RanCAD: Random Channel Access Deterrence Attack against Spectrum Coexistence between NR-U and Wi-Fi on the 5GHz Unlicensed Band

Md Rashedur Rahman and Moinul Hossain
George Mason University, Fairfax, VA, USA
Email: mrahma47@gmu.edu, mhossa5@gmu.edu

***Abstract*—Spectrum coexistence between 5G and Wi-Fi in the coveted 5GHz spectrum band unleashes new possibilities for more effective spectrum utilization. While the Listen-Before-Talk-based channel access mechanism with the self-deferral-based method enhances the relative fairness of this coexistence framework, it introduces new vulnerabilities yet to be addressed. This research presents a unique attack approach, *Random Channel Access Deterrence* (*RanCAD*), that exploits a novel vulnerability in the channel access mechanism. In the proposed attack, a *malicious* access point deceives a victim 5G base station into deferring its access to the shared channel, resulting in higher channel access delay and lower spectrum utilization. In addition, we propose a Discrete Time Markov Chain (DTMC) to study the proposed attack model, which helps illustrate the attack's impact on the victim's performance. To our knowledge, this is the first work to introduce this vulnerability in the channel access mechanism between coexisting 5G and Wi-Fi networks in the 5GHz band.**

I. Introduction

The growing adoption of cellular technology in numerous applications, like industrial automation systems and autonomous vehicles, highlights the demand for broadening the available spectrum by incorporating the unlicensed spectrum band [1]. As a result, regulatory bodies such as 3GPP have introduced the concepts of LTE-LAA and 5G NR-U to design the coexistence mechanism with Wi-Fi [2] in the 5GHz unlicensed spectrum band. The goal is to formulate a fair coexistence mechanism between Wi-Fi and cellular technologies while offering adequate performance enhancement for cellular technologies. Although a duty cycle-based mechanism called Carrier-Sensing Adaptive Transmission (CSAT) was initially proposed to preserve the scheduled access mechanism employed by cellular technologies, 3GPP later adopted a CSMA/CA-like Listen-Before-Talk (LBT) based access mechansim due to widespread regulatory requirements [3].

In the research community, considerable emphasis was concentrated on improving the fairness of cellular and Wi-Fi technologies [3]–[6] operating in the unlicensed 5GHz spectrum band; however, security concerns received less attention. The authors of [7] have proposed a starvation attack for Wi-Fi AP by utilizing the vulnerability of the Energy Detection threshold and proposed a joined channel coordination framework. Authors of [8], [9] have presented how an existing vulnerability in CSMA/CA-based access mechanism can be resurrected to model a new attack strategy to impact the performance and fairness of the coexisting technologies. However, limited research was conducted on security issues, considering cellular technologies as potential victims. Therefore, to ensure the fair coexistence of cellular and Wi-Fi technologies, it is critical to assess vulnerabilities from all avenues and design exploits to assess them further to offer suitable defensive or deterrent techniques against them.

This work was supported by the US National Science Foundation (NSF) under Grant No. 2304668.

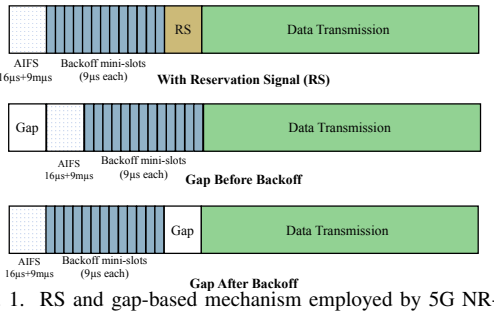


Fig. 1. RS and gap-based mechanism employed by 5G NR-U.

In the proposed CSMA/CA-like approach, the cellular technologies initially conduct a CCA based on an energy-level-based detection mechanism. If the channel appears to be clear, a backoff procedure is carried out, followed by a DIFS period. However, like IEEE 802.11 technologies, cellular technologies such as NR-U/LTE-LAA cannot begin transmission after the backoff procedure and must wait until a specified slot boundary is reached. While the idea of a reservation signal (RS), was brought up to address with this issue, fairness concerns led to the separation of this approach, and a self-deferral-based mechanism was presented. The comparison between RS-based and gap-based mechanisms is illustrated in Fig. 1.

