2024.05.17

Open RAN for detection of a jamming attack in a 5G network

monthly seminar

경희대학교
최호성

MCL
KYUNGHEE

Outline

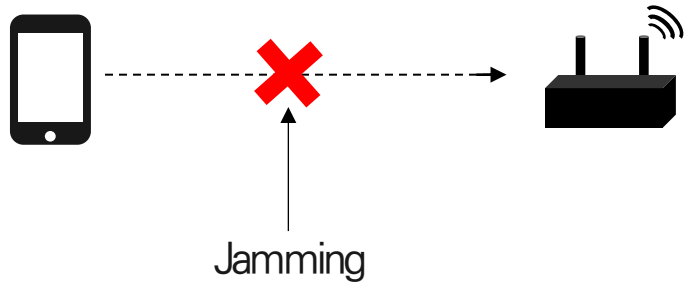
1. Background
   - 1.1 Jamming in ORAN
   - 1.2 CQI, RSRP
   - 1.3 Kolmogorov – Smirnov Test
2. Previous research
3. Simulation architecture
4. Simulation environment & Result
5. Contribution & Future work

MCL
KYUNGHEE

1.1 Jamming in ORAN

Jamming

- 주파수 대역에 신호를 주입하여 피해 수신기의 성능을 저하시키는 행위
- 저렴한 HW + 얕은 지식
- 예) URLLC를 요구하는 서비스



Open RAN

- RAN 구성요소(DU, CU, RU)의 탈 중앙화
- RIC(RAN Intelligent Controller)에 배치된 closed-loop algorithm을 통해 RAN을 조율
- E2Node와 RIC을 연결하는 E2 interface를 통해 Physical layer의 metric에 access 가능
- RIC 내부의 xApp, rApp으로 metric을 분석

1.2 CQI, RSRP

CQI (Channel Quality Indicator)

- Channel 품질을 〈1, 15〉 범위로 나타내는 값
- Channel-state information(CSI)는 CQI, RI, PMI로 구성, DL channel sounding에서 CSI-RS를 통해 측정됨
- CSI 중 jamming과 가장 관련 있음
- gNB가 보낸 CSI-RS를 기반으로 UE가 CQI를 측정하여 gNB로 report

RSRP(Reference Signal Receiver Power)

- 특정 대역폭 내에서 Reference signa의 수신 강도를 나타내는 값 (-141dBm, -44dBm)
- Physical layer에서 CRS를 통해 측정됨
- RRC layer에서 cell selection과 handover를 결정하기 위해 필요함
- RRC measurement configuration을 통해 측정이 요구되며, UE는 측정한 값을 RRC measurement report를 통해 gNB에 report

1.3 Kolmogorov – Smirnov Test

MCL KYUNGHEE

비모수적 검증 방법 (Non-parametric test)

- 데이터 분포에 대한 사전 지식이 없거나 특정 분포일 것이라는 가정이 맞지 않을 때 사용하는 검증
- 데이터가 특정 분포에 따르지 않거나 특정 가정이 필요하지 않을 때 사용

- 장점
  - 다양한 데이터 유형에 적용 가능
  - 이상치(outliner)나 비정규 분포에 민감하지 않음
  - 작은 샘플 크기에서도 유용

- 단점
  - 모수적 검증과 동일한 검증력을 얻기 위해서 더 큰 샘플의 크기가 필요할 수 있음.
  - 데이터의 순위만 사용하기 때문에 데이터의 절대적 차이를 반영하지 못함

1.3 Kolmogorov – Smirnov Test

Kormogrov-Smirnov statistic

- 두 개의 분포를 비교하는 비모수적 검정 방법
- 특정 환경 조건에서 얻은 데이터가 기존의 데이터와 동일한 분포를 따르는지 확인하기 위해 사용
- 얻은 sample이 연속적이면 CDF를 사용, 비연속적이면 EDF를 사용

EDF (Empirical Distribution Function)

