원격 키리스 엔트리시스템에 대한 재생공격 무력화 기법

김영민 · 김성환

경상대학교

Defense Mechanism against Replay Attack on Remote Keyless Entry System

Young Min Kim · Seong Hwan Kim

Gyeongsang National University

E-mail : kymin328@gmail.com, seonghwan.kim@gnu.ac.kr

요 약

1세대 RKE 시스템은 재생공격에 매우 취약하며 2세대 RKE 시스템의 암호기법 또한 네 번에서 여덟 번의 수신으로 무력화될 수 있다. RKE 시스템의 보안성을 강화하기 위해 RKE 시스템에 물리 계층 보안 기법을 도입하여, 도청자가 수신하는 신호의 품질을 저하시켜 재생공격을 무력화 하는 기법을 제안한다.

ABSTRACT

The first-generation RKE(Remote Keyless Entry) system is very vulnerable to replay attacks and the encryption of the second-generation RKE system is known to be disabled by four to eight signal receptions and analysis. In order to enhance the security of the RKE system, we introduce a physical-layer security methods in the RKE system and propose a technique to disable the replay attack by reducing the quality of the signal received by an eavesdropper.

키워드

replay attack, remote keyless entry system,

Ⅰ. 서 론

전자소자 및 통신기술의 발달로 자동차 및 가정의 보안방식이 과거의 열쇠를 사용하는 방식에서 키폽을 이용한 원격제어 방식으로 바뀌었다. 특히, 자동차 문 열림 및 시동 장치에 대한 보안 방식에 큰 변화가 있었으며 대표적 보안 방법으로 이모빌라이저, PKE 시스템 (passive keyless entry), RKE 시스템 (remote keyless entry) 이 있다 [1]. 이모빌라이저는 무단 시동을 방지하기 위해 차량에 설치하는 RFID 장치로써 사용자의 키폽에서 보내는 코드와 이모빌라이저에 저장된 코드가 일치하면 사용자의 시동이 허용된다. 대부분의 이모빌라이저는 인증을 위한 암호기법을 사용하며 차량과 키폽 사이에 도전-응답 프로토콜을 사용한다. PKE 시스템은 이모빌라이저와 유사하게 양방향 도전-응답 방식을 사용하며 1 미터 가량의 근거리에서 작동한다. 키폽이 유효한 응답을 보내면 문이 개방되고, 경보 시스템이 꺼지고, 시동이 허용된다. 최근 사용자와 차량이 서로 멀리 떨어진 상태에서 중계공격을 통해 PKE 시스템이 무력화 될 수 있음이 증명되었으며 [2] 그 후 PKE 시스템의 취약점을 개선하고자 하는 연구들이 다수 수행되었다.

RKE 시스템은 단방향 통신을 기반으로 하며 무선 송신기가 내장된 키폽에서 차량으로 데이터가 전송된다. RKE 시스템은 사용자가 멀리서도 차량 문을 잠그거나 열수 있게 하며, 도난 방지 알람을 조종할 수 있게 한다. 1세대 RKE 시스템은 키폽에서 고정 코드가 전송되고 차량이 이를 성공적으로 수신하면 고정 코드에 해당하는 제어명령이 수행된다. 이러한 시스템은 도청자가 신호를 수신 후 저장했다가 추후 정규 사용자인 것처럼 신호를 전송하는 재생 공격에 매우 취약하다. 이후에 개발된 2세대 RKE 시스템은 암호기법이 도입된 롤링 코

드 시스템으로, 버튼을 누를 때 마다 카운터 값이 증가한다. 차량에서 코드를 복호하고 카운터 값을 수신 한 후, 수신한 카운터 값이 마지막으로 검증된 카운터 값보다 크면 인증된다. 하지만 이러한 메커니즘 또한 4~8개의 롤링코드를 도청함으로써 몇 분 이내에 암호화 키를 복원해낼 수 있다 [1]. 최근 RKE 시스템의 암호키 복원을 어렵게 하는 암호화 기법들이 연구되었으며 또한 새로운 공격 기법이 발표되었다 [3]. 그러나 신호를 수집한 후 슈퍼 컴퓨터 등을 활용하면 암호키 복원이 가능할 수 있다.

최근 인위적인 간섭 신호를 도청자 쪽으로 전송하여, 도청자 측 수신신호의 신호대잡음간섭비(Signal-to-noise-interfernce ratio, SINR) 를 낮추어 도청자가 복원한 이진신호의 신뢰성을 떨어뜨리는 방식으로 보안성을 증대시키는 연구가 진행되어 왔다 [4]. 기존의 물리 계층 보안 연구는 다음의 다섯 가지로 분류된다: 이론적 보안 용량 계산, 전송 전력 조절, 부호화 기법, 채널 활용, 신호 검출 기법. 그 중 전송 전력 조절은 방향성 안테나의 사용과 인위적인 잡음을 통하여 공격자의 공격을 막는 물리 계층 기법이라고 할 수 있다.

