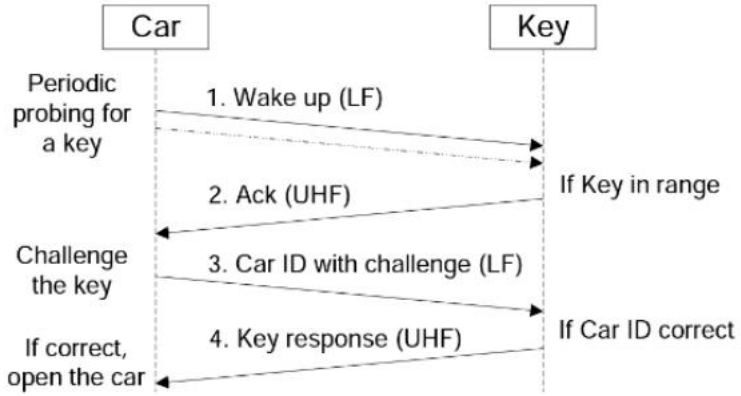
Remote Keyless Entry

20210638 최무송

Digital Key



- 자동차 도난 문제: Immobilizer를 의무화

- Remote Keyless Entry: 원격 차량 잠금을 할 수 있는 시스템
  - LF (vehicle transmission): 유효범위 확인
  - RF (smart key transmission): 차량 제어 메시지
  - Passive Keyless Entry: 거리를 감지하여 자동 잠금 해제

