무선 오버쉐도윙 공격의 구현 및 성능 평가

김경민, 김용강, 박재형, 임혁
광주과학기술원 전기전자컴퓨터공학부
{gyungminkim, ygkim, jaehyoungpark, hlim}@gist.ac.kr

Implementation and Performance Evaluation of Wireless Overshadowing Attack

Gyungmin Kim, Yonggang Kim, Jaehyoung Park, and Hyuk Lim
Gwangju Institute of Science and Technology (GIST)

요 약

오버쉐도윙 기법은 두 신호가 충돌할 경우 더 강한 세기의 신호를 따르는 각도 변조(angular modulation)의 특성을 이용하여 전송중인 신호를 더 강한 세기의 공격 신호로 덮어씌우는 공격 기법이다. 이때 공격 신호를 통한 신호 조작(signal manipulation)이 전송 신호가 수신 노드에 도달하는 정확한 시간에 이루어져야 하고, 기존의 전송신호를 덮어씌울 수 있을 정도의 신호세기가 요구된다. 본 논문에서는 실험을 통해 공격 신호의 시간 동기화와 신호세기에 따른 오버쉐도윙 공격의 성능을 측정한다.

Ⅰ. 서 론

전송 노드로부터 수신 노드로의 데이터 전송이 이루어지는 무선채널에는 해당 전송 신호와 함께 그 외 다른 노드들로부터의 전송 신호가 동시에 존재할 수 있고, 수신 노드 외의 다른 노드들도 전송 노드로부터의 신호를 수신하는 것이 가능하다. 이러한 무선채널의 특성으로 동일 무선채널 내의 공격자는 전송 노드의 신호를 도청하거나, 의도적으로 방해 신호를 생성하여 수신 노드의 신호 수신율을 낮추는 것이 가능하다. 신호 수신을 방해하기 위한 방법에는 일정 범위의 주파수 대역에 대해 지속적으로 강한 신호 세기의 방해 신호를 전송하는 콘스턴트 재밍(constant jamming), 도청중인 채널을 통한 신호 전송이 감지되는 경우에만 방해 신호를 생성하는 리액티브 재밍(reactive jamming) 등의 여러 재밍 기법이 있으며, 이와 더불어 단순히 상대의 통신을 가로막는 것을 넘어 수신되는 데이터를 왜곡시키는 오버쉐도윙 공격(overshadowing attack) 기법이 있다 [1,2].

오버쉐도윙 공격은 수신 노드가 공격자의 존재를 모른 채 왜곡된 신호를 정상 신호로 인식하게 함과 동시에 전송 노드가 데이터 전송이 성공적으로 이루어졌다고 여기게 하는데 목적이 있으며, 수신 노드가 왜곡된 정보를 토대로 다음 프로세스를 진행하게 된다는 점에서 단순히 통신을 방해하는 재밍 기법보다 더욱 치명적이다. 이러한 오버쉐도윙 공격은 무선채널상의 전송중인 신호에 신호 조작(signal manipulation)을 가하여 수행되는데, 공격 신호를 통한 조작이 전송 신호가 수신 노드에 도달하는 정확한 시간에 이루어져야 하고 기존의 전송신호를 덮어씌울 수 있을 정도의 신호세기가 요구된다. 또한 조작된 신호는 수신 노드가 예상하는 프레임 구조와 데이터를 따라야 하기에, 공격 대상 신호의 통신 프로토콜 정보 및 전송 데이터 분석을 필요로 한다. 앞의 요구 조건들로 인해 오버쉐도윙 공격은 구현에 어려움이 따르지만 물리 계층 공격을 통해 인식되지 않고 상대를 기만할 수 있다는 점에서 큰 이점이 있고, 오버쉐도윙 공격을 구현하기 위한 연구들이 진행되고 있다 [3]. 본 논문에서는 오버쉐도윙 공격을 구현하기 위한 실험 환경을 구축하였고, 공격 신호의 전송 세기와 시간 동기화의 정확도에 따른 오버쉐도윙 공격의 성능을 측정하고 평가하였다.