본 연구는 RKE 시스템에 물리 계층 보안 기법을 도입하여, 도청자가 수신하는 신호의 품질을 저하시켜 재생공격을 무력화시키는 것을 목적으로 한다. 이는 수집한 신호들의 품질을 저하시켜 롤링 코드를 사용하는 RKE 시스템의 암호를 알아내고자 하는 공격을 더욱 어렵게 만들 수 있다. 보다 구체적으로, 키폽에서 신호가 전송되는 동안 차량 주변에 배치된 복수의 안테나에서 간섭신호 전송되어 차량 인근에 있는 도청자 측 수신신호의 SINR을 감소시키며, 반면 차량 내부의 수신기에는 간섭신호가 영향을 미치지 않도록 신호처리하는 방안을 제안한다.

II. RKE 시스템

RKE 시스템은 키폽의 버튼을 눌렀을 때 키폽에서 차량 방향으로 데이터가 전송는 단방향 시스템이다 RKE 시스템의 주파수 대역은 북아메리카의 315MHz 대역과 유럽의 433MHz 또는 868MHz 대역이 있으며, 신호의 일반적인 도달 범위는 수십 미터에서 수백 미터이다. 대부분의 RKE 시스템은 Amplitude Shift Keying (ASK)과 Frequency Shift Keying (FSK) 변조 방식을 사용한다. 데이터 비트들을 인코딩하는 방법 중에서 가장 널리 사용되는 방법은 맨체스터 인코딩과 펄스-폭 인코딩이다. 비트 전송률의 범위는 1 kBit/s 에서 20 kBit/s 이다. 일반적인 RKE 시스템의 패킷은 그림 1과 같이 프리앰블, 시작 패턴, 암호화된 데이터 페이로드 및 체크섬으로 구성된다. 데이터 페이로드에는 일반적으로 키폽의 고유 시별자 (UID), 롤링 카운터 값 및 명령값이 포함된다.

예를 들어 폭스바겐 그룹의 일부 차량에 채택된 RKE 시스템은 434.4MHz의 주파수를 사용하며 온-오프 변조(OOK) 또는 맨체스터 인코딩을 사용한다 [1].

그림 1. RKE 시스템의 패킷구조

III. RKE 시스템에 대한 재생공격 및 무력화 기법

III-A. RKE 시스템에 대한 재생공격

재생공격은 공격자들이 유효한 신호가 전송되는 시점에 그 신호를 도청 및 저장하여, 추후 정규 사용자인 것처럼 신호를 전송하는 공격방법이다. 원래의 송수신되는 데이터를 그대로 보내는 특성으로 인해 공격자는 암호화된 데이터라도 해독 없이 전송할 수 있고 수신자는 공격자의 재생공격을 원래 송신하던 유효한 데이터인 전송인 것처럼 여기게 된다. 롤링 코드를 사용하지 않는 1세대 RKE 시스템의 경우 재생공격으로 쉽게 보안이 뚫린다.

III-B. 제안하는 재생 공격 무력화 기법

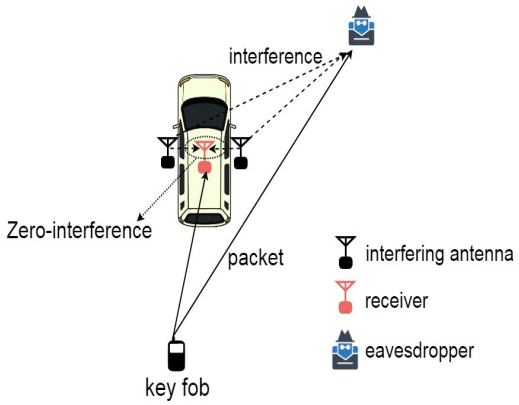

그림 2. 재생공격 무력화 기법

그림 2는 재생공격을 시도하는 도청자가 있는 상황에서 이를 무력화하는 제안 기법을 묘사하고 있다. 차량 중앙에는 사용자의 패킷을 수신하는 수신기가 달려있고, 도청자에게 간섭신호를 발생시키는 두 개의 간섭 안테나가 차량의 양 옆에 장착되어 있다. 도청자는 차량 주변에서 사용자의 패킷을 수신하고 있다.

사용자가 키폽의 버튼을 눌러서 패킷을 전송하면, 차량의 간섭안테나는 간섭을 발생시키며 도청자의 수신 SINR을 낮게 만들어 도청자가 패킷을 제대로 디코딩하지 못하도록 한다. 따라서 도청자는 저장한 신호를 재생공격에 사용할 수 없게 된다. 이 때, 차량의 수신기에 간섭 안테나로부터의 간섭신호가 도달하지만 간섭 신호들의 합이 0에 가깝도록 간섭기에서 발생되는 신호의 위상과 진폭을 적절히 조정한다.