- 주어진 데이터 샘플 기반으로 한 확률 분포의 경험적인 표현

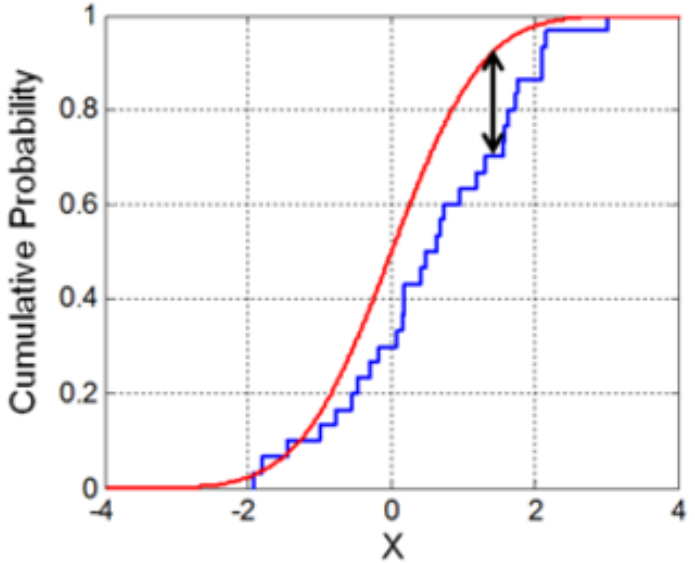
$$\widehat{F_n}(x) = \frac{1}{n}\sum_{i=1}^{n} I\,(X_i \le x\,)$$

I : 지시 함수 (조건이 참이면 1, 거짓이면 0을 반환)

n : sample 크기

X_i : sample data point

Cf. CDF ($F_X(x) = P\,(\,X \le x\,)$)



1.3 Kolmogorov – Smirnov Test

MCL KYUNGHEE

K-S test의 검증 방법

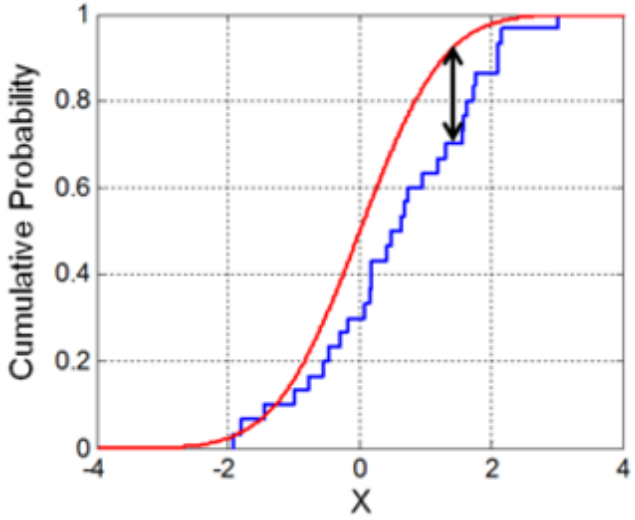
① 이론 값 또는 학습가능한 데이터를 이용하여 reference가 되는 분포 를 구한다.
② 실제 sample 값을 추출하여 EDF를 구한다.
③ 앞서 구한 두 분포를 이용하여 "k-s static"을 구한다. (분포 간 차의 최대값)

$$D_n = sup|F_n(x) - F(x)|$$

④ "k-s static"이 표에서 제시되는 기준 값과 비교하여 두 분포가 유의미한 차이를 갖는지 판단한다.

$$D_n > c(\alpha), c(\alpha) = \sqrt{-\frac{1}{2}\ln\alpha}$$

⑤ "k-s static"이 기준 상수보다 높으면 두 분포 사이에 유의미한 차이가 있음을 의미함



α	0.20	0.15	0.10	0.05	0.025	0.01	0.005	0.001
$c(\alpha)$	1.073	1.138	1.224	1.358	1.48	1.628	1.731	1.949