- Car Connectivity Consortium에서 NFC, BLE, HRP UWB 표준화

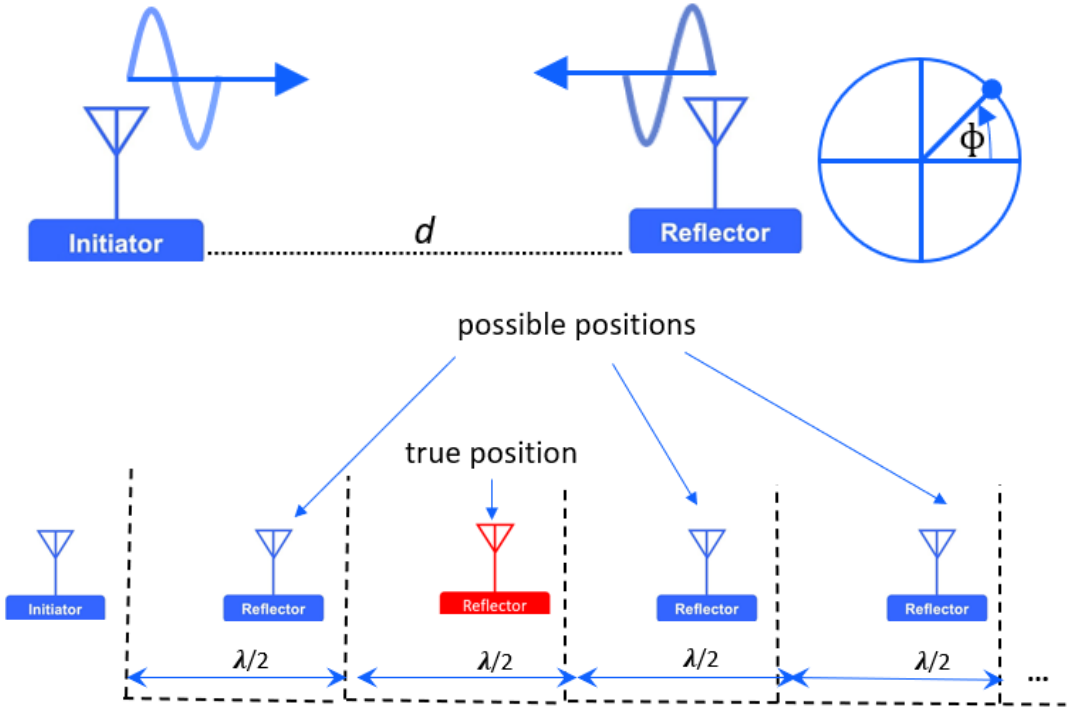
NFC/BLE 기반 인증

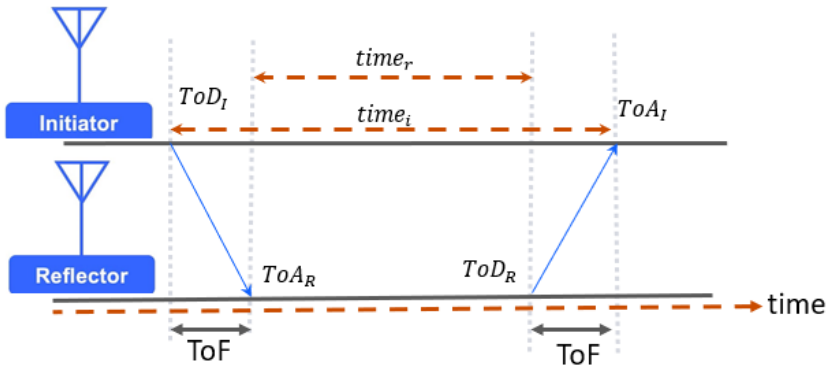
- Near-Field Communication
  - 13.56MHz, 10cm 이내에서 전자기 유도 방식 Tag 감지

- Bluetooth Low Energy (Bluetooth 4.0)
  - Bluetooth Beacon(단방향)
  - 2.4GHz, 10m 거리 대략적 인식
  - 저전력, 저용량 기반 Bluetooth 통신

Channel Sounding

- RRSI(Received signal strength indication) 기반
- Phase 기반 + RTT(Round-Trip Time) 기반

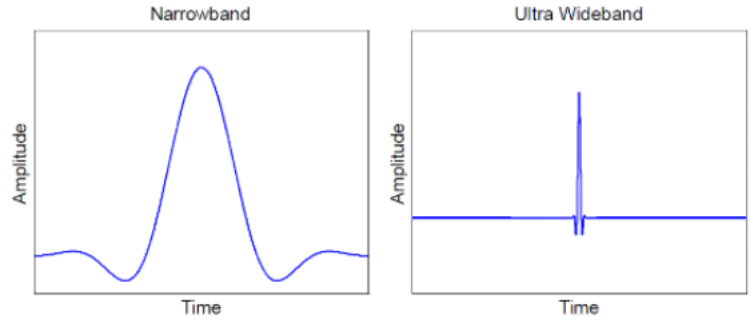




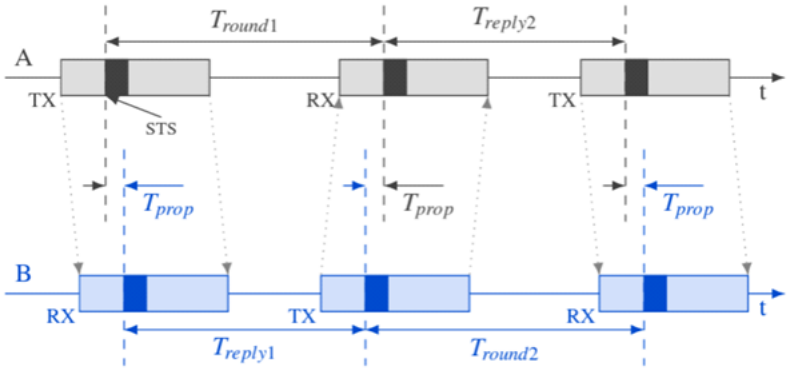
UWB 기반 인증

- Ultrawide Band
  - 3.1~10.6GHz (초광대역) 이용
  - Time-of-Flight 활용 정밀한 거리/위치 측정
  - Two-Way Ranging
  - STS(Scrambled Timestamp Sequence)

- BLE보다 더 정확한 거리 측정 가능



〔그림 4〕 협대역 (narrowband) 신호와 초광대역 (ultra wideband) 물리 레벨 신호〔7〕



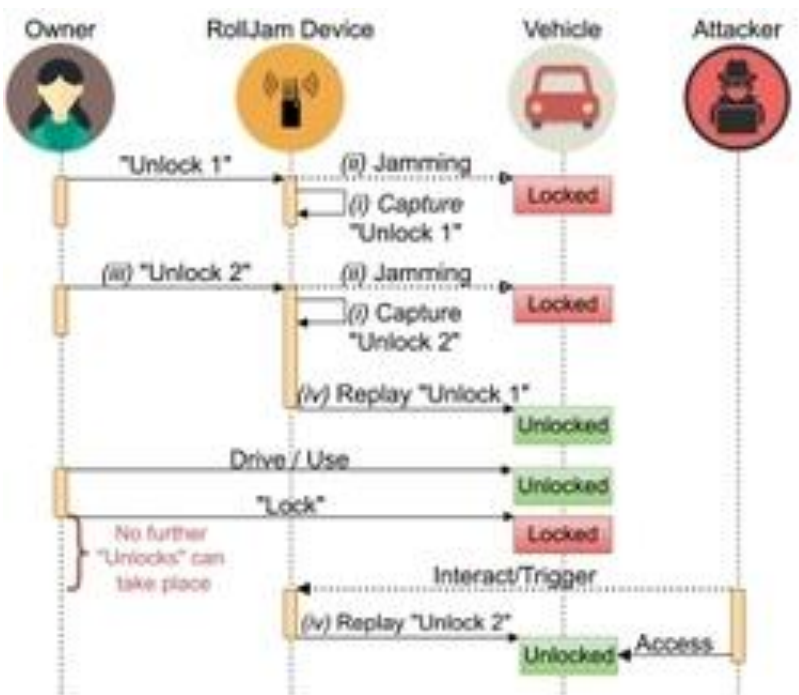
〔그림 6〕 DS-TWR 통신 흐름도〔3〕

Replay → Rolljam/Rollback attack

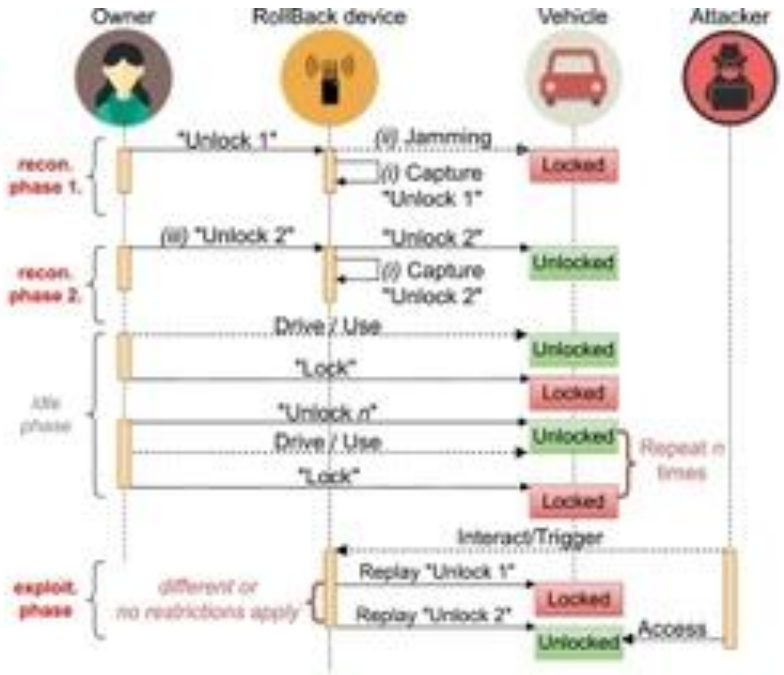
- Rolling code/Hopping code
  - 도청을 당하더라도 Replay Attack을 하지 못하도록 동기화 카운터 도입
  - Ex - Keeloq

- Rolljam attack
  - Jamming + Capture (첫 번째 FOB 신호 무효화 및 캡쳐)
  - Jamming + Replay (두 번째 FOB 신호 무효화 및 첫 번째 신호 대신 사용 → 공격자는 자동차가 앞으로 사용할 것이라고 믿는 두 번째 신호를 획득)

- Rollback attack
  - 재동기화과정에서의 취약점 이용
  - 연속된 두 신호를 이용하여 자동차의 카운터를 롤백



(a) RollJam is particularly sensitive to timing; it has to be aware of the next valid unused code.

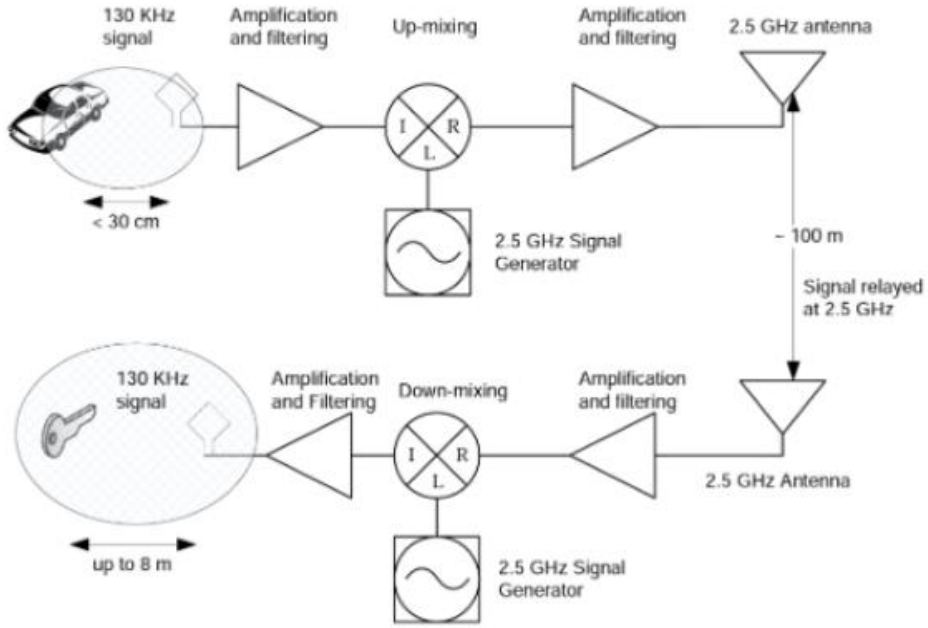


(b) A RollBack variant using only two captured signals at any time.

Relay Attack

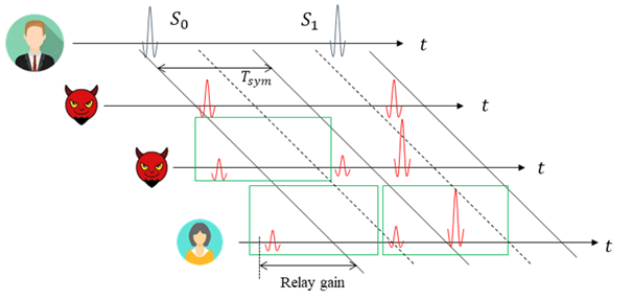
- 신호를 증폭하여 차량과 사용자 간을 중계하여 사용자의 거리를 속이는 공격

- High-repetition pulse UWB 도입

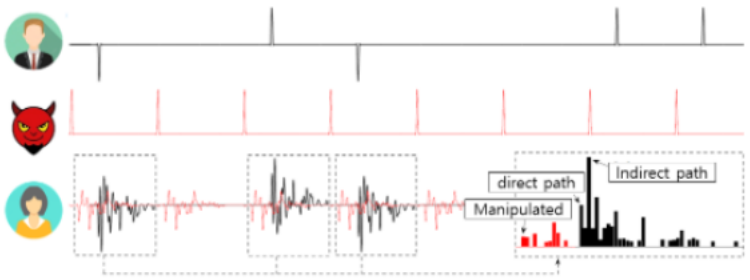


Distance reduction attack

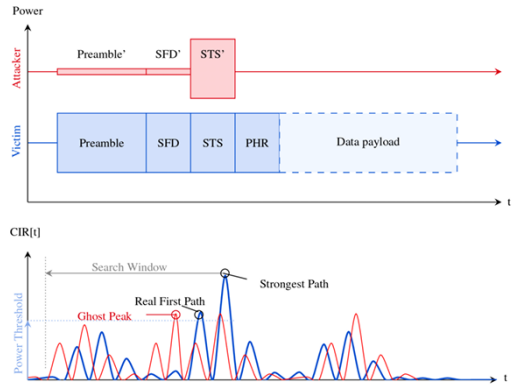
- Early detect/late commit (ED/LC) Attack
  - Early detect from user and sends commit signal to car
- Cicada attack
  - Distance error by repeated signals
- Ghost peak attack
  - Sending signal to occur signal overshadowing



〔그림 14〕 PPM 변조기법에 대한 ED/LC 공격



〔그림 13〕 Cicada attack



〔그림 15〕 Signal overshadowing 공격 〔3〕

Reference

- https://doi.org/10.7467/KSAE.2024.32.7.609
- 논문보기 - DBpia