Ⅱ. 본론

2.1 오버쉐도윙 공격의 원리

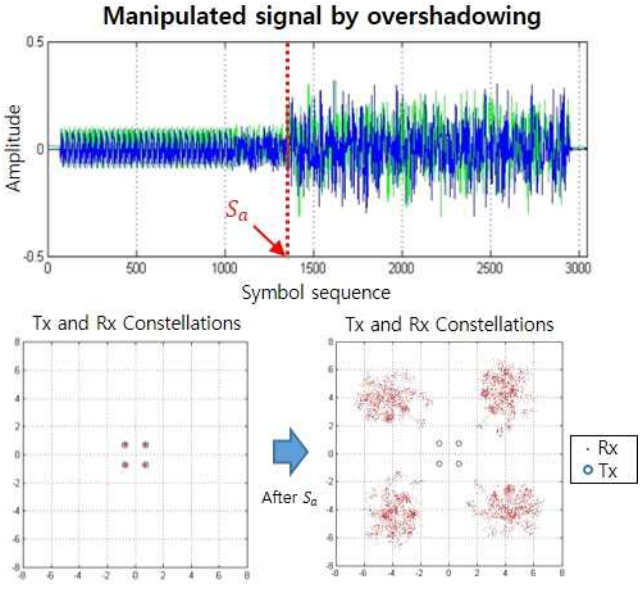

그림 1. 오버쉐도윙을 통한 신호 조작

그림 1은 QPSK 변조 방식을 이용한 통신에서 전송중인 신호에 S_a 이후부터 강한 세기의 공격 신호가 가해진 모습을 나타낸다. 이 경우 공격 신호가 기존 전송 신호를 덮어씌우게 되고 수신 노드가 신호를 복조하는 과정에서 공격 신호를 인식하게 된다. 오버쉐도윙 기법은 위와 같이 두 신호가 충돌할 경우 더 강한 세기의 신호를 따르는 각도 변조(angular modulation)의 특성을 이용하여 전송중인 신호를 더 강한 세기의 신호로 덮어씌우는 공격 기법이다. 공격 신호를 통해 공격자가 의도하는 신호를 타겟 노드가 수신하도록 유도할 수 있고, 이에 따라 데이터를 조작하는 것이 가능하다.

2.2 오버쉐도윙 공격의 과정

오버쉐도윙 공격이 이루어지는 과정은 다음과 같다. 먼저 공격하고자 하는 두 노드간의 통신 신호를 도청하여 통신 프로토콜 및 전송 데이터를 분석하고, 이를 통해 해당 프로토콜과 프레임 구조를 고려한 공격신호를 생성한다. 이후 공격하고자 하는 전송 신호가 포착될 경우 즉각적으로 공격 신호를 전송하여 전송중인 신호의 일부를 공격 신호로 덮어씌우게 된다. 그림 2는 오버쉐도윙 공격에 따라 수신된 정보가 왜곡된 것을 보여준다. 공격자는 공격 신호의 통신 프로토콜 정보에 기반하여 공격신호를 생성하기에 수신 노드는 CRC를 이용한 오류 검사에서 공격 신호로 인한 신호의 변화 여부를 인식할 수 없게 된다.

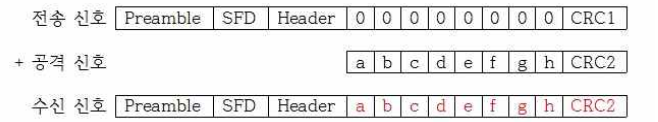

그림 2. 오버쉐도윙에 따른 수신 신호 왜곡

2.3 시간 동기화와 신호세기에 따른 오버쉐도윙 공격의 성능

오버쉐도윙 공격을 위해서는 정확한 타이밍이 요구되고 또한 기존의 전송신호를 덮어씌울 수 있을 정도의 신호세기가 요구된다. 때문에 두 가지 중 하나의 요구조건에라도 문제가 발생할 경우 오버쉐도윙 공격의 성공률은 크게 낮아지게 된다. 먼저 정확한 타이밍 조건을 만족시키지 못할 경우 수신된 데이터와 공격 노드가 의도한 데이터가 일치하지 않게 되고, 이것은 오버쉐도윙 공격의 실패를 의미한다. 다음으로 신호세기 조건을 만족시키지 못할 경우 수신 신호를 의도하는대로 조작하는 것이 불가능함에 따라 공격 신호가 단순한 재밍 신호로 그치게 된다.