2. Previous study

MCL KYUNGHEE

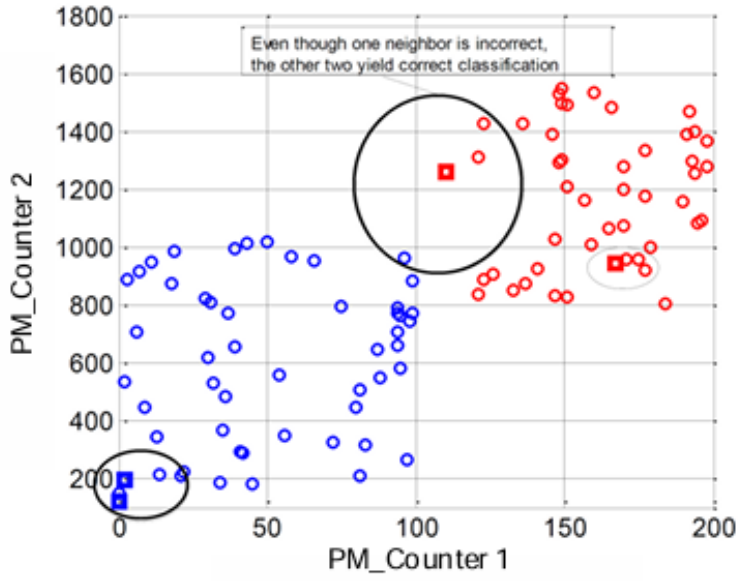
K-NN Clustering algorithm

- 초기 입력 값
  - 특징벡터 : PM Counters/Key Performance Indicator [metric1, metric2]
  - Classification category : C1, C2
  - 올바르게 분류된 벡터 형태의 훈련 sample

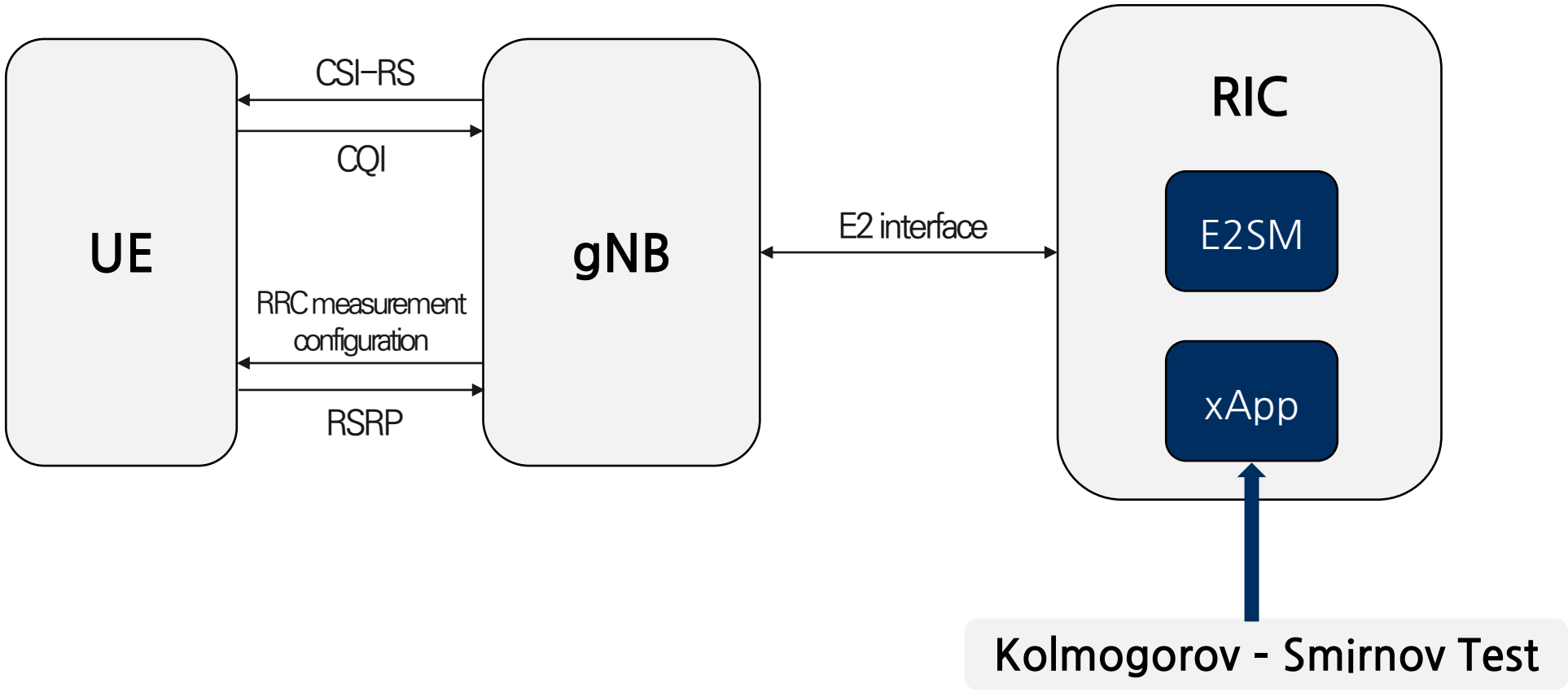
- 반복 algorithm
  - 특징 벡터와 훈련 sample의 거리 계산
  - 훈련 sample 중 가장 짧은 거리를 갖는 sample k개를 선택
  - K개의 sample 중 다수의 sample이 포함된 Class로 분류