However, this technique contains flaws that malicious actors can exploit to disrupt the coexistence framework. In the former RS-based approach, NR-U would have provision to acquire the channel until the end of the slot boundary to start its transmission, which would render the true slot boundary hidden from the malicious observers. However, in the latter strategy, the attacker can predict future slot boundaries because NR-U is idle after the backoff procedure until the slot boundary, rendering to conceal the information on the slot boundary unattainable. A malicious AP can be employed to sense the channel to detect this information and design a strategy to undermine the channel access of the victim NR-U. For ex-

ample, the malicious AP can carefully design its transmission to restrict the channel access of the victim. As NR-U lacks a Wi-Fi module in its design to detect the preamble and only relies on the energy level of the channel to conduct the CCA, detection of the attacker can be challenging. Thus, the attacker can significantly disrupt the channel access of the victim NR-U and undermine the performance of coexistence.

In light of the aforementioned, (i) we introduce a novel attack strategy called *Random Channel Access Deterrence*, or *RanCAD*, in which an unauthorized Wi-Fi AP takes advantage of a self-deferral-based mechanism's vulnerability to interfere with 5G NR-U communication in the unlicensed 5GHz spectrum band. The malicious AP initially observes the channel to detect the NR-U transmission and predict the future slot boundaries. Later, the attacker randomly starts its transmission inside the slot (and finishes transmission at the slot boundary) to deter the channel access of the victim NR-U in the next slot, compromising the channel access of the victim and degrading the performance significantly, (ii) we assess the impact of the attack using a Discrete Time Markov Chain (DTMC) model from the victim's perspective, and using simulation, we have presented the impact of such anomaly and (iii) we demonstrate how the malevolent AP may carry out this assault covertly by acting in a random manner to remain undetected.

II. Related Work

Though numerous works focused on varying aspects of fairness between Wi-Fi and cellular technologies, security aspects of the given coexistence mechanism gained relatively limited attention. While security was not explicitly covered, [10]–[13] investigated hidden node problems in the context of coexisting Wi-Fi and LTE. Although the authors of [14] conducted a comprehensive study on the security issues of the coexistence of 5G/6G and Wi-Fi in the physical layer, existing security issues in the MAC Layer did not receive the required attention. In [8], the authors discussed backoff manipulation attacks within the coexistence of LTE and Wi-Fi spectrum. This involved a scenario where a malicious LTE eNB strategically employs selfish backoff values to disrupt fairness. Despite the concern regarding the potential for a rogue base station to execute such an attack, the associated implementation costs act as a limiting factor, constraining the potential gains for the attacker. The exploration by the authors in [7] introduced a starvation attack targeting Wi-Fi APs. This attack exploits a vulnerability in the energy detection threshold and the authors propose a coordinated channel sensing scheme against such a scenario. Notably, neither of these studies included cellular technology as a potential victim.

The author of [15] proposed employing a jamming attack carried out by a malevolent Wi-Fi AP to impede the efficiency of concurrent LTE users. While a jamming attack can significantly impact the performance of cellular users of the channel, such an approach is not appropriate for an attacker with energy constraints. On the other hand, the proposed jamming strategy directly causes interference against non-Wi-Fi transmission, thus causing the victim to move to the new channel and making such strategies ineffective. In [9], the authors introduced the concept of a mobile rogue AP in a Private 5G-enabled Industrial Automation System, utilizing an unlicensed spectrum band. The malicious entity employs a MAC layer misbehavior approach, like a selfish backoff attack, aiming to restrict victim channel access; however, the attack's efficiency is contingent on brief channel access rather than continuous occupation. In [16], the authors introduced a smart terminal scheduling scheme for cellular technologies in the presence of multiple eavesdroppers. Though eavesdroppers can pose significant implications in terms of privacy, the proposed RanCAD attack model can actively attack to deter the victim from accessing the channel while remaining undetected. Although the authors of [17], [18] proposed an attack utilizing a periodic nature of a sensing period of the victim secondary user of the spectrum band, proposed RanCAD attack utilizes the scheduling pattern of NR-U in its implementation.

III. Proposed Vulnerability and Attack Strategy

A. Design Vulnerability

Based on 3GPP Release 13 [19], before starting the transmission, an NR-U device must wait for the channel to be idle for $16\mu s$. When the idle counter expires and the channel is confirmed to be clear, NR-U needs to wait for m observation periods (m is variable and ranges from 1-3) of $9\mu s$ each, followed by a random backoff operation. In this paper, we are considering NR-U as utilizing an LBT-based access mechanism where there is a defined backoff stage and no exponential backoff procedure is employed. However, NR-U cannot begin transmission immediately after the backoff phase ends and must wait until the slot boundary is reached. Although 3GPP clearly defined the LBT-based access mechanism, the protocol did not address the remaining period or gap period before the slot boundary. Initially, RS was proposed to reserve the channel occupancy of the cellular user of the channel. But RS-based mechanism can potentially introduce fairness concerns and spectrum resource wastage and the self-deferral-based or gap-based mechanism was introduced as of figure 1 [20].

