2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) | 979-8-3503-1114-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/VTC2023-Spring57618.2023.10201067

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

Pawel Kryszkiewicz
Rimedo Labs
Institute of Radiocommunications
Poznan University of Technology
Poznan, Poland

Marcin Hoffmann
Rimedo Labs
Institute of Radiocommunications
Poznan University of Technology
Poznan, Poland

***Abstract*—One of the essential security threats for 5G networks is jamming. It is relatively easy to be performed utilizing cheap and publically available devices. Open Radio Access Network (O-RAN) architecture is very suitable for detecting such events thanks to the openness of interfaces and the ability to analyze wireless traffic metrics and exchange control messages in a RAN Intelligent Controller (RIC) using some dedicated xApp or rApp. This paper presents a statistical method for downlink jamming detection utilizing the link quality reports provided by User Equipments (UEs). A vision of its implementation in O-RAN is presented altogether with performance quality metrics obtained via simulations.**

I. Introduction

Jamming of a wireless network is a relatively simple attack when an adversary injects some signal into the frequency band used by the victim network in order to deteriorate the reception performance of the victim receivers. While the 5G physical layer (PHY) is relatively well-protected from jamming, it can still be harmful, e.g., to the Ultra Reliable Low Latency Communications (URLLC) devices [1] by increasing their communications latency. There are various ways jamming can be performed with a comparison for a 4G system provided in [2]. Most importantly, contemporary jamming can be realized using very cheap hardware, even without any specialized knowledge, increasing this threat probability.

There is a need for mechanisms detecting jamming attacks in a 5G network. While this can be done using some external sensors, the simplest solution is to analyze signal quality indicators measured by UEs or gNodeBs. The O-RAN architecture is suitable for this purpose as it provides direct access to PHY measurements via interfaces connected to RICs and the possibility of running a specialized analysis within a dedicated xApp or rApp [3].

This paper presents a method of 5G downlink (DL) jamming attack detection based on Reference Signal Received Power (RSRP) and Channel Quality Indicator (CQI) values reported by UEs, though it can be extended to other PHY reports depending on their availability. There are various options for jamming detection from such reports, e.g., in [4] the k-NN method has been used for an LTE cell. However, this method requires two reference datasets (with and without jamming) that are difficult to be obtained in a real network scenario. Here, a two-dimensional version of the Kolmogorov–Smirnov (KS) test is used [5] that detects jamming as an anomaly from the normal CQI-RSRP values distribution. It is simpler than [4] as it requires only a single reference dataset.

The presented work has been funded by the Polish Ministry of Education and Science within the status activity task no. 0312/SBAD/8164, and by the National Centre for Research and Development in Poland within project no. CYBERSECIDENT/487845/IV/NCBR/2021.

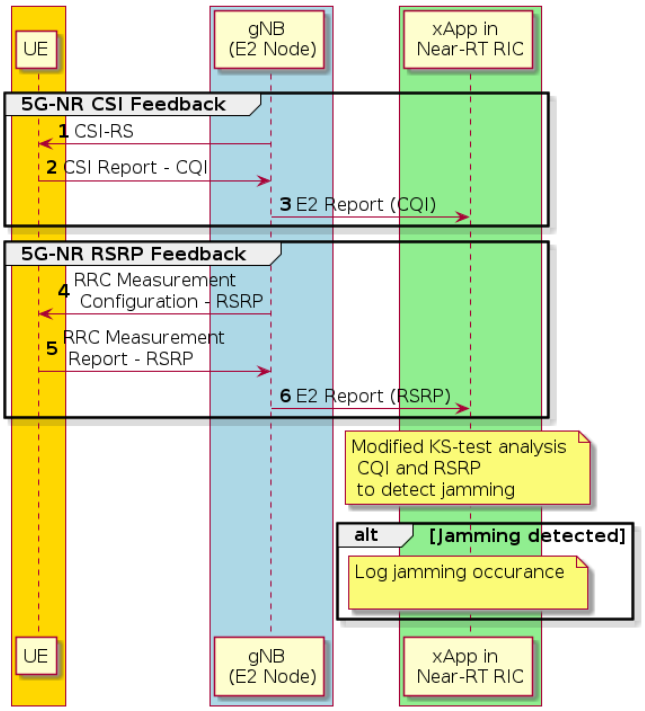

Fig. 1. Control messages exchanged between UE, gNB, and jamming detection xApp placed in the Near-RT RIC.

II. Jamming detection using O-RAN

The proposed jamming detection algorithm operates as an O-RAN xApp with the control messages exchange

via proper interfaces as shown in Fig. 1. The quality of UEs' radio links is constantly monitored by collecting CQI and RSRP reports. First, the CQI values, being integers in the range $\langle 1; 15\rangle$, are obtained as a part of Channel State Information (CSI) Reports [6]. The CSI Reports are based on the UE measurements of the CSI Reference Signals (CSI-RS). In addition, each UE is configured (via Radio Resource Control Measurement Configuration [7]) to send the so-called Measurement Reports to the gNB containing the RSRP value in the range of -141 to -44 dBm respectively that also may be computed based on CSI-RS. The O-RAN E2 interface provides a mechanism to copy control plane messages send between the UE and the gNB (acting as a so-called E2 Node), to the Near-Real Time (RT) RIC where jamming detection xApp is placed i.e., the E2 Report Service [8]. The jamming detection xApp initially stores the reported CQI-RSRP values, each report as a two-dimensional vector $\mathbf{x}$. Initially or when given samples are not categorized as jammed, these are used to create a reference distribution $F(\mathbf{x})$. After the initialization phase, N new CQI-RSRP reports coming from various users are utilized together to estimate the current distribution denoted as $F_N(\mathbf{x})$. The KS test decides if the null hypothesis, i.e., *The current N samples have the same distribution as the reference set* ($F_N(\mathbf{x}) = F(\mathbf{x})$), can be rejected, suggesting jamming occurred changing network reports distribution. While the standard KS test is suitable for one-dimensional data, here is two-dimensional extension has been used [5]. If the jamming is detected, the xApp puts specific information in its log files to be visible to the Mobile Network Operator (MNO). A network reconfiguration can be ordered, though it is out of the scope of this paper.

III. Simulation Results

The proposed algorithm is tested in a factory-like scenario, i.e., 24 dBm 5G base station operating at 3.5 GHz carrier, covering a circle area. The UEs are uniformly distributed with the path loss and shadowing generated according to non-line of sight industrial scenario of ITU-R P1238.11. Additionally, a 12-path small-scale fading channel TDLA30 [9] is generated independently for each link. After collecting reference CQI-RSRP distribution the false alarm probability is evaluated by estimating the current distribution using N new and independent UEs reports. Moreover, the detection probability is estimated by placing a 20 dBm transmitter jamming only the CSI-RS subcarriers in a random location of the cell. The influence of N and cell radius on the probability of detection and false alarm at 5% significance level is shown in Fig.2. It is visible that the probability of a false alarm drops fast with N for both cell sizes. Except for some anomalies for very low numbers of reports the probability of detection rises fast with N. For a bigger cell, the 20 dBm jamming is less harmful, especially for UEs much distanced from the jammer, justifying lower detection probability.

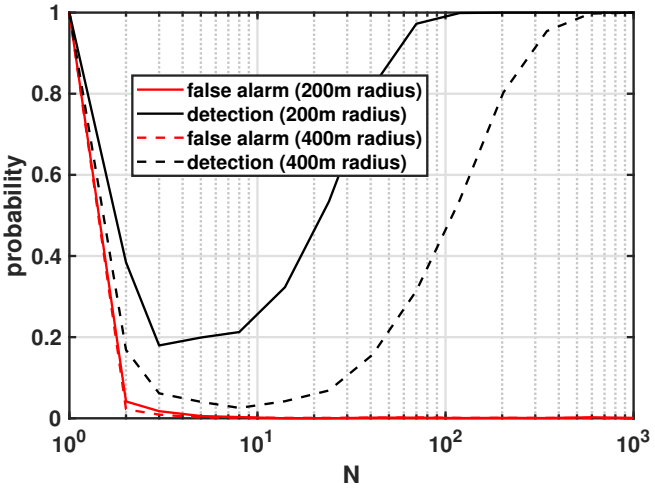

Fig. 2. Probability of false alarm and detection for varying N and cell size.

IV. Conclusion

The proposed jamming detection method can work effectively in an O-RAN architecture. It maintains low false alarm probability while enabling jamming detection with high probability even for relatively low, in comparison to reporting rate, number of channel quality reports utilized N. Thus, even short-term jamming can be detected using Near-RT RIC and appropriate xApp. Most importantly, the proposed method uses no assumption regarding network structure or UEs distribution as it *learns* the reference distribution.

References

[1] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5g new radio: A review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 1010–1015.

[2] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[3] M. Dryjański, Ł. Kułacz, and A. Kliks, "Toward Modular and Flexible Open RAN Implementations in 6G Networks: Traffic Steering Use Case and O-RAN xApps," *Sensors*, vol. 21, no. 24, p. 8173, 2021.

[4] V. Marojevic, R. M. Rao, S. Ha, and J. H. Reed, "Performance analysis of a mission-critical portable lte system in targeted rf interference," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1–6.

[5] J. A. Peacock, "Two-dimensional goodness-of-fit testing in astronomy," *Monthly Notices of the Royal Astronomical Society*, vol. 202, no. 3, pp. 615–627, 1983.

[6] 3GPP, "Physical layer procedures for data ," TS 38.214 v.17.3.0, Sep. 2022.

[7] ——, "NR; Radio Resource Control (RRC); Protocol specification ," TS 38.331 v.17.2.0, Oct. 2022.

[8] O-RAN ALLIANCE WG3, "Near-real-time ran intelligent controller e2 service model (e2sm), ran control, v.1.03," Tech. Rep., 10 2022. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[9] 3GPP, "NR; Base Station (BS) conformance testing; Part 1: Conducted conformance testing ," TS 38.141-1 v.17.7.0, Oct. 2022.