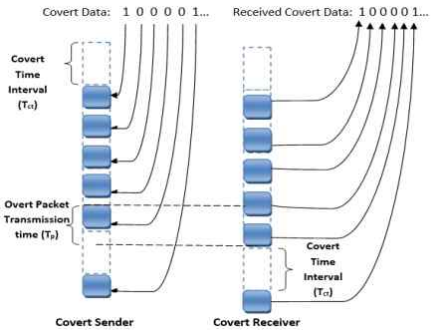

그림 2. DPOI 알고리즘.

2-3 Time-Replay

기존의 은닉 채널 생성 알고리즘은 패킷 간 지연의 분포에 변화를 발생시키기 때문에 상대적으로 탐지되기 쉽다. 이를 해결하기 위해 Cabuk은 Time-Replay 알고리즘을 제안하였다 [7]. 이 방식에서는 정상 네트워크에서 발생한 패킷 간 지연 값을 미리 수집한 후 송신자와 수신자는 임계값을 합의하여 은닉 메시지를 송수신할 수 있다. 예를 들어, 임계값을 평균으로 설정할 경우 패킷 간 지연 데이터는 두 구간으로 나뉘게 된다. 송신자는 비트 '1'을 전송하기 위해서는 첫 번째 구간의 패킷 간 지연 값을 사용하고 비트 '0'을 전송하기 위해서는 두 번째 구간의 패킷 간 지연 값을 사용할 수 있다. 경우에 따라서 다수의 임계값을 활용할 수 있다.

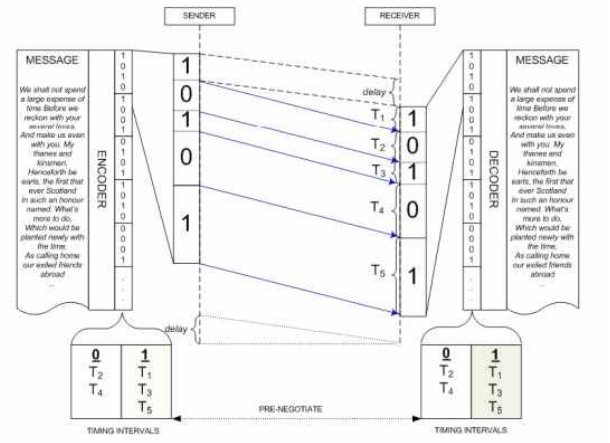

그림 3. Time-Replay 알고리즘.

2-4. PPCTC (PingPong Covert Timing Channel)

PPCTC는 2022년 Seong 등에 의해 제안된 은닉 시간 채널 생성 알고리즘이다. [8] IEEE 802.11 기반 Wi-Fi 통신환경에서는 패킷 간 시간 간격이 일반적으로 102.4ms으로 고정된다. PPCTC 알고리즘에서는 이를 활용하여 비트 '0'을 보낼 경우 102.4ms보다 이르게 다음 패킷을 전송하고 비트 '1'을 보낼 경우 102.ms보다 조금 더 늦게 다음 패킷을 전송한다. 패킷 수신자는 이를 토대로 은닉 비트를 알아낼 수 있다.

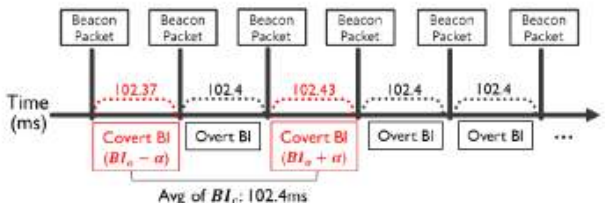

그림 4. PPCTC의 은닉 비트 전송 방법.

또한 PPCTC에서는 비트 인코딩 방식을 포함한다. 연속된 은닉 비트가 '01'으로 도착할 경우 경우 이는 메시지 '0'으로 간주되며 연속된 은닉비트가 '01111'으로 도착할 경우 이는 메시지 '1'로 간주된다. PPCTC 방식은 최근에 제안된 은닉 시간 채널 생성 알고리즘으로 기존의 알고리즘에 비해 많은 부분에서 개선되었으며, 특히 하나의 패킷이 손실되더라도 스스로 비트를 복구할 수 있다는 강점을 가진다.

Ⅲ. 결론

본 논문에서는 은닉 시간 채널 알고리즘을 분석 및 파악하였다. 무선통신 환경을 통한 메시지 송수신은 공격자에 의한 재전송, 위장, 중간자 공격 등에 취약할 수 있다. 하지만 통신 당사자간 은닉 시간 채널을 통해 메시지를 송수신한다면 제 3자가 둘 간의 메시지 송수신여부를 인지하지 못하게 함으로써 무선 채널에서 발생할 수 있는 공격을 원천적으로 예방할 수 있다. 기존에 제안된 패킷간 지연 기반의 은닉 시간 채널은 과거의 통신 환경을 기반으로 제안되었기 때문에 최근에 활용되는 6G 및 와이파이 통신 환경에서 활용되기 어려울 수 있다. 특히, 대다수의 기존 알고리즘은 패킷 손실에 대해서 매우 취약하다. PPCTC의 경우도 한 개의 패킷 손실에 대해서는 저항성을 가지지만 두 개 이상의 패킷이 연속적으로 손실될 경우 복구기능을 상실하여 메시지를 성공적으로 전송하기 어렵다. 따라서 본 연구자는 추후 연구를 통해 두 개 이상의 패킷 손실에 대한 저항성을 가지며 최신 IEEE 802.11 환경 등 와이파이 환경에서 활용될 수 있는 은닉 시간 채널을 제안할 예정이다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

[1] D. K. Kwon, S. J. Yu, J. Y. Lee, S. H. Son, and Y. H. Park, "WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks," Sensors, pp. 936-958, Jan. 2021.

[2] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," IEEE Transactions on Network Science and Engineering, pp. 1346 - 1358, May 2022.

[3] K. Park, J. Lee, A. K. Das, and Y. Park, "BPPS:Blockchain-enabled privacy-preserving scheme for demand-response management in smart grid environments," IEEE Transactions on Dependable and Secure Computing pp. 1719 - 1729, Mar./Apr. 2023.

[4] D. Dharminder, C. B. Reddy, A. K. Das, Y. Park, and S. S. Jamal, "Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT," IEEE Internet of Things Journal, pp. 2680 - 2692, Feb. 2023.

[5] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: Design and detection," In Proceedings of the 11th ACM conference on Computer and communications security, 2004, pp. 178 - 187.

[6] F. Rezaei, M. Hempel, P. L. Shrestha, and H. Sharif, "Achieving robustness and capacity gains in covert timing channels," in 2014 IEEE International Conference on Communications (ICC), 2014, pp. 969 - 974.

[7] S. Cabuk, "Network covert channels: Design, analysis, detection, and elimination," PhD Dissertation, Pordu University, West Lafayette, IN, USA, 2006.

[8] H. Seong, I. Kim, Y. Jeon, M.-K. Oh, S. Lee, and D. Choi, "Practical covert wireless unidirectional communication in IEEE 802.11 environment," IEEE Internet of Things Journal, pp. 1499 - 1516, Jan. 2023.