Det-RAN: Data-Driven Cross-Layer Real-Time Attack Detection in 5G Open RANs

Alessio Scalingi*, Salvatore D'Oro§, Francesco Restuccia§, Tommaso Melodia§ and Domenico Giustiniano*
*IMDEA Networks Institute, Madrid, Spain {alessio.scalingi, domenico.giustiniano}@imdea.org
§Northeastern University, Boston, USA {s.doro, f.restuccia,t.melodia}@northeastern.edu

Abstract—**Fifth generation (5G) and beyond cellular networks are vulnerable to security threats, primarily due to the lack of integrity protection in the Radio Resource Control (RRC) layer. In order to address this problem, we propose a real-time anomaly detection framework that leverages the concept of distributed applications in 5G Open RAN networks. Specifically, we identify Physical Layer (PHY) features that can generate a reliable fingerprint, infer in a novel way the time of arrival of uplink packets lacking integrity protection, and handle cross-layer features. By identifying legitimate message sources and detecting suspicious activities through an Artificial Intelligence (AI) design, we demonstrate that Open RAN-based applications that run at the edge can be designed to provide additional security to the network. Our solution is first validated in extensive emulation environments achieving over 85% accuracy in predicting potential attacks on unseen test scenarios. We then integrate our approach into a real-world prototype with a large channel emulator to assess its real-time performance and costs. Our solution meets the low-latency real-time constraints of 2 ms, making it well-suited for real-world deployments.**

I. Introduction

The deployment of Fifth Generation (5G) cellular networks promises to revolutionize several industries via more efficient and agile networking capabilities. However, it comes with new and unprecedented threats that arise from the *increased attack surface*. Among others, the *absence of message integrity protection* at the layer 2 of Control Protocol Data Unit (PDU) in 5G New Radio (NR) technologies is largely an open issue, and currently available solutions still rely upon outdated procedures [1] that only partially solve the problem. This leaves 5G networks exposed to several security threats to the most important components of 5G systems, such as the RRC layer [2], [3]. RRC is essential to perform Radio Resource Management, and any attack to its integrity might severely disrupt communications and reliability.

This problem is further exacerbated by the effort to reduce control-plane signaling to the 5G Core Network. In the attempt of balancing between battery efficiency and delivering low latency, 5G has introduced the Inactive State in the RRC. Although particularly beneficial in reducing overhead—especially now that the number of User Equipment (UE) devices connected to 5G networks steadily increases [4])—this state has resulted in a new security threat. In fact, every time the UE transitions to the Inactive state, its low-latency re-connection procedure might lacks the integrity protection. As the change of state for each UE occurs frequently to save energy, the opportunity for an attacker to successfully carry out an attack increases significantly, posing severe threats to cellular network security. In the absence of a mitigation system, users may be disconnected from the network using Denial-of-Service (DoS) attack [5] [6].

This evolving threat landscape prompts action to design and implement timely security measures. However, current state-of-the-art research fails to provide viable solutions to these vulnerabilities. Existing studies predominantly focus on demonstrating these vulnerabilities in 4G and 5G protocols, often through simulations, *but offer no reliable and experimentally tested and validated solutions*. The 3rd Generation Partnership Project (3GPP)'s ongoing efforts in Release 17 to mitigate privacy and security issues, such as protecting broadcast and unicast messages, have not yet yielded a definitive solution [7]. Some messages, including those within the RRC protocol, occur before the establishment of security measures. Despite proposals for solutions like the application of asymmetric cryptography to all RRC messages, there is currently no work affecting RRC procedure protection standards.

Summary of novel contributions. Given the aforementioned state of the art, open issues and current network vulnerabilities, in this paper we introduce an Open Radio Access Network (RAN)-based real-time framework that enhances control plane security by *proactively detecting attacks*. The Open RAN paradigm emphasizes openness, virtualization, programmability, and data-driven control [8]–[10]. Our proposed framework leverages the concept of dApps [11], i.e., decentralized applications that extend Open RAN xApps and rApps executing at the RAN Intelligent Controllers (RICs), to bring intelligence at the edge of Open RAN systems and perform on-the-spot inference of malicious users. Our framework is *designed to counter malicious attacks by addressing the vulnerabilities in the RRC protocol* with specific focus on the increasing usage of Inactive state in 5G and its vulnerabilities.

The primary scientific contribution of this paper is the introduction of a real-time framework that aims at detecting attacks in the RRC messages and procedures of 5G networks. We leverage openness and software-based principles of Open RAN to develop a cross-layer approach where we extract heterogeneous data from the different layers of the protocol stack (such as In-phase and Quadrature (IQ) samples, channel state information, ranging, and temporary user identity) for creating reliable, dynamic, UE-specific fingerprints that are updated over time according to user mobility and varying channel conditions, thus offering a reliable and effective mechanism to detect attacks even when network condition change. Our framework extracts Time of Arrival (ToA) measurements that offer localization capabilities. The novelty of the approach is that it works *without* relying on 5G positioning reference signals that could be used only after the UE is connected to the network (hence too late if another UE is a malicious identity spoofer already connected to the network [12], [13]).

All these cross-layer measurements are part of our full-stack features which are processed by our AI design. Our key findings indicate that, upon comparison with relevant AI-based solutions, our framework can accurately predict potential attacks with an accuracy exceeding 85%. Moreover, we show via experimental results that our approach is also general and delivers high accuracy even in the case of unseen channel conditions, topologies and mobility patterns, thus making it a good candidate to be deployed and used in real-world cellular deployments. Our model exhibits high precision in predicting attacks, substantially minimizing the incidence of false negatives. Our solution's efficacy is validated through testing in large-scale emulation environments, reflecting real-world scenarios. Furthermore, we have deployed and tested an integrated prototype for real-time inference that adheres to the network's operational time constraints, ensuring seamless integration and secure operation. As part of our contribution, we also release the dataset for further research, fostering broader innovation in telecommunications security.

II. Challenges

In this section, we discuss the main challenges related to designing, developing and prototyping our system.

Challenge A: identifying PHY features that can generate a reliable fingerprint. Existing vulnerabilities of 5G systems primarily stem from the messages in the RRC layer where an adversary can impersonate UE either to gain access to the network, or to force the disconnection of a target UE (see Section III-C). We aim to design a framework that can instantaneously scan these messages and verify their legitimacy to ensure they have not originated from potential attackers. Thus, understanding which PHY features are relevant and which are redundant or not representative to identify attacks is necessary.