그림 3은 간섭 신호가 전송되는 시점을 결정하는 방법을 설명한다. 키폽의 버튼이 눌러지면 먼저 Wake up 신호가 전송된 후 암호화 된 패킷이 전송된다. Wake up 신호는 기존의 프리앰블 신호로 대체할 수 있다. Wake up 신호를 수신한 수신기는 정해진 대기 시간 후에 암호 키를 수신하고 간섭 안테나에서는 간섭신호가 전송된다. 키폽에서 패킷이 전송되는 동안만 간섭 신호가 전송되므로 전력 소모를 줄이며 다른 차량의 수신기에게 간섭을 줄 확률을 최소화 할 수 있다.

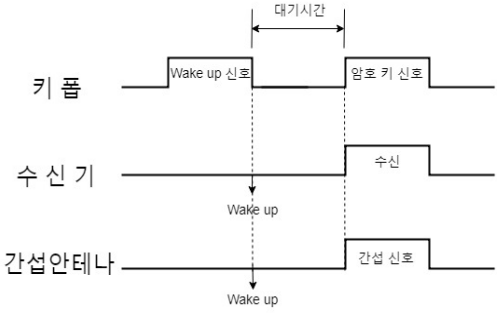

그림 3.

Ⅳ. 실험 결과

반사체가 없는 환경에서 복수의 간섭 안테나를 설치하였을 때, 차량 주변에서 측정한 간섭 신호의 전력을 관찰한다. i번째 간섭 안테나에서 전송되는 신호를 다음과 같이 정의한다.

$$I(t) = \alpha_i \sin(2\pi f_c t + \theta_i), \quad 0 \le t \le T. \qquad (1)$$

여기서 T는 신호의 주기이다. 경로 감쇄는 다음 공식을 사용하였다.

$$PL = \frac{\lambda}{4\pi d^2}. \qquad (2)$$

여기서 d는 송신 안테나와 수신안테나 사이의 거리이다.

그림 4는 한 변이 20미터인 공간의 중앙에 두 개의 간섭안테나가 2 미터 간격으로 배치되어 있는 환경에서 0.1미터 간격으로 간섭 전력 [dBW]을 측정한 결과다. 중심 주파수는 $f_c = 434$MHz이고 $\alpha_1 = \alpha_2 = 0,\ \theta_1 = 0, \theta_2 = \pi$를 사용하였다.

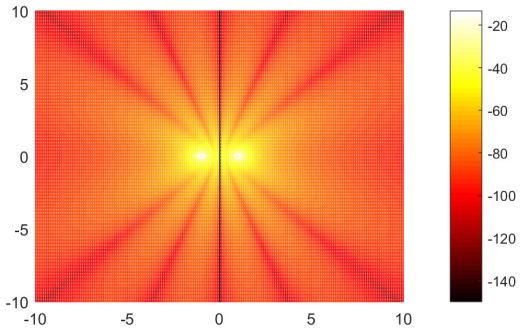

그림 4. 두 간섭 안테나가 배치되었을 때의 위치별 간섭 에너지 [dB].

두 간섭 안테나를 연결한 선을 이등분하는 수직선에 위치한 곳에서는 간섭 에너지가 0이다. 따라서 두 간섭 안테나의 가운데에 수신기를 위치할 경우 간섭이 0 인 것을 알 수 있다. 수직선 이외의 대부분의 지역에서는 간섭 에너지가 -100dBW 이상인 것을 알 수 있다. 따라서, 도청자가 차량 인근에 존재할 경우 간섭의 영향으로 수신 신호의 질이 저하될 것이다.

Ⅴ. 결 론

본 논문에서는 RKE 시스템의 보안성을 강화하기 위해 RKE 시스템에 물리 계층 보안 기법을 도입하여, 도청자가 수신하는 신호의 품질을 저하시켜 재생공격을 무력화 하는 기법을 제안한다. 이는 수집한 신호들의 품질을 저하시켜 롤링 코드를 사용하는 RKE 시스템의 암호를 알아내고자 하는 공격을 더욱 어렵게 만들 수 있다. 시뮬레이션을 통해 복수의 간섭 안테나에서 발생하는 신호가 도청자가 있을 차량 주변의 위치에서 간섭을 주는 반면 간섭 안테나들의 중심에 위치한 수신기에는 간섭을 주지 않음을 확인하였다. 추후 간섭 안테나의 수가 성능에 주는 영향과 실제에 가까운 통신 채널을 고려한 연구가 필요하다.

References

[1] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlid`es. “Lock it and still lose it —on the (in)security of automotive remote keyless entry systems.” In 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, Aug. 2016. USENIX Association

[2] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the

Network and Distributed System Security Symposium", NDSS 2011 (2011), The Internet Society.

[3] R. Benadjila1, M. Renard, J. Lopes-Esteves, and C. Kasmi, "One car, two frames: attacks on Hitag-2 remote keyless entry systems revisited," 11th USENIX Workshop on Offensive Technologies, Aug. 2017.

[4] Y. Shiu et al., "Physical layer security in wireless networks: A tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.