Although the self-deferral mechanism improves the fairness of the given coexistence mechanism, it introduces a new set of vulnerabilities for malicious entities to exploit. In the previously mentioned RS-based framework, the attacker could not detect the slot boundary because RS can be started at any given moment within the transmission slot and the attacker needs to predict the exact backoff value to achieve its goal. But in the latter, as NR-U remains idle during this period and starts its transmission after that, the attacker can detect the timing of the actual start point of transmission. Utilizing this knowledge, the attacker can eventually predict future slot boundaries and conduct the attack in that manner. In summary, the periodicity of the victim in the proposed gap-based mechanism assists the malicious entity in predicting the future transmission cycle and exploiting this information to disrupt the victim's communication framework.

B. Attack Stages

To successfully utilize this design vulnerability, the malicious AP needs to first *observe* the victim's transmission and later *execute* the attack based on the data from the *observation*

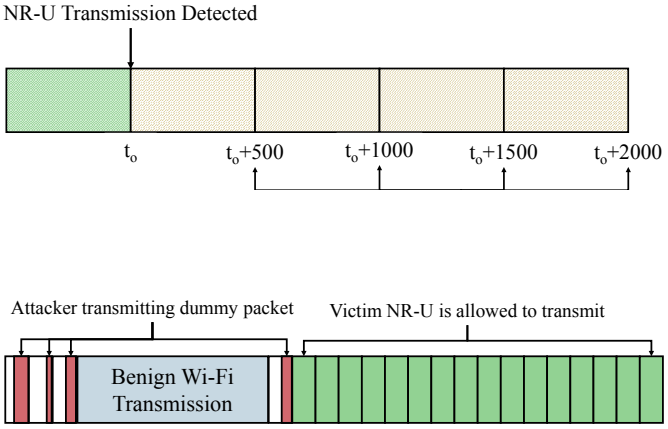


Fig. 3. Execution Stage of RanCAD attack (slot size = 500μs)

period. In the following, two stages of the RanCAD attack namely *observation* and *execution* are discussed in detail:

*1) **Observation Stage**:* In this stage, the malicious AP first traverses through the available channels to determine the victim NR-U's operating channel. When the victim's operating channel is detected, the rogue AP initially observes the channel to understand the transmission cycle of the victim. As an AP, rogue AP can detect benign Wi-Fi transmission using a preamble-based detection technique and non-Wi-Fi transmission using an energy-detection-based mechanism. When the attacker detects the victim's NR-U transmission, utilizing the transmission protocol, it can predict the future slot boundaries of the victim. For example, if a victim NR-U using 5G Numerology 1 would have the transmission slot size of $500\mu s$ and if the attacker detects an NR-U transmission at time t_o, the next slot boundary values would be $(t_o{+}500, t_o{+}1000....)$ or $t_o + 500n$; where n is an integer multiplier. In Fig. 3, the actions taken by the rogue AP are presented.

*2) **Execution Stage**:* In the execution stage, the rogue AP conducts its attack based on the collected data from the *observation stage*. The attacker can only transmit at the end of the transmission slot to make the channel busy for the NR-U to start its transmission. But in this approach, the detection of this anomaly is easier from the victim's perspective as the victim can potentially notice a particular transmission at a certain minislot of the transmission slot and employ a deterrence mechanism. Instead, the rogue AP can choose a random minislot within the transmission slot to start its transmission and transmit until the slot boundary to restrict the channel access of the victim NR-U. The attacker's behavior can employ randomness in its execution to introduce more complexity for the victim to detect such an anomaly by introducing the *attack probability* variable. Although the attacker's goal is to disrupt the victim NR-U's channel access, it does not interrupt the coexisting benign Wi-Fi AP to evade suspicion.

IV. Proposed Attack Model

A. Formation of DTMC

Based on our previous discussion, we comprehend that NR-U implements an LBT-based access mechanism in the unlicensed spectrum band, which is identical to Wi-Fi's CSMA/CA approach. 3GPP stated four types of LBT-based access mechanisms for cellular technologies such as NR-U or LTE-LAA, with categories 3 and 4 having been adopted by the community [2]. In the proposed DTMC mode, we consider NR-U to operate with LBT Category 3, omitting the utilization of the exponential backoff technique. In LBT Category 3, during the backoff phase, NR-U employs random values ranging from 0 to W_o, where W_o is defined as the *Maximum Backoff Value* or cw_{max}. In our proposed model, we are considering cw_{max} or W_o to be 32. Each backoff stage contains minislots of the length of $9\mu s$. If NR-U detects a busy channel during the backoff phase, it will stop its backoff timer until the channel becomes available; whenever the channel is available, NR-U can resume its timer. After completing the backoff phase, NR-U goes through the gap or self-deferral phase until the slot boundary is reached. After this period, if the channel is available, NR-U can transmit for a fixed duration defined as the *Maximum Channel Occupancy Time ($mcot$)*(In this model, $mcot = 6ms$).

Let p_b and p_g represent the unified probability of the channel being busy during the backoff stage and gap period respectively. At the same time, n_g denotes the number of possible minislots for the gap period. In the RanCAD attack scenario, while the attacker can start its transmission from any minislot during the transmission slot, p_b and p_g are

$$p_b = {p_b}' + p_a - {p_b}' \cdot p_a, \tag{1}$$

$$p_g = {p_g}' + p_a - {p_g}' \cdot p_a. \tag{2}$$

where ${p_b}'$ and ${p_g}'$ are the unified probability of the channel being busy due to the *benign Wi-Fi transmission* and p_a is the attacker's probability of conducting its attack. If there is no attack going on or $p_a = 0$, value of p_b and p_g would be characterized as $p_b = {p_b}'$ and $p_g = {p_g}'$ respectively.

Because of its simplicity and versatility, DTMC has been widely employed by scholars to model the transmission cycle of wireless technologies such as 5G NR, Wi-Fi, and others. In [21], the author modeled the Wi-Fi transmission using a DTMC model and evaluated the performance of the CSMA/CA-based access mechanism utilized by IEEE 802.11 technologies. In [22], [23], the authors designed the transmission model of the cellular technologies in the unlicensed spectrum band of 5GHz while coexisting with Wi-Fi. However, none of the previous works considered the presence of the malicious Wi-Fi AP while designing their transmission model. In the proposed DTMC model, as illustrated in Fig. 4, we have considered the presence of malicious AP employing the proposed *RanCAD* attack to disrupt the victim NR-U's transmission. Based on this model, NR-U can have three distinct stages: backoff, gap, and transmission. For our proposed DTMC model, we are considering a saturated throughput scenario where the transmitter has always a packet to transmit. The steady-state probability of each stage can be calculated as

$$b_j = \frac{W_o - j}{W_o(1 - p_b)} \cdot b_o; \quad j\epsilon[1, ..., W_o - 1], \tag{3}$$

$$b_j = \frac{1 - (1 - p_g)^{-j}}{1 - (1 - p_g)^{n_g}} \cdot b_o; \; j\epsilon[-n_g + 1, ... - 1] \tag{4}$$

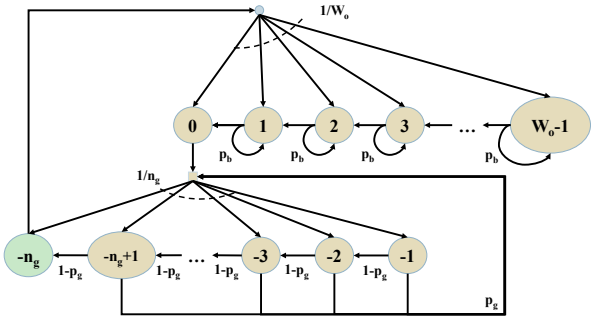


Fig. 4. Impact of RanCAD attack using Discrete Time Markov Chain model

$$b_j = b_o;\ j = -n_g. \tag{5}$$

According to the DTMC model, the summation of all the total steady-state probabilities is 1. So, we can derive:

$$\sum_{j=-ng}^{W_o-1} b_j = 1. \tag{6}$$

Based on the proposed DTMC model, NR-U transmits at the n_g state. So the transmission probability of NR-U or τ_n can be derived as the following:

$$\tau_n = b_{-ng}. \tag{7}$$

In light of the work of [21], [23] the transmission probability of Wi-Fi or τ_w can be formulated as

$$\tau_w = \frac{2(1-p_b)(1-2p_b)}{2(1-p_b)^2(1-2p_b) + W_o p_b(1-2p_b) + (1+W_o-2p_b)(1-2p_b)}. \tag{8}$$

In our proposed model, we are considering in a particular channel, only one NR-U gNB coexists with at least one Wi-Fi AP. From the perspective of NR-U, the probability of the channel being busy or ${P_b}^{NR-U}$ can be formulated as

$${P_b}^{NR-U} = 1 - (1-\tau_w)^w, \tag{9}$$

where w denotes the number of coexisting Wi-Fi APs and $w = (1, 2, 3, ...)$. By solving Equation (3)-(6), we can determine the transmission probability or τ_n. On the other hand, we can also formulate the probability of the channel being busy from the perspective of Wi-Fi or ${P_b}^{Wi-Fi}$ as

$${P_b}^{Wi-Fi} = 1 - (1-\tau_n)\cdot(1-\tau_w)^{w-1}. \tag{10}$$

B. Modeling the Performance Impact

To model the performance of the victim NR-U in the presence of the attacker, we need to understand the possible events in the given coexistence framework. As w number of Wi-Fi AP is coexisting with one NR-U gNB in the presence of an attacker, there can be five distinct events: channel being idle, NR-U successfully occupying the channel, Wi-Fi successfully occupying the channel, Wi-Fi experiencing collision with other Wi-Fi AP and Wi-Fi experiencing collision with NR-U. If their corresponding probability is P_{idle}, $P_{w,s}$, $P_{n,s}$, $P_{w,c}$ and $P_{nw,c}$, respectively, and their respective time length is T_{idle}, $T_{w,s}$, $T_{n,s}$, $T_{w,c}$ and $T_{nw,c}$. Thus, the probability and their corresponding transmission of these events can be formulated as follows based on the work of [22]:

$$P_{idle} = (1-\tau_n)(1-\tau_w)^w, \tag{11}$$

$$T_{idle} = \sigma, \tag{12}$$

$$P_{w,s} = w\tau_w(1-\tau_w)^{w-1}(1-\tau_n), \tag{13}$$

$$T_{w,s} = T_{WP} + T_{SIFS} + T_{ACK} + T_{DIFS} + \sigma, \tag{14}$$

$$P_{n,s} = \tau_n(1-\tau_w)^w, \tag{15}$$

$$T_{n,s} = T_{MCOT} + T_d + \sigma, \tag{16}$$

$$P_{w,c} = (1-\tau_n)[1-(1-\tau_w)^w - w\tau_w(1-\tau_w)^{w-1}], \tag{17}$$

$$T_{w,c} = T_{WP} + T_{DIFS} + \sigma, \tag{18}$$

$$P_{nw,c} = 1 - P_{idle} - P_{w,s} - P_{n,s} - P_{w,c}, \tag{19}$$

$$T_{nw,c} = max(T_{w,c}, T_{n,c}). \tag{20}$$

In this context, σ represents the duration of the channel being idle. Additionally, T_{WP}, T_{SIFS}, T_{ACK}, and T_{DIFS} denote the time intervals for Wi-Fi packet transmission, Short Interframe Space (SIFS), acknowledgment transmission, and Distributed Interframe Space (DIFS), respectively. Furthermore, T_{MCOT} and T_d stand for the transmission opportunity and defer period for NR-U. From Equation (11)-(20), we can derive the mean interval of all these events T_{interval} as follows:

$$\begin{aligned} T_{\text{interval}} = {} & P_{\text{idle}} \times \sigma + P_{\text{w,s}} \times T_{\text{w,s}} + P_{\text{n,s}} \times T_{\text{n,s}} \\ & + P_{\text{w,c}} \times T_{\text{w,c}} + P_{\text{nw,c}} \times T_{\text{nw,c}}. \end{aligned} \tag{21}$$

*1) **Channel Occupancy**: Channel occupancy*, denoted as C_n, can be defined as the proportion of time during which NR-U occupies the channel, encompassing both successful and unsuccessful or, interrupted transmissions. It can be derived as

$$C_n = \frac{P_{\text{n,s}} \times T_{\text{n,s}} + P_{\text{nw,c}} \times T_{\text{nw,c}}}{T_{\text{interval}}}. \tag{22}$$

*2) **Throughput**: Throughput* can be defined as the quantity of data bits transmitted successfully in unit time. According to [22], while U_n is the packet transmission rate of NR-U, the average payload transmission time of NR-U data packet, t_n and throughput for NR-U, T_n can be derived as

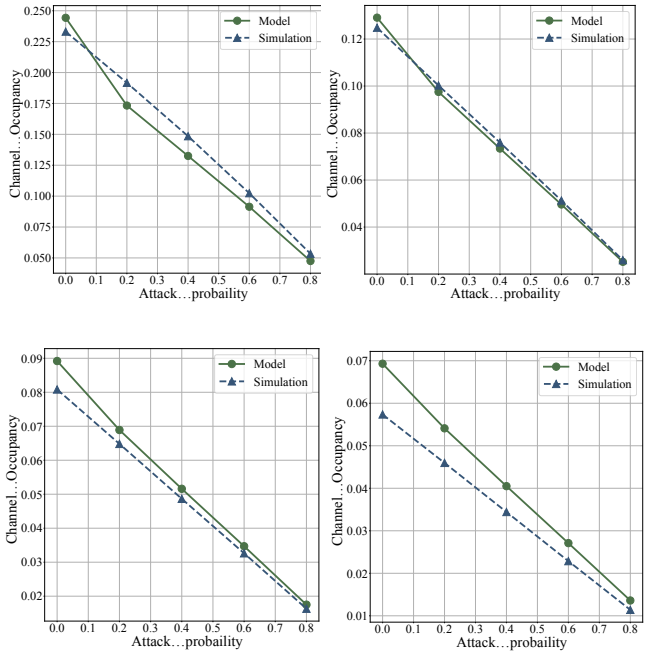
$$t_n = \frac{Pl_n}{U_n}, \tag{23}$$

$$T_n = \frac{Pl_n \times t_n \times U_n}{T_{\text{interval}}}. \tag{24}$$

V. Performance Evaluation

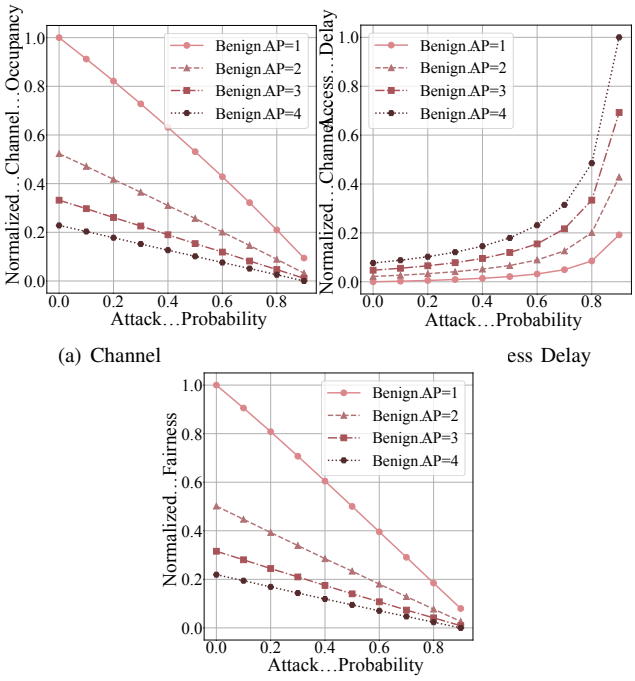
A. Validation of the Proposed Analytical Model

To verify the validity of the proposed DTMC model, we developed a simulation model based on the work of [24], [25]. This simulation addresses the coexistence scenario involving a single NR-U gNB alongside a varying number of Wi-Fi APs under different attack probabilities where $attack\ probability = 0$ is flagged as a non-attack or benign scenario. Our validation process entailed the generation of channel occupancy data for the NR-U in the given coexistence scenarios and subsequent comparison with the DTMC model as illustrated in Fig. 5. Based on the analysis of the generated channel access occupancy, the calculated margin of error between the simulation and the proposed DTMC model was found to be less than 10%, which affirms the model validity.



(c) Benign AP=3 (d) Benign AP=4

Fig. 5. Validation of proposed DTMC model to the simulation model.



(a) Channel ess Delay

(c) Fairness

Fig. 6. Impact of RanCAD attack in the performance of the victim NR-U

B. Performance Analysis of Coexistence Metrics

1) ***Channel Occupancy****:* To maintain a fair coexistence mechanism between Wi-Fi and NR-U, the *channel occupancy* of Wi-Fi and NR-U should not be disrupted due to the malicious behavior of the coexisting technologies. However, based on the simulation result, as depicted in Fig. 6(a), we notice a significant decline in channel occupancy of NR-U due to the impact of the proposed RanCAD attack, posing substantial coercion to the throughput of the NR-U in the unlicensed spectrum band and adversely impacting the performance of high-throughput applications. Thus, the necessity of having an effective mitigation strategy for RanCAD attack emerges as a crucial step towards ensuring the overall efficiency and fairness of the coexistence of Wi-Fi and NR-U in 5GHz spectrum band.

2) ***Channel Access Delay****: Channel access delay* is defined as the time interval between the generation of a data packet and a successful acquisition of channel access by a transmitter. The malicious AP using RanCAD attack strategically obstructs the victim NR-U impeding its channel access and consequently extending the average channel access delay experienced by the victim. As illustrated in Fig. 6(b), an apparent exponential escalation in channel access delay is evident with increasing attack probabilities by the malicious AP. This substantial rise in channel access delay holds ramifications, particularly for applications with stringent latency requirements such as AR/VR and autonomous vehicles.

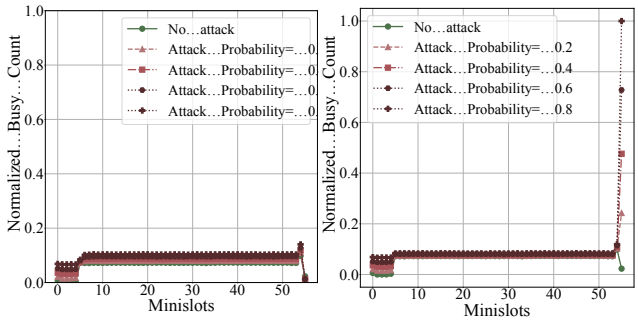
3) ***Fairness****:* Since the notion of spectrum coexistence first emerged, fairness in the coexistence of NR-U/LTE-LAA and Wi-Fi has been a key research problem addressed by the community. With the assistance of Jain's fairness index [26], the fairness of a system where multiple entities are sharing a certain resource can be analyzed. If there are n users sharing a similar resource R and x_i is the throughput of i'th user where $i\epsilon\{1, \cdots, n\}$, Jain's fairness index can be denoted as,

$$\Im(x_1, x_2...., x_n) = \frac{(\sum_{i=1}^{n} x_i)^2}{n \cdot \sum_{i=1}^{n} {x_i}^2}. \tag{25}$$

The proposed RanCAD attack caused significant fairness issues from the perspective of the victim NR-U in the given coexistence mechanism by impeding the victim from getting its fair share of channel access. From Fig. 6(c), it can be derived that, the proposed attack can significantly impact the quantitative fairness of the given coexistence mechanism. Thus it is imperative to introduce a deterrence or detection mechanism against such anomaly.

C. Stealthiness of the Attack

As mentioned earlier, NR-U employs an energy-level detection strategy to initiate CCA and trigger its backoff or self-deferral phase. This approach enables NR-U to identify the minislots in which the channel becomes busy or occupied by the other users of the channel. With a total of approximately 55 minislots within the transmission slot of the length of $500\mu s$ ($500/9 \approx 55$), we introduce the *Minislot busy count* as a key metric. *Minislot busy count* can allow NR-U to track instance of the channel activity during the contention period and gather valuable insights. When a malicious AP incorporates a deterministic approach to begin transmitting at a specific minislot to block the victim from accessing the channel, the victim NR-U could potentially be able to detect this behavior of the attacker. But in the proposed RanCAD attack, the malicious AP chooses a random minislot to begin its transmission, thus evading the potential detection mechanism employed by the victim NR-U.



(a) RanCAD attack (b) Deterministic attack

Fig. 7. Normalized channel busy counts in terms of mini-slots of a slot in Random and Deterministic attack model.

In our proposed simulation model, we simulate another attack scenario where the malicious AP only transmits at the last minislot to restrict the victim's access to the channel, which is defined as a deterministic approach. For comparing the difference between random and deterministic approaches, we are only considering the coexistence scenario of one NR-U gNB and one Wi-Fi AP. Based on the results illustrated in Fig. 7, a noticeable rise in minislot busy count for the last minislot with the increase of the attack probability in the deterministic approach. Contrary to this, in the RanCAD attack model, such discernible features can not be noticed from the provided data. Thus, the malicious AP utilizing the proposed RanCAD attack model can be stealthy from the generic anomaly detection mechanism and victim NR-U is required to employ a more sophisticated detection strategy to thwart such anomalies.

VI. Conclusion

While unlicensed spectrum bands like 5GHz allow cellular technologies like 5G and beyond to extend their spectrum resources cost-effectively, the heterogeneous coexistence can present novel security vulnerabilities for the malicious entity to exploit and disrupt the fair coexistence environment. This paper primarily focused on proposing a novel attack model utilizing the design vulnerability of the gap-based channel access mechanism employed by the NR-U in the unlicensed spectrum band. Using the proposed DTMC model and simulation, we have presented the negative impact of such an anomaly in terms of varying performance metrics like channel access delay, channel occupancy and fairness. We have also illustrated the difficulty of a generic statistical approach to detect such an anomaly in a dynamic coexistence scenario.

References

[1] A. Mamadou Mamadou *et al.*, "Survey on wireless networks coexistence: resource sharing in the 5G era," *Mobile Networks and Applications*, vol. 25, no. 5, pp. 1749–1764, 2020.

[2] 3GPP. 3GPP TR 21.916 V16.2.0 (2022-06). [Online]. Available: https://itecspec.com/archive/3gpp-specification-tr-21-916/

[3] V. Sathya *et al.*, "Standardization advances for cellular and Wi-Fi coexistence in the unlicensed 5 and 6 GHz bands," *GetMobile: Mobile Computing and Communications*, vol. 24, no. 1, pp. 5–15, 2020.

[4] Y. Gao *et al.*, "Achieving proportional fairness for LTE-LAA and Wi-Fi coexistence in unlicensed spectrum," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3390–3404, 2020.

[5] G. Naik *et al.*, "Coexistence of wireless technologies in the 5 GHz bands: A survey of existing solutions and a roadmap for future research," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1777–1798, 2018.

[6] F. Luo *et al.*, "Optimal Coexistence of NR-U with Wi-Fi under 3GPP Fairness Constraint," in *proc. of IEEE ICC*, 2022, pp. 4890–4895.

[7] S. Dongre *et al.*, "Implicit Channel Coordination to Tackle Starvation Attacks in 5G and Wi-Fi Coexistence Systems," in *proc. of IEEE GLOBECOM 2022*, pp. 4136–4141.

[8] I. Samy *et al.*, "Misbehavior Detection in Wi-Fi/LTE Coexistence over Unlicensed Bands," *arXiv preprint arXiv:2104.02776*, 2021.

[9] M. R. Rahman *et al.*, "PACMAN Attack: A Mobility-Powered Attack in Private 5G-Enabled Industrial Automation System," in *proc. of IEEE ICC*, 2023, pp. 4379–4384.

[10] V. Sathya *et al.*, "Hidden-nodes in coexisting LAA & Wi-Fi: a measurement study of real deployments," in *proc. of IEEE ICC Workshops*, 2021, pp. 1–7.

[11] M. Iqbal *et al.*, "Impact of changing energy detection thresholds on fair coexistence of Wi-Fi and LTE in the unlicensed spectrum," in *proc. of IEEE WTS*, 2017, pp. 1–9.

[12] M. Hossain *et al.*, "Jump and wobble: A defense against hidden terminal emulation attack in dense IoT networks," in *proc. of IEEE ICC 2021*, 2021, pp. 1–6.

[13] M. Hossain et al., "Hidden Terminal Emulation: An Attack in Dense IoT Networks in the Shared Spectrum Operation," in *proc. of IEEE GLOBECOM*, 2019, pp. 1–6.

[14] K. Ramezanpour *et al.*, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, p. 109515, 2023.

[15] Z. Liu *et al.*, "CTJammer: A Cross-Technology Reactive Jammer towards Unlicensed LTE," in *proc. of IEEE/ACM IoTDI*, 2022, pp. 95–106.

[16] X. Ding *et al.*, "Security-reliability tradeoff for multi-terminal multi-mode coexisting systems in the presence of multiple eavesdroppers," *IET Communications*, vol. 14, no. 8, pp. 1221–1227, 2020.

[17] M. Hossain *et al.*, "Hide and seek: A defense against off-sensing attack in cognitive radio networks," in *proc. of IEEE INFOCOM*, 2019, pp. 613–621.

[18] M. Hossain et al., "Hide and seek: A Markov-based defense strategy against off-sensing attack in cognitive radio networks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 3028–3041, 2020.

[19] 3GPP. LAA standardization: Coexistence Is The Key. [Online]. Available: https://www.3gpp.org/news-events/1789-laa_update

[20] S. Szott *et al.*, "Using self-deferral to achieve fairness between wi-fi and nr-u in downlink and uplink scenarios," *Computer Communications*, vol. 193, pp. 176–188, 2022.

[21] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on selected areas in communications*, vol. 18, no. 3, pp. 535–547, 2000.

[22] Q. Ren *et al.*, "Performance analysis of an LAA and WiFi coexistence system using the LAA category-4 LBT procedure with GAP," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8007–8018, 2021.

[23] Y. Gao *et al.*, "Performance analysis of LAA and WiFi coexistence in unlicensed spectrum based on Markov chain," in *proc. of IEEE GLOBECOM*, 2016, pp. 1–6.

[24] J. Cichon. A Wi-Fi and NR-U Coexistence Channel Access Simulator based on the Python SimPy Library. [Online]. Available: https://github.com/CichonJakub/5G-Coexistence-SimPy

[25] M. R. Rahman. A Wi-Fi and NR-U Coexistence Channel Access Simulator based on the Python SimPy Library. [Online]. Available: https://github.com/nil0819/simpy-wireless-simulator-nru-wifi-coexistence

[26] M. Zajac *et al.*, "Resolving 5G NR-U contention for gap-based channel access in shared sub-7 GHz bands," *IEEE Access*, vol. 10, pp. 4031–4047, 2022.