Ⅲ. 테스트베드 구현 및 실험결과

3.1 실험 환경

타이밍과 신호세기에 따른 오버쉐도윙 공격의 성능을 측정하기 위한 실험을 진행하였다. 무선통신 실험을 수행하기 위하여 SDR 장비인 Wireless Open-Access Research Platform (WARP)를 이용하였다 [4]. 전송 안테나와 공격 안테나를 각각 수신 안테나로부터 2m 거리에 배치하였고, 시간 동기화에 따른 정확한 성능 평가를 위하여 두 안테나를 동일 노드에 연결하였다. 전송 노드의 프레임 구조는 preamble 과 데이터로 이루어지고 preamble 전송이 끝나는 것과 동시에 공격 신호가 전송되도록 하였다. 통신 방식은 OFDM (orthogonal frequency division multiplexing)과 QPSK (quadrature phase shift keying) 변조 방식을 이용하였고 2.4GHz 대역에서 통신을 수행하였으며 전송 노드의 신호세기는 -25dBm 으로 설정하였다. 신호세기에 의한 영향을 측정하기 위하여 공격 노드의 신호세기를 -22dBm 에서 -13dBm 까지 3dBm 씩 증가시키며 진행하였고, 시간 동기화에 의한 영향을 측정하기 위하여 공격 신호의 전송 지연을 0 ns 에서 100 ns 까지 25 ns 씩 증가시키며 수행하였다.

3.2 실험 결과

그림 3 은 공격신호의 시간 동기화와 신호세기에 따른 오버쉐도윙 공격의 성공률을 나타낸 것이다. 신호 왜곡 기법은 수신 노드로 하여금 공격 노드의 의도대로 신호를 수신하게 하는 것이 목적이므로 공격 신호가 오류없이 수신된 것을 성공으로 판단하였다. 공격신호의 시간 동기화 오차가 증가할수록 성능이 감소하고, 신호세기가 강할수록 성능이 증가하는 것을 볼 수 있다. 또한 공격 신호세기가 전송 신호의 16배 이상이고 공격 신호의 전송 지연이 25 ns 이하일 때 95% 이상의 확률로 오버쉐도윙이 이루어진 것을 통해 해당 조건을 만족할 경우 오버쉐도윙 공격이 현실적으로 가능하다는 것을 확인하였다. 위의 결과를 토대로 오버쉐도윙 공격을 위해서는 공격 노드를 수신 노드와 근접시켜 전파지연 시간을 줄이고 근접한 거리를 통한 적은 경로손실 이득을 취하는 것이 필수적이다.

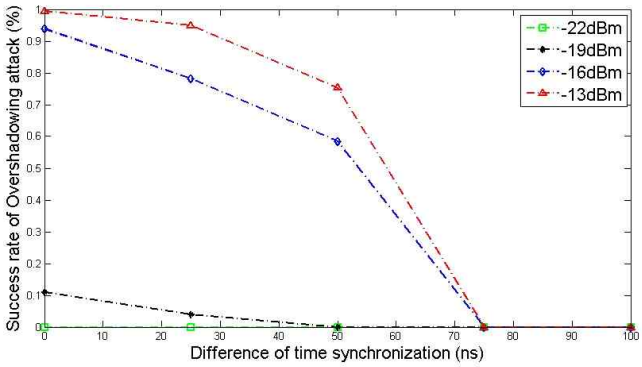

그림 3. 시간 동기화와 신호세기에 따른 오버쉐도윙 공격의 성능

Ⅳ. 결론

본 논문에서는 오버쉐도윙 공격 기법의 성능 평가를 위해, SDR 장비를 통해 테스트베드를 구축하고 실제 환경에서 공격 신호의 시간 동기화와 신호세기에 따른 오버쉐도윙 공격의 성능 측정을 수행하였다.

ACKNOWLEDGMENT

본 연구는 광주과학기술원 전자전특화연구센터를 통한 방위사업청과 국방과학연구소 연구비 지원으로 수행되었습니다.

참 고 문 헌

[1] C. Pöpper, N. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," European Symposium on Research in Computer Security, pp. 40-59, September. 2011.

[2] M. Wilhelm, et al. "Short paper: reactive jamming in wireless networks: how realistic is the threat?," Proceedings of the fourth ACM conference on Wireless network security, p.47-52, June. 2011.

[3] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in IEEE 802.15.4 wireless networks," in Workshop Proc. MMB '12, pp. 29-31, Mar. 2012.

[4] Wireless Open-Access Research Platform (WARP). [Online]. Available: http://warpproject.org/trac