Challenge B: integrating cross-layer features. We detect anomalous messages by combining PHY features with PDU-related data extracted at the RRC layer, thus coupling information to be used as inputs for our AI models. This cross-layer mechanism introduces a technical challenge related to synchronization and management where data from the different layers has different formats and is generated at different times.

Challenge C: developing AI capabilities at the edge. As discussed in Section III-C, some RRC attacks can instantaneously cause the detachment of a UE targeted by a malicious user. This exposes the network to severe threats that call for real-time attack and anomaly detection. The flexibility offered by Open RAN could help in addressing these security concerns. However, current efforts have not shown how Open RAN can effectively mitigate these vulnerabilities and help in identifying anomalies that could suggest the occurrence of attacks. Most importantly, Open RAN-based solutions for security applications are still in their infancy and have been not tested in realistic, large-scale, experimental environments. The real-time constraint and the need for robust and precise AI inference is a technical hurdle demanding interplay of system design and computational efficiency.

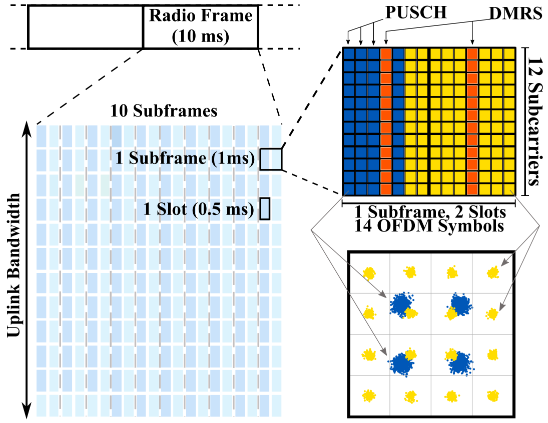


Fig. 1: Physical layer and Resource Grid of uplink data.

Challenge D: experimental dataset and system testing. Aiming to ensure the reliability and robustness of our AI, we require a rich and extensive dataset replicating real-world network environments. The generation of this dataset, encompassing various network conditions, user behaviors, and potential security threats, becomes a substantial challenge.

III. Background and attacker model

This section provides an overview of the 5G NR architecture focusing on PHY and RRC procedures relevant to this study, and introduce the attacker model.

A. 5G System architecture

The architecture of 5G systems comprises three main components: UE, the 5G Radio Access Network (5G-RAN), and the 5G Core Network (5G-CN). A UE is a device, e.g., a smartphone or Internet of Things (IoT) device, equipped with a Universal Subscriber Identity Module (USIM). Each USIM possesses a unique Subscription Permanent Identifier (SuPI), akin to how International Mobile Subscriber Identity (IMSI) is used to identify users in previous 3G/4G generations. In 5G, to protect the SuPI, the UE sends its correspondent Subscriber Concealed Identifier (SuCI) to the 5G-CN for authentication. Upon authentication, the Access and Mobility Management Function (AMF) assigns a 5G Temporary Mobile Subscriber Identity (5G-TMSI) to the UE. This 5G-TMSI is used in all communication between the UE and the network, in order to protect the SuCI from potential eavesdroppers.

The 5G-RAN is represented by the fabric of base stations (i.e., Next Generation NodeB (gNB)s) that use 5G radio technology for providing high-speed, low-latency coverage to UEs. Finally, the 5G-CN offers services necessary to control and monitor the network, handle billing and mobility, authentication, paging, and manage user and data planes.

B. Physical layer and resource grid

At the PHY layer, uplink data from the UE to the gNB is transmitted using the Physical Uplink Shared CHannel (PUSCH), a logical channel that contains user and signaling data. UE's transmissions on PUSCH are transmitted over dedicated resources in the Resource Grid (RG). The RG consists of a time-frequency matrix of slots that contains Orthogonal Frequency-Division Multiplexing (OFDM) symbols as shown on the left of Fig. 1. A single Radio Frame in OFDM has a duration of 10 ms, and contains 10 sub-frames of 1 ms each. In the simplest configuration, we have two slots per sub-frames. One slot consists of 14 small blocks called *symbols* in time domain transmitted over the 12 sub-carriers. The Resource Block (RB) consists of 12 sub-carriers and 14 OFDM symbols and it divides the RG. Finally, the single Resource Element (RE) is the smallest block in the RB which is the single sub-carrier for a symbol, and it represents one value in the IQ constellation. The gNB uses a scheduler to assign RBs, in uplink, to each UE that needs to send data through the PUSCH.

C. RRC states and procedures

The RRC layer hosts several processes designed to facilitate communication, manage resources, and ensure seamless mobility while UEs move throughout the 5G network.

In 5G, there are three possible RRC states, namely RRC Idle, RRC Connected, and RRC Inactive. A UE is in RRC Idle when there is no active radio connection toward the network. The RRC Connected state indicates that a secure radio connection has been established between the UE and the network. The RRC Inactive state is an intermediate state introduced in 5G where the UE maintains a context within the network, but without establishing an active dedicated radio connection with the goal of facilitating faster reconnection times while reducing power consumption. The management of the above states is performed via a set of RRC procedures. The most relevant for our work are briefly described below.

RRC Setup. This procedure is initiated by a UE to establish a connection with the network. The UE sends the gNB an RRC Setup Request (*RRCSetupRequest*) that includes its 5G-TMSI.

RRC Release. The network can release the radio resources allocated to the UE and suspend its established RRC connection through the RRC Release (*RRCRelease*) message. This procedure effectively transitions the UE into an Inactive state.

RRC Resume. The transition from Inactive to Connected state can be initiated by the UE through the RRC Resume procedure, involving a subset of the messages of the RRC Setup procedure, like RRC Resume Request (*RRCResumeRequest*), and RRC Resume Complete (*RRCResumeComplete*).

D. Attacker model

In this section, we describe the attacker model, and illustrate how the attacker can wreak havoc of 5G systems if proper defense mechanisms (such as the one we propose) are not in place. A high-level attacker model is illustrated in Fig. 2, and details are provided in the following. The 5G-TMSI takes a crucial role in protecting the UE's identity(Sec. III-A). The low 5G-TMSI refresh rates in commercial 5G networks enable the spoofing of identities by malicious users [14], [15], posing threats to legitimate UEs, leading to disconnection or identifier compromise. Indeed, integrity protection mechanisms used for some RRC control messages are not applicable at Layer 2 [1], thus enabling an adversary to build and carry out attacks [16].

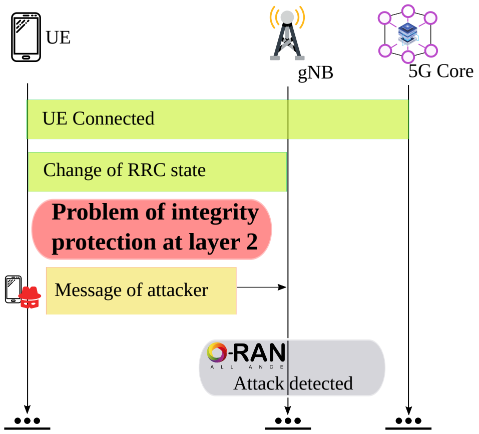


Fig. 2: The absence of message integrity protection at the layer 2 leaves 5G networks exposed to several security threats such as the Radio Resource Control (RRC) layer. We propose an O-RAN-based real-time framework aimed at enhancing control plane security by proactively detecting attacks.

These vulnerabilities can be exploited in several ways. For instance, upon completion of the registration procedure the UE goes into RRC Inactive state if no traffic is exchanged. If the attacker is able to eavesdrop victim's 5G-TMSI, it can generate an *RRCSetupRequest* containing the spoofed 5G-TMSI and trigger a DoS because the 5G-CN removes the UE's security context. An alternative version of this attack can be performed via *RRCResumeRequest* by sending them over the initial signaling [3]. It is worth mentioning that such attacks are possible due to procedures included in standard's specifications. For example, the recently introduced Short Data Transmission (SDT) procedure introduced in the 3GPP [17] is designed to further reduce signaling with the 5G-CN in case of small and infrequent data transmission while the UE remains in RRC Inactive. We find that this procedure employs *RRCResumeRequest* messages, which are the same that can be exploited by an attacker to perform DoS. Additionally, despite *RRCResumeRequest* over the initial signaling being unusual, but demonstrated in [3], we emphasize the importance of considering these messages within the system design in order to alert an ongoing attack attempts.

Another family of uplink messages without integrity protection that can be used to expose the victim's identifier. Here the attacker can act as a Man-in-the-Middle relay and exploit *RRCSecurityModeFailure*, then in case of limited service the UE may even expose its SuPI in plaintext, which can be captured by fake base stations [3].

All of the above attacks have not yet found an effective solution, and countermeasures to discern the legitimacy of the UE and proactively avoid these attacks in real-time are still greatly needed at the gNB.

IV. Cross-layer Features for attack detection

To provide an effective solution against the vulnerabilities and attacks illustrated in the previous section, we describe the set of cross-layer features that are at the basis of our solution and discuss why they are important in addressing Challenges A and B. The summary of the features is presented in Tab. I.

A. *IQ, Channel Features and UE Identity*

IQ Features. Every RRC message, including those without integrity protection (Sec. III-D), consists of PUSCH-related IQs transmitted at specific symbols in the RGs (Sec. III-B). We collect these IQ samples to create a PHY layer fingerprint of the transmitting UE. Note that while IQs before channel equalization provide essential information about the status of the channel, this information alone is not sufficient to distinguish between different UEs due to the large impact that ambient noise and mobility (e.g., phase rotation, Doppler's effect, interference) has on received IQs. For this reason, we use IQ samples collected after channel equalization as they contain constellations where the majority of channel impairments have been removed by the equalization process.

Channel Features. In order to not lose channel state information, together with the PUSCH IQ samples after equalization, we also collect channel features for every received packets. Channel state information is calculated by the gNB for every received packet, with the list provided in Tab. I. These PHY layer characteristics jointly with the PUSCH-IQ after equalization, are fundamental to identify the singularity of the RRC messages from different UEs. In fact, as we will show in Section VIII, they increase detection accuracy and can effectively be used to determine if a transmission has been originated by a legitimate UE or an attacker.

UE Identity. Lastly, we store both 5G-TMSI and the current Radio Network Temporary Identifier (RNTI) which we use to map received message's features with its estimated UE.

B. *Fast Ranging Estimation*

Assuming that the legitimate user is a distance d_1, and the attacker at $d_2 \neq d_1$, the network could discern a potential attacker from a legitimate user of the network through accurate ranging. The Ranging estimation leverages ToA information of radio frequency signals to compute the distance between devices. 5G systems heavily rely on the Sounding Reference Signal (SRS) reference signal for ToA estimate, which are sent over the full bandwidth of the signal to provide the highest accuracy in estimating such distance [18]. However, the critical problem is that it requires the UE to be in RRC Connected state, which is not suitable for early detection of threats.

TABLE I: Summary of features used in this work.

Type	Name	Layer
IQ Features	PUSCH-IQ Samples	PHY
	Received DMRS-IQ Samples	
	Expected DMRS-IQ Samples	
Channel Features	Signal-to-Noise Ratio	
	Channel Frequency Offset	
	Energy per Resource Element	
	Energy per Resource Element in Decibels	
	Measured Reference Signal RE Average Power	
	Noise Estimate	
	Noise Estimate in dB Full Scale	
	Time Alignment Error	
UE Identity	Temporary Mobile Subscriber Identity	
	Radio Network Temporary Identifier	RRC

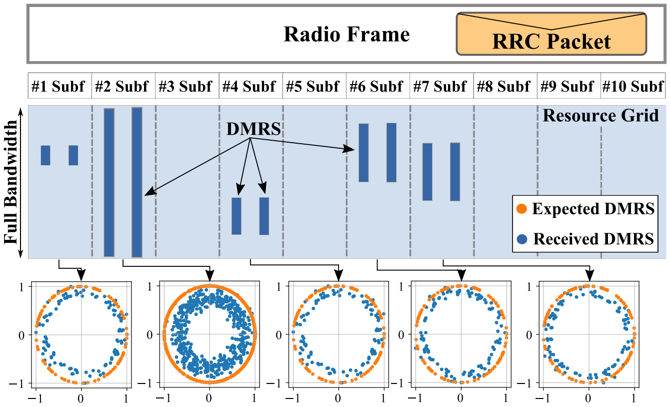


Fig. 3: We leverage Demodulation Reference Signal (DMRS) pilot sequences in subframe 2 of RRC packets for fast estimation of the range between the transmitting UE and the gNB.

In contrast, we find that the DMRS is a known pilot sequence that is embedded in transmitted data such as RRC packets, and it does not need the UE to be in RRC Connected state. Therefore, it is essential to achieve reliable communication, and each UE (even the attackers) must use DMRS to guarantee that its messages are decoded correctly. Although DMRS is a pilot sequence, it is typically not used for localization purposes. However, as shown in Fig. 3, *we find that some sequence of DMRS in the RRC packets, in particular those related to subframe 2 ("#2 Subf" in Fig. 3) are sent over the full bandwidth, as the SRS for localization does.* Our goal is to explore this subset of Received DMRS sequences for fine ToA estimation. We also consider the Expected DMRS IQ samples, which are known and available at the gNB as they are used to provide ground truth to perform channel equalization.

More formally, in the frequency domain, the gNB receives the DMRS $Y[j]$, which can be expressed as:

$$Y[j] = H[j]X[j] + W[j] \tag{1}$$

where $H[j]$, $X[j]$, and $W[j]$ represent the j-th sample of the channel, the Expected DMRS (transmitted by the UE), and white Gaussian noise, respectively. Note that as we use DMRS in subframe of RRC packets, where samples are computed with the resolution of the full bandwidth (Fig. 3). The observed cross-correlation between the Received DMRS and Expected DMRS, denoted as $r_{DMRS}[n]$, is given by

$$r_{DMRS}[n] = IDFT\{Y[J]X^*[J]\} \tag{2}$$

where n represents the discrete time sample, $(\cdot)^*$ is the conjugate operator, and $IDFT\{\cdot\}$ represents the Inverse Discrete Fourier Transform. The gNB estimates the ToA by identifying the argument that maximizes the absolute value of the cross-correlation between Received DMRS and Expected DMRS:

$$i = \arg\max |r_{DMRS}[n]| \tag{3}$$

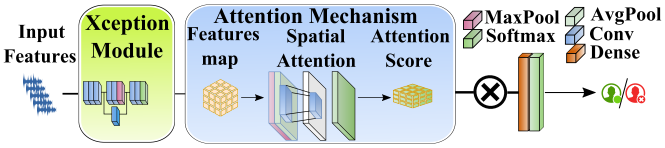


Fig. 4: AI module of the proposed framework.

The computed i-th sample in Eq. 3 represents the ToA delay computed in number of discrete time samples. This metric provides an estimate of the distance between the UE and the gNB. Estimating range involves errors that create uncertainty in identifying the user or attacker's distance. Using a threshold for binary decisions may increase false positives or negatives.

We then propose to use a *soft decision that relates to the probability distribution of distance estimates*, employed by our framework (cf. Sec. V) to identify potential attacks. However, the multipath channel between the UE and the gNB is unknown. To overcome this issue, we use the formula from the *Chebyshev's inequality* [19]:

$$P_r(|X-\mu| \geq \alpha\sigma) \leq 1/\alpha^2. \tag{4}$$

It provides an upper bound over a random variable X deviating from its mean μ by a factor of α standard deviations σ for a wide class of distributions. The procedure involves calculating μ and σ for a specific data window and determines the absolute deviation of a distance from μ, expressed in terms of σ units, referred to as α. For instance, with α=2, the probability that it deviates more than 2σ must be equal or smaller than 25%, or that at least 75% of the data must be within 2σ.

For the analysis, we first compute $\alpha = (X-\mu)/\sigma$ over the rolling window of the latest K messages. A large α indicates that the estimated ToA delay X is far from the mean (potentially an outlier). Conversely, a small α indicates that X is close to the mean. Inversely, $1/\alpha^2$ reflects the deviation from the mean: small values of $1/\alpha^2$ suggest large deviations (potential outliers), and large values of $1/\alpha^2$ suggest small deviations (closer to the mean). We then use $1/\alpha^2$ as input feature of our AI module, as this soft decision better relates to probabilities, and in particular, Chebyshev's inequality (cf. eq. 4). In the next section, we describe how the above cross-layer features can be combined and used to develop an AI-based module that can detect attacks.

V. AI Module

The AI module is the core of our framework and it is designed to consider the following aspects:

- Given the complexity and heterogeneity of features, establishing a linear relationship is challenging. As an example, it is hard to determine a clear relationship between IQs of a UE and the distance probability soft-metric defined in IV. For this reason, the use of AI, which can extract such relationships from the data and provide a non-linear link between such metrics, becomes crucial;
- The input relies on recent RRC messages, and AI distinguishes between legitimate UE and potential attackers in real time, detecting attacks before they become effective.

Starting with the simplest design, our investigation progressively integrates more complex and well-established models like 2DCNN-model, ResNET, and Xception [20]. The final design is inspired by the work of [21] that explores *attention mechanisms* to augment the representational power of the model by focusing on salient features and suppressing superfluous ones, which is critical to address Challenge A. Attention is particularly beneficial in our context. The Ranging Estimation as an input feature could be important for the model's decision, but suffers from noise in practical deployments due to quantization errors in the measurement that depend on the bandwidth used by the UE also because it could move to different locations with different spatial characteristics and multipath. The attention mechanism, considering UE's mobility, addresses this issue by adjusting the importance of RRC message fingerprinting based on data quality and its relationship with other features.

As depicted in Fig. 4, the foundation of the design of the AI module is the Xception architecture [20], [22], which we extend with the *spatial attention mechanisms* to learn which features extracted by Xception are more important for the final output, and under which conditions.

The Xception module operates on the premise of *depth-wise separable convolutions*, enabling it to learn cross-channel correlations and spatial correlations independently. Then, the attention mechanism is deployed on top of the high-dimensional feature map returned by the Xception module. The spatial attention aggregates information using both average-pooling and max-pooling operations over the convolution, yielding the attention score feature map. The output of the attention block is integrated with the initial Xception module via element-wise multiplication in the training phase. Then network's final output is the *SoftMax* layer that outputs the probability of the latest RRC message belonging to the same UE.

VI. Det-RAN Framework

We present a high-level overview of the proposed framework and its components in Fig. 5. The goal of `Det-RAN` is to extract the cross-layer features identified in Section IV from the incoming messages, and use the AI module introduced in Section V to identify the occurrence/absence of attacks. Upon detection of an attack (e.g., a *RRCSetupRequest* generated to disconnect a target UE as discussed in Section III-D), the system automatically reacts by rejecting the request and notifies the 5G-CN that an attack might be ongoing.

We also describe how the proposed AI solution can be developed and integrated within a 5G system by leveraging the concept of *dApps*, i.e., intelligent applications that extend xApps and rApps hosted at the RICs by bringing AI capabilities to CUs and DUs directly, therefore addressing Challenge C. We then illustrate how cross-layer data can be extracted from the protocol stack of messages received by the gNB, and processed together to create a unified data structure, e.g. a buffer, that can be fed to our AI module.

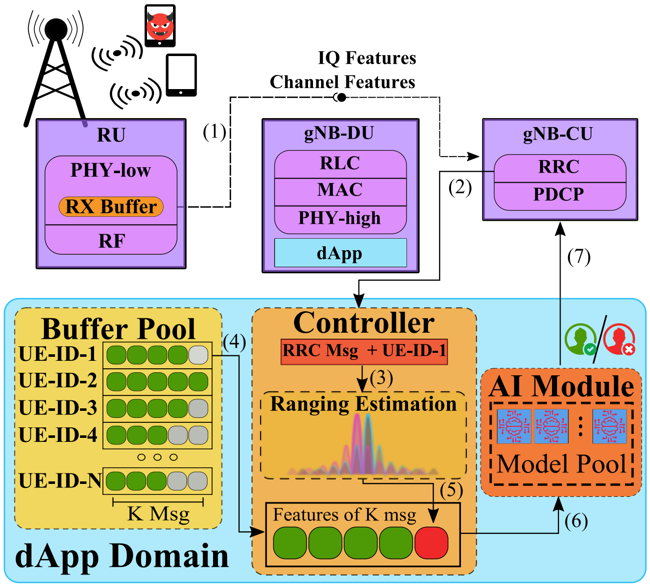


Fig. 5: High-level illustration of dApp design, where we highlight the three main modules and how they interact.

A. dApp Design in Open RAN

As mentioned in Section III-D, *a successful attack to RRC procedures can be accomplished with a single message. For this reason, an effective solution must be able to detect such attacks in real time and upon receiving such messages*. This requires being able to host the defense mechanism directly at the gNB. The combination of the O-RAN architecture with dApps offer the ideal platform to meet the above requirement and perform early attack detection at gNB in real-time. We design a `Det-RAN` to be hosted directly at the gNB where all of the Features (Section IV) are collected and made available.

The main components of our dApp are: a *Buffer Pool* storing features collected over time for each UE; a *Controller* taking decisions on the occurrence of attacks; and the *AI Module* introduced in Section V, that compares past and present features of received packets to detect anomalies. The Controller also hosts a *Ranging Estimation* that computes attack probability with Eq.4 described in Section IV-B.

Walk Through. The gNB-node communicates with multiple UEs. Following 3GPP and O-RAN specifications, the gNB is split into Radio Unit (RU), Distributed Unit (DU) and Centralized Unit (CU). The dApp runs on the gNB-DU. The uplink signals from all UEs are stored into a receiver buffer, referred to as *RxBuffer*, located at *PHY-Low layer*. The steps executed by our solution are described below (cf. Fig. 5):

(1) IQs collected at the PHY layer are converted from time to frequency domain and equalized. The features in Tab. I are extracted and forwarded to the higher layer via the already existing 5G interfaces between PHY, MAC, and RRC.

(2) The *Controller*, upon receiving an RRC message, extracts the features generated in the previous step together with UE's identity[1] and feeds them to the AI module to inspect a possible attack *before* the RRC message is decoded.

(3) The *Ranging Estimation Module* in the *Controller* processes the *DMRS-IQ* of the RRC message to compute ToA and Chebyshev's probability (cf. Secion. IV).

(4) Using the User-ID, the *Controller* pulls the corresponding buffer from the *Buffer Pool* and appends the new features. Each buffer of the pool is identified by the 5G-TMSI. Although one could potentially maintain features for any UE that visited the gNB, a more scalable solution maintains only those that recently visited the gNB.

(5) The Chebyshev's probabilities of ranging measurements (see Eq. 4) are stored in the pool together with the other features. We only store the last K features so that the buffer represents the short history of the UE's RRC messages. How to compute the value of K will be discussed in Section VIII-B.

(6) The *AI Module* processes the evolution of the features and infers if the latest message is an attempt of attack.

(7) The inference output is returned to the RRC layer which rejects the RRC request in case of detected attack.

B. Cross-layer Feature Link: from Layer 1 to Layer 2

In the software stack, a *Worker* thread decodes the *RxBuffer* by processing signals over the RG within a Radio Frame. To differentiate among UEs and accurately decode transmissions, the Worker relies on a grant mechanism, iterating over all users' RNTIs to identify the RBs assigned to each UE, which are logically transmitted over the PUSCHs (Sec.III-B). Firstly, channel equalization utilizing the DMRS calculates Channel Features for the current UE. At this point, pointers with copies of the *Received* and *Expected* DMRS along with Channel Features values are stored as the first part of the system. After channel equalization, the software proceeds to decode the associated PUSCH symbols. To limit resource consumption, only a vector of 128 IQ-PUSCH is maintained. After completing the decoding process at the PHY, these pointers are transferred to the RRC layer, so that the dApp can access the memory area where PHY features are stored, thus addressing *Challenge B*.

A parallel thread handles the above operations to guarantee that communication procedures proceed uninterrupted while `Det-RAN` processes data and the dApp performs inference.

C. Capture UE's Messages evolution with the AI

The *Buffer Pool* is designed so that each connected UE has a dedicated buffer, known as *UE-ID-X-Buffer*. Upon a new UE connects to the gNB, a new buffer is instantiated, using the UE-5G-TMSI to identify and access the buffer. The k-th entry in the buffer is a data structure that incorporates the IQ-PUSCH, Channel Features, and the *Distance probability* computed by the Range Estimation. We use a First-Input-Fist-Output policy to maintain the latest K entries only.

As the AI model has to run in the gNB and in real-time, the *Buffer Pool* is fundamental to capture the history of the message and jointly foster the AI capability at the edge, addressing the Challenge C. Larger values of K imply increased inference latency, but also provide more information for the model's decision. In this sense, the parameter K must be selected carefully to strike a balance between resource consumption,

[1] At this layer, the decoded PDU has the User-ID information, e.g. the 5G-TMSI in the *RRCSetupRequest* (TS 38.331).

accuracy and real-time responsiveness (i.e., $\leq$10ms). These aspects will be studied in detail in Sec. VIII.

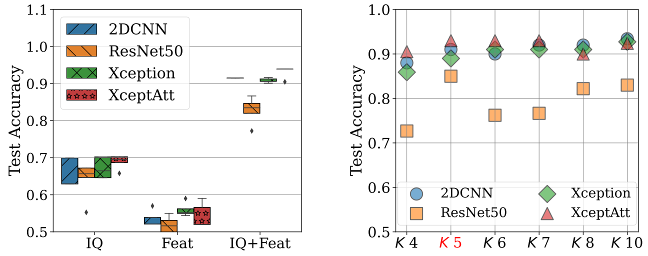
VII. Data collection

To address Challenge D, the experiments conducted for this research utilize the *Colosseum* testbed [23], a high-fidelity RF emulation environment with software-defined radios (SDRs) in-the-loop. Central to Colosseum is MCHEM, a massive channel emulation system, capable of emulating wireless channels (including effects such as fading, mobility and obstacles) with high accuracy and in a reproducible way between any pair of its 128 SDR-based radio nodes. Such a testbed ensures the reproducibility and repeatability of our experiments.

Colosseum offers *Scenarios* emulating real-world deployments of various cities world-wide with gNBs (whose coordinates are extracted from OpenCellID) serving UEs. We consider three Colosseum scenarios—Rome (Italy), Boston (USA), and Powder (USA)—simulating various urban cellular deployments across $0.5km^2$, $0.95km^2$, and $3.6km^2$ areas. Each scenario involves a gNB serving five UEs using RF configuration operating at 1GHz frequency and 20MHz bandwidth in Frequency Division Multiplexing (FDD) using the open-source srsRAN project [24]. Noteworthy, in these scenarios UE mobility is also emulated by the MCHEM, a the user mobility is crucial for the evaluation.

We have designed the following pipeline to collect a dataset that is representative of potential RRC messages lacking integrity protection. First, the UE is turned on and proceeds through initial registration with the RAN and 5G-CN. Upon completing registration, we do not exchange any traffic so that the *Inactivity Timer*[2] expires and UE's state changes to Inactive. At this point, the UE exchanges traffic with the gNB with the sole purpose to resume the connection using an RRC message which will reset the Inactivity Timer. During all these interactions, `Det-RAN` captures the Features (cf. Section IV) related to the uplink RRC messages. In this way, we can at the same time generate a dataset that contains only specific RRC messages and accounts for varying typologies, channel conditions and mobility, thus addressing Challenge D.

We generate a binary label for each K-long sequence of RRC messages we capture. If all K RRC messages are generated by a legitimate UE, we set the label to 0. If the K-th message is instead generated by an attacker (but the previous *K-1* messages are from the same legitimate UE) the label is 1 to describe an ongoing attack. We also shuffle the *K-1* messages' temporal order to introduce uncertainty and facilitate AI model's generalization, making it robust against time-varying channel conditions. The final AI model is trained over a dataset of 4720 balanced sample instances of attacks and legitimate RRC messages. Lastly, acknowledging that real-world scenarios often involve more than five UEs per gNB, the study aims to evaluate the feasibility of our methodology in initial model development and testing.



(a) Accuracy of NNs trained with different combinations of features.

(b) Test accuracy of the different models as a function of the buffer size K.

Fig. 6: Performance evaluation of the different models.

VIII. Experimental Evaluation

This section benchmarks various AI designs—2DCNN, ResNet50, Xception, and our extended Xception with attention mechanism (Sec. V). We report accuracy as a metric due to a balanced dataset and paper's space constraints.

A. Model and feature comparison

In this study, we aim at understanding what features are the most effective in detecting attacks. Fig. 6a shows the test accuracy of the different models trained with different combinations of features. For this evaluation, we only consider data from the Rome scenario. The model trained with only IQs demonstrates roughly equivalent performances across different architectures, with none exceeding 70% accuracy on test data. A notable performance decrease is observed when models are trained exclusively with only the Channel Features. Considering the fact that our datasets are balanced, the failure to surpass 60% accuracy suggests these models are struggling to learn. As the training scenario involves user mobility, Channel Features alone may not be adequate to discern consistent patterns due to their dynamic nature. However, training models with all the features, improves their capability in identifying patterns corresponding to the UEs achieving an accuracy close to 90%. This suggests a precise detection of the message's fingerprint sent by the UE, which makes it possible to accurately identify attacks. Specifically, our custom architecture, referred to as *XceptAtt*, surpasses other models in terms of accuracy due to the inclusion of an attention mechanism atop the *Xception* base model. It is important to note that, for this study, the buffer capacity K for every UE is set to 5 messages.

B. Selecting the value of the K parameter

A study on the parameter K is presented, i.e., the capacity of the feature buffer. This evaluation is essential to strike a balance between minimal buffer capacity and maximal accuracy as increasing the buffer size inherently requires more storage and computational resources, impacting inference time.

With Rome scenario as a reference, we compare performance for different values of K, ranging from 4 to 10. In Fig. 6b, we report the test accuracy as a function of K. While the results across different models exhibit slight variations, the highest overall accuracy is attained with K=10. However, we notice that our XceptAtt model attains very close results with

[2] This timer is generally set to values in the order of a few couple tens of seconds. When it expires, the gNB places the UE into INACTIVE/IDLE state as defined in 3GPP TS 38.331.

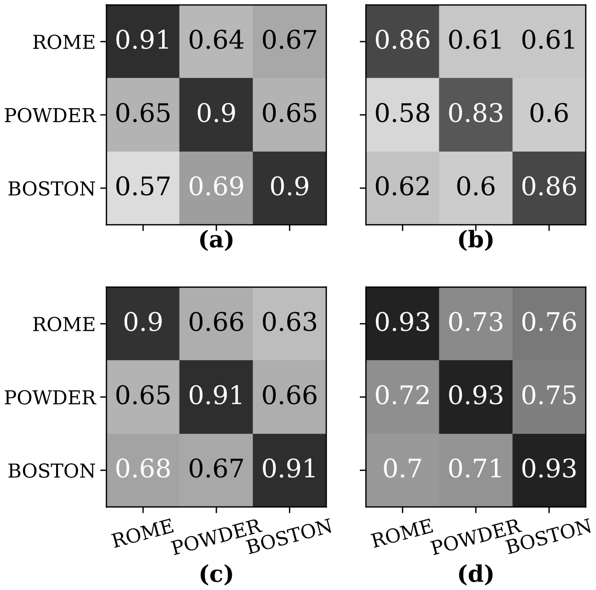


Fig. 7: Testing accuracy of different Neural Network (NN) architectures trained with a single scenario and tested on other scenarios. (a) Baseline 2DCNN Model. (b) ResNet50. (c) Xception. (d) Xception with the attention mechanism.

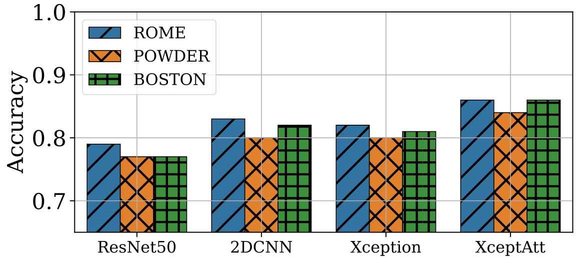


Fig. 8: Different NN architectures trained on multiple scenarios and tested on single scenario, achieving over 85% accuracy in predicting potential attacks on unseen test scenarios.

only K=5, which is 50% smaller and thus offers a better trade-off in terms of accuracy, memory utilization and fast inference time. We use K=5 as a reference value hereafter.

C. Generalization

In the previous evaluations, all the models are trained and tested with data collected from the same scenario. This study attempts to evaluate the models' ability to generalize across unseen scenarios by mixing training and testing sets. This is a crucial factor for real-world applications where, for instance, a network operator may deploy the model in an area never encountered during training. With this study, we aim to identify an AI model that can generalize across unseen scenarios and channel conditions.

The methodology is the following: in the training NNs are fed with data from a scenario, e.g. Rome, then the accuracy is calculated on test data from an unseen scenario, e.g., Boston. The results are summarized in Fig. 7. Each cell represents the accuracy of the corresponding model when trained on a scenario (left label) and tested on another (bottom label). Fig. 7-(a) shows that the baseline 2DCNN architecture is unable to surpass 70% accuracy under unseen conditions. Overall, all the models studied show good performance when tested in

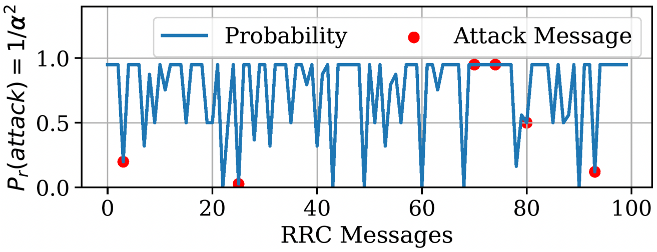


Fig. 9: Chebyshev's probability to discern if an RRC message is received at the gNB from the same UE.

the same training scenario, but lack performance when tested over unseen scenario. Moreover, the custom architecture in Fig 7-(d) shows that, despite a loss in accuracy when tested on unseen data, our XceptAtt is best at generalizing.

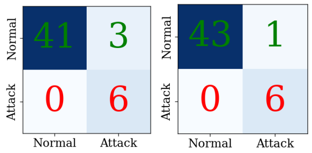
We also consider the case where we train our AI models using data from multiple scenarios and testing it on an unseen one. The results are reported in Fig. 8 where the legend shows the name of the city used in the testing phase only and not included in the training set. If compared to Fig. 7, they show that all models benefit from being trained on diverse scenarios. For example, XceptAtt attains the best performance with a testing accuracy of 85% over unseen scenarios.

D. Using fast ranging feature alone

The analysis of the Ranging component is presented in this section. The test set of the Boston scenario is used. The main objective is to evaluate the robustness of this method to differentiate between the same or different UEs. Fig. 9 depicts Chebyshev's probability P_r computed with the RRC messages received over time for a single UE according to Eq. 4. In the test dataset, the red dots represent the injected DMRS from an attacker located at different distances. As described in Sec. IV-B, the P_r is computed over the rolling window of the latest K messages, with a higher P_r indicating that it is likely a different UE. The results show that out of six attacks, half results in low probability, indicating False Negative (FN). For instance, *an attacker could be at the same distance from the gNB, but at a different location*. Additionally, a few False Positive (FP) occur for the same UE with high P_r, which could occur in presence of *large multipath in the channel or high mobility*. This suggests that ranging alone is insufficient for the final decision. However, the results presented above show that they can highly enrich all other features (cf. Sec. IV-A) to attain a higher accuracy in the attack detection.

E. Offline Test Attacks

`Det-RAN` is tested by emulating a real attack scenario. Colosseum scenario is set up involving two legitimate UEs, one gNB and one attacker. During the experiment, the UE connects to the gNB, exchange 5 s of traffic, and goes in RRC Inactive state until a random time when it resumes the connection. The attacker, having procured the 5G-TMSIs of both UEs attempts to launch six attacks within the Inactive window time, for each of the victims. To emulate this behavior, the RRC messages of the attacker are injected into the test dataset and `Det-RAN` infers over all the received messages.



(a) UE 1 (b) UE 2

Fig. 10: The confusion matrices for two UEs demonstrates the ability of `Det-RAN` to detect the attacks.

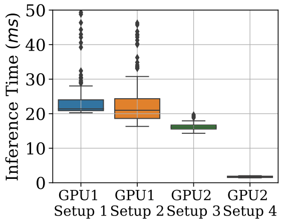


Fig. 11: Inference time for different setups. In Setup 4 `Det-RAN` meets the real-time requirements

In Fig. 10a and 10b, we report the confusion matrices for the two UEs. Despite some FP, the model demonstrates a high degree of precision in detecting the attacks. In this context, absence of FN ensures that the framework does not miss any attack. On the other hand, rejecting a few RRC requests from legitimate UEs may only require to establish a reconnection procedure involving the 5G-CN.

F. Inference time analysis on hardware

The key impact on performance stems from the AI component, where inference time is critical. The AI's model complexity may necessitate robust computational capabilities, typically provided by high power-consuming GPUs. For instance, network operators may need to scale the *Model Pool* to guarantee reliability and security. Hence, we analyze different deployment Setups ($S1, S2, S3, S4$) with two different GPUs and virtualization environments, summarized in Table II, to test the inference time and provide insight into deployment costs. Fig. 11 illustrates the inference time distribution for a single prediction, repeated 50 times over a 180s experiment. $S1$ and $S2$ do not yield satisfactory results: an inference time of 20 ms exceeds the Radio Frame target, rendering the system unable to respond timely enough to mitigate an attack. Despite switching to a more powerful GPU in $S3$, we only achieve a slightly improved inference time leading us to reconsider our deployment strategy to improve system performance. In $S4$, we utilize TensorRT, the SDK with its model optimization capabilities. This solution provides remarkable results: we achieve an inference time of 2 ms, reducing the latency factor of 8x and meeting the real-time Radio Frame requirements.

IX. Related Work

Despite the 3GPP 5G standard has significantly enhanced the protection of subscribers, vulnerability for these procedures remains. Existing work has shown that an attacker can map the 5G-TMSI with RNTI and impersonate the victim, triggering various attacks, e.g., DoS, Man-In-The-Middle (MitM), due to the absence of message integrity protection at the lower layers of the network protocol [2] [3]. The potential for UE identity spoofing is a significant concern, as the RNTI and 5G-TMSI can be matched during the connection establishment process and could be exploited to identify victims [3] [16].

IMSI-catching attacks have been a persistent concern since the early days of cellular networks. In literature there are plenty of studies about privacy related to tracking users, with a significant emphasis on exploiting the linkability of identifiers such as the IMSI, TMSI, SUPI [25]–[32]. For instance, [15] has demonstrated the feasibility of stealing the IMSI in 4G networks. Moreover, recent research [33] has unveiled a method to extract the SuPI in 5G networks.

TABLE II: Benchmark of Prototype on Different Machines

Setup	Virtualization	CPU	Mem (GB)	GPU Model	GPU (GB)
S1 GPU_1	No Virtualization	i5	32	RTX2080	2
S2 GPU_1	Docker+TfServing	i5	32	RTX2080	2
S3 GPU_2	Docker+TfServing	i7	1000	A100	4
S4 GPU_2	Docker+TensorRT	i7	1000	A100	4

Rupprecht et al. [34] and Chlosta et al. [35] have independently investigated and demonstrated the existence of potential Man-in-the-Middle (MitM) and impersonation attacks, respectively. Rupprecht et al. focused on exploiting implementation bugs in an LTE dongle, while Chlosta et al. explored vulnerabilities present in operational LTE networks. In separate studies, researchers [36]–[40] have examined various methods to launch Denial-of-Service (DoS) attacks targeting 3G and 4G subscribers. Specifically, Kim et al. [16] have unveiled novel DoS attacks that can be directed towards specific users or entire base stations, leveraging vulnerabilities inherent in 4G networks. The authors in [3] have conducted an extensive study on a distinct class of vulnerabilities present in the initial messages of the NAS and RRC layers within the 5G protocol stack, their work does not provide any explicit defenses against the investigated attacks, nor were their findings validated within the context of the complete 4G/5G protocol stack. In contrast, our research focuses on the same class of attacks and offers effective mitigation strategies to counter such threats. Finally, overshadowing technique, explored in cellular network vulnerability assessments [41]–[43], has evolved in recent simulated studies. Unlike simulation-based approaches, this work goes beyond reproducing attacks and introduces countermeasures for diverse implementation scenarios.

X. Conclusion

In this work, we have shown that Open RAN can be leveraged for designing novel AI solutions at the edge of the network that can swiftly detect the presence of attackers, significantly contributing to enhancing the security of 5G networks. Our proposed `Det-RAN` framework is designed to process cross-layer features and proactively detect the attacks generated with RRC messages, while achieving strict real-time constraints in 5G systems. We provide public access to code and data here: https://doi.org/10.5281/zenodo.10473882.

Acknowledgements

Work at IMDEA was supported by the project MAP-6G, ref. TSI-063000-2021-63, granted by the Ministry of Economic Affairs and Digital Transformation and the European Union-NextGenerationEU. This work was partially supported by the U.S. National Science Foundation Grants CNS-1925601, CNS-2112471, OAC-2201536, ECCS-2229472 and CNS-2312875, as well as by the Air Force Office of Scientific Research under contract FA9550-23-1-0261 and the Office of Naval Research under contract N00014-23-1-2221.

References

[1] "TS 38.323, NR; Packet Data Convergence Protocol (PDCP) specification," in *3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Release 17*, 2023.

[2] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1121–1136.

[3] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 669–684.

[4] "TS 38.331, nr; radio resource control (RRC); protocol specification," in *3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Release 17*, 2023.

[5] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[6] N. Seddigh, B. Nandy, R. Makkar, and J.-F. Beaumont, "Security advances and challenges in 4g wireless networks," in *2010 Eighth International Conference on Privacy, Security and Trust*. IEEE, 2010, pp. 62–71.

[7] Ericsson. (2022) 3gpp release 17 security and ran. [Online]. Available: https://www.ericsson.com/en/blog/2022/10/3gpp-release-17-security-ran?utm_medium=social_organic&utm_source=linkedin&utm_campaign=bnew_blog_accessnetw_20221031

[8] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," *IEEE Communications Surveys & Tutorials*, pp. 1–23, January 2023.

[9] xRAN Forum. (2018) xran forum merges with c-ran alliance to form oran alliance. [Online]. Available: https://www.businesswire.com/news/home/20180227005673/en/

[10] T. O.-R. Alliance. (2023) O-ran. [Online]. Available: https://www.o-ran.org/

[11] S. D'Oro, M. Polese, L. Bonati, H. Cheng, and T. Melodia, "dapps: Distributed applications for real-time inference and control in o-ran," *IEEE Communications Magazine*, vol. 60, no. 11, pp. 52–58, 2022.

[12] S. Bartoletti, L. Chiaraviglio, S. Fortes, T. E. Kennouche, G. Solmaz, G. Bernini, D. Giustiniano, J. Widmer, R. Barco, G. Siracusano, A. Conti, and N. B. Melazzi, "Location-based analytics in 5g and beyond," *IEEE Communications Magazine*, vol. 59, no. 7, 2021.

[13] M. Singh, M. Roeschlin, A. Ