

# RF Fingerprint 기반 신호 생성 및 위성-지상 통신 적용

최길한, 유광운, 최우열<sup>†</sup>, 김용강\*  
공주대학교, 중앙대학교

choikilhan12@smail.kongju.ac.kr, yugwangun@smail.kongju.ac.kr, wchoi@cau.ac.kr<sup>†</sup>,  
ygkim@kongju.ac.kr\*

## RF Fingerprint-Enabled Signal Generation for Satellite to Ground Communications

Gilhan Choi, Gwangun Yu, Wooyeol Choi<sup>†</sup>, Yonggang Kim\*  
Kongju National University\*, Chung-Ang University<sup>†</sup>.

### 요약

본 논문에서는 위성-지상 통신 환경에서 송신기 고유의 하드웨어 왜곡을 이용한 RF Fingerprint 기반 신호 생성 기법을 제안한다. Python 을 이용하여 16-QAM 기저대역 신호에 PA 3 차 비선형성, LO 주파수 오프셋, I/Q 위상 불균형 및 도플러 효과를 모사한 왜곡을 삽입하고, RRC 펄스 성형을 통해 실제 RF 파형을 생성하였다. 생성된 신호 간 시간 및 주파수 영역 비교를 통해 동일 송신기 fingerprint 의 일관성을 확인하였으며, 향후 이 데이터를 활용한 딥러닝 분류기를 통해 정상/위조 신호를 효과적으로 식별하는 연구를 계획하고 있다.

### 1. 서론

최근 위성 통신 시스템은 대역폭 확대와 서비스 다변화에 따라 스푸핑·재밍·재전송 공격 등의 위협에 노출 되고있다. 특히 지상국과 위성 간 링크에서는 대규모 트래픽이 단일 채널을 통해 오가므로, 악의적 공격자가 정상 장치의 신호를 위조하거나 재전송함으로써 서비스 중단 및 데이터 유출 위험이 커진다. RF Fingerprint 는 I/Q 변조시의 불균형, Local Oscillator(LO)의 주파수 불안정성, Power Amplifier(PA)의 3 차 비선형 계수와 같은 송신 장치의 하드웨어 불완전성이 신호 파형에 남기는 고유 왜곡을 이용하여, 기존 암호 기반 인증과 달리 추가 전송 오버헤드 없이도 송신자를 식별할 수 있는 방법이다.[1] 본 연구에서는 위성-지상 통신 환경을 대상으로 RF Fingerprint 가 삽입된 신호 생성 기법을 제안한다. Python 을 이용한 16-QAM(Quadrature Amplitude Modulation) 신호에 임의의 LO 주파수 오프셋, PA 계수, I/Q 변조 노이즈를 삽입해 신호를 생성한다. 이렇게 생성된 신호는 추후에 딥러닝 분류기를 개발하여 보다 효율적인 올바른 접근 혹은 올바르지 않은 접근인 신호를 구분할 계획이다. 이를 통해 패킷 검증 전 1 차적인 보안기법을 적용할 수 있게 된다. 이와 같은 물리계층 Fingerprint 기법은 위성통신의 보안을 보다 적은 오버헤드로 효율적이고 저비용의 방식으로 서비스가 가능할 것으로 기대된다.[2]

### II. 본론

먼저 신호를 생성하려면 비트를 각각의 신호에 매핑해야 한다. 이를 위해 우리는 I/Q 변조 방식을 활용한 QAM 기법을 적용했다. 따라서 QAM 은 직교하는

두 Carrier Frequency 즉 코사인 성분(I 성분)과 사인

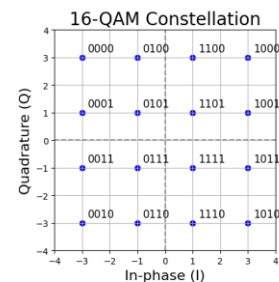


그림 1. 16-QAM 의 Constellation 을 나타낸다.

성분(Q 성분) 의 진폭을 각각 독립적으로 변화시켜 하나의 심볼로 전송함으로써, 동일 대역폭 내에서 높은 스펙트럼 효율을 달성할 수 있다. 본 실험에서는 16-QAM 을 사용하여 심볼당 4 비트( $\log_2 16$ )를 전송하며, 이를 통해 총 16 개의 고유한 진폭 조합을 활용한다. 구체적으로, 전송할 비트열을 4 비트씩 묶은 뒤 앞의 두비트는 I 로 나머지 두비트는 Q 로 할당하고 식(1)의 Gray 인코딩을 거쳐 인접 심볼 간 해밍 거리를 1 로 유지함으로써, 심볼 오류 발생시 비트 오류를 최소화한다.

$$G = B \oplus (B \gg 1) \quad \text{식 (1)}$$

G 는 그레이코드를 나타내고 B 는 비트열을 나타낸다.  $\gg$ 는 Right Shift 연산이다. 마지막으로 Gray 코드 결과를 16-QAM Constellation 의 I/Q 레벨 집합  $\square = \{-3, -1, +1, +3\}$ 과 일대일 매핑하여, I 성분 과 Q 성분을 얻는다. 이때 각 진폭 값은 반송파의 진폭 크기를 의미하며, 심볼 평면 상에서 4 개의 격자점으로 구성된  $4 \times 4$  그리드를 형성한다. 그림 1을 보면 어떠한 방식으로 값을 지정하는지를 볼 수 있는데 앞의 두비트는 I 의

값을 나타내고 뒤의 두 비트는 Q 의 값을 나타낸다. 매핑된 I/Q 심볼은 업샘플링(샘플 간 0 삽입) 과정을 거친 후 Root-Raised-Cosine(RRC) 펄스 성형 필터를 적용한다. RRC 필터는 롤오프 계수  $\alpha$ 에 따라 스펙트럼의 꼬리(tail)와 대역폭을 제어하며, 인접 심볼 간 간섭(ISI)을 최소화하도록 설계된다. 실제 RF 송신 신호는 이렇게 생성된 기저대역 신호를  $2\pi \cdot (f_c + \varepsilon_f + f_d) \cdot t + \phi$  오프셋이 적용된 캐리어 주파수 위에 실어 전송하며, 송신기 고유의 PA 비선형성( $\alpha \cdot s^3$ ), LO 오프셋( $\sigma_f$ ), 위상 불균형( $\sigma_\phi$ ), Doppler 효과( $f_d = v_{sat}/c \cdot f_c$ ) 등이 추가되어 각 단말기의 RF Fingerprint 를 모사한다. 따라서 최종 송신 신호 I/Q Modulation 을 적용한  $S(t)$ 은 다음과 같다:

$$S(t) = \left[ s_b, I(t) + \alpha \cdot (s_b, I(t))^3 \right] \cdot \cos(2\pi \cdot (f_c + \varepsilon_f + f_d) \cdot t + \phi_I) - \left[ s_b, Q(t) + \alpha \cdot (s_b, Q(t))^3 \right] \cdot \sin(2\pi \cdot (f_c + \varepsilon_f + f_d) \cdot t + \phi_Q)$$

$s_b, I(t)$ 와  $s_b, Q(t)$ 는 각각 업샘플링 및 RRC 필터링을 거친 기저대역 I/Q 성분 신호이다.  $\alpha$ 는 PA 의 3 차 비선형 계수로,  $\alpha \cdot (s_b, \cdot(t))^3$  항을 통해 실제 PA 에서 발생하는 고조파 왜곡을 모사한다.  $f_c$  는 Carrier Frequency 주파수(Hz)이고  $\varepsilon_f$  는 LO 의 주파수 오프셋으로  $\varepsilon_f \sim N(0, \sigma_f^2)$ ,  $\sigma_f = 5$  Hz 로 모델링 된다.  $f_d$  는 Doppler shift 로서  $f_d = (v_{sat}/c) \cdot f_c$  형태로 계산되며,  $v_{sat}$  은 위성 속도,  $c$  는 광속이다.  $\phi_I$  와  $\phi_Q$  는 I/Q 경로의 위상 불균형을 나타내는 위상 오프셋(라디안)으로  $\phi_I, \phi_Q \sim N(0, \sigma_\phi^2)$ ,  $\sigma_\phi = 2^\circ$  로 설정된다.  $t$  는 시간 변수(초)이고,  $\cos(\dots)$ 와  $\sin(\dots)$ 은 각각 위상 오프셋이 반영된 Carrier Frequency 의 Sinusoidal Wave 성분을 뜻한다. 이를 통해 송신기 자체의 Fingerprint 를 나타내고 구분이 가능하다.

### III. 결론

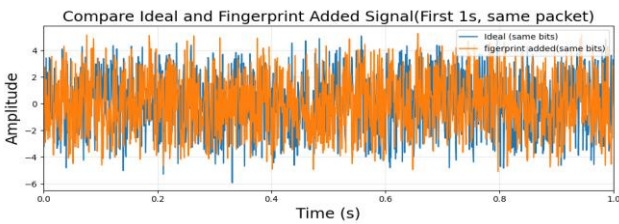


그림 2 동일 패킷을 이상적인 상황 과 Fingerprint 가 삽입된 신호와 비교

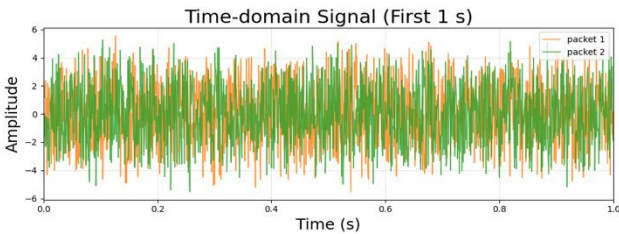


그림 3 서로 다른 패킷을 같은 Fingerprint 를 적용한 신호 비교

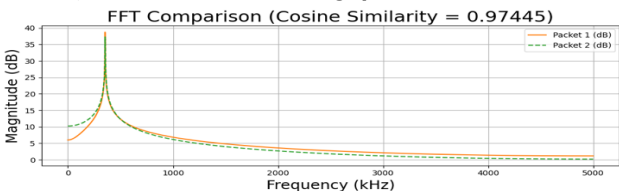


그림 4 서로 다른 패킷의 Fingerprint 코사인 유사도 비교

그림 2 은 동일 패킷에 대해 PA 비선형성, LO 오프셋, 위상 불균형, Doppler 효과 등을 포함한 RF Fingerprint 를 추가하기 전(파랑)과 추가한 후(주황)의 시간 영역 파형을 중첩하여 보여준다. 두 파형이 거의 비슷한 것을 확인할 수 있는데, 이는 Fingerprint 를 적용해도 전달하는 데이터(비트) 자체에는 변화가 없고, 미세한 왜곡만 추가되었음을 의미한다. 그림 3 는 서로 다른 두 개의 랜덤 비트 시퀀스(패킷 1: 주황, 패킷 2: 초록)에 동일한 송신기 Fingerprint 파라미터를 적용한 후 시간 영역에서 비교한 것이다. 서로 다른 비트 패턴으로 생성된 두 신호가 전반적인 파형 분포와 진폭 범위에서 유사함을 보여, 하나의 송신기가 생성하는 각 패킷이 동일한 'Fingerprint 특성'을 공유함을 확인할 수 있다. 그림 4 은 그림 3 의 두 신호를 주파수 영역으로 변환한 FFT 스펙트럼을 중첩하여 나타낸 것이다. 두 스펙트럼이 거의 완전히 일치하며, 코사인 유사도 값(similarity = 0.97445)이 1 에 매우 근접함을 통해, 서로 다른 비트 스트림에도 불구하고 동일 송신기 fingerprint 가 일관되게 관측된 것임이 확인된다.

### IV. 향후 연구 방향

이들 신호를 바탕으로 후속 연구에서는 우선 주파수 영역 스펙트럼 이미지를 CNN 에 입력하여 송신기별 왜곡 패턴을 정밀 분류하는 모델을 개발할 것이다.[3] 다음으로 기저대역 신호의 Eye Diagram 을 활용해 PA 비선형성 및 위상 불균형 등 미세 왜곡을 추출·학습하는 CNN 기반 기법을 설계하고[4], 소량의 라벨 데이터로도 높은 분류 성능을 달성할 수 있는지를 검증한다. 아울러 실험실 환경을 넘어 실제 위성-지상 데이터를 활용하여 모델의 현장 적용 가능성을 평가하고, 모바일·엣지 단말에서도 실시간 추론이 가능하도록 모델 경량화 기술을 도입할 계획이다. 마지막으로, 채널 동적 페이딩·대기 감쇠·빔포밍 오차 등을 반영한 상세 위성-지상 통신 모델을 확장하고, 적응형 변조·부호화(AMC) 및 네트워크 계층과의 크로스 레이어 설계를 통해 RF Fingerprint 기술이 실제 위성 네트워크 경로 선택과 자원 할당에 어떻게 기여할 수 있을지 고도화할 예정이다.

### ACKNOWLEDGMENT

본 연구는 2025 년 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학사업 지원을 받아 수행되었음(2024-0-00073)

### 참 고 문 헌

- [1] Y. Shao, J. Liu, Y. Zeng and Y. Gong, "A Radio Frequency Fingerprinting Scheme Using Learnable Signal Representation," IEEE Communications Letters, vol. 28, no. 1, pp. 73-77, Jan. 2024.
- [2] URETEN, Oktay; SERINKEN, Nur. "Wireless security through RF fingerprinting," Canadian Journal of Electrical and Computer Engineering, vol. 32, no.1, pp 27-33, 2007.
- [3] JIAN, Tong, et al. "Deep learning for RF fingerprinting: A massive experimental study," IEEE Internet of Things Magazine, vol. 3, no.1, pp 50-57, 2020.
- [4] PENG, Linning, et al. "Deep learning based RF fingerprint identification using differential constellation trace figure," IEEE Transactions on Vehicular Technology, vol. 69, no.1, pp 1091-1095, 2019.