- Simulation
  - 특징벡터 : ISRRE (Interference to Signal Ratio per Resource Element), ISRF (Interference to Signal Ratio per Frame)
  - Classification category : 간섭 o / 간섭 x (2개의 class)
  - K=3

➔ 간섭인 경우와 간섭이지 않은 경우 2가지 reference data가 필요!



3. Simulation architecture



4. Simulation & Result

MCL KYUNGHEE

Simulation environment

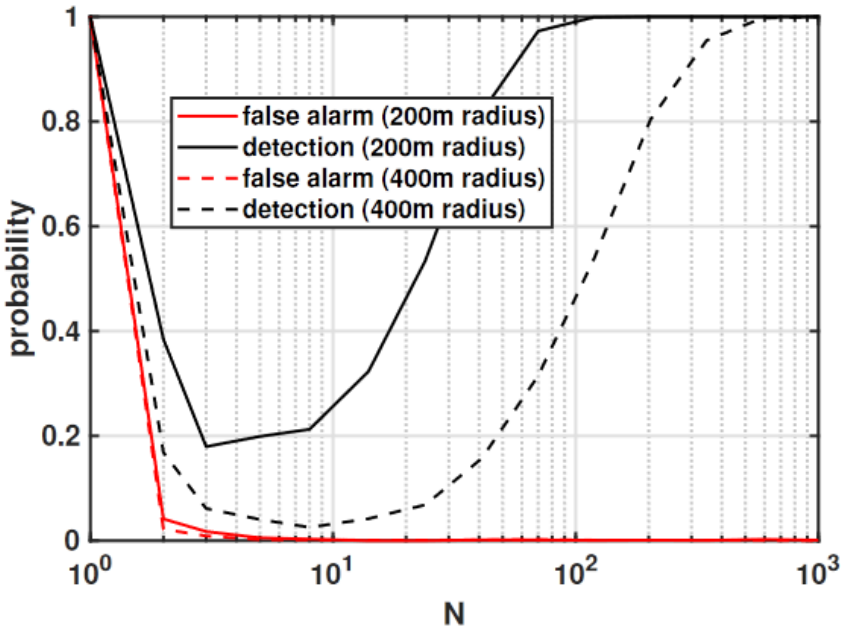
- 주파수 : 3.5GHz
- 기지국 : 24dBm 5G 기지국 (원형 영역을 커버)
- Scenario : non-LOS, industrial scenario에 따라 균일하게 분포된 UE
- Channel model : TDLA30 (시간지연확산 model), link 당 12개 경로의 소규모 fading channel
- Jammer : 20dBm 송신기 (cell 임의의 위치에 배치, CSI-RS subcarrier만 방해)

Result

- False alarm : xApp이 잘못 detection할 확률 (xApp의 성능)
- Detection : 탐지확률 (xApp의 성능)

- Sample 수 증가
  - False alarm 감소 : xApp이 제대로 jamming을 detection
  - Detection 증가 : sample 증가로 인해 더 나은 분포 비교 가능으로 성능 증가

- 반경 200m vs 반경 400m
  - 더 큰 반경일 때 jammer와 UE 사이의 거리가 멀기 때문에 탐지확률이 더 낮음



5. Contribution & Future work

Contribution

- 낮은 false alarm
- 상대적으로 적은 수의 sample 활용
- 네트워크 구조나 UE 분포에 대한 가정을 사용하지 않은 가벼운 algorithm

Future work

➢ **다른 algorithm 적용**

- Machine learning
- 다양한 AI/ML
- Kuiper's Test (더욱 균등한 민감도)

➢ **다른 dataset 적용**

- RSRP, RSSI, RSRQ
- $RSRQ = N \times \frac{RSRP}{RSSI}\ [Watt]$

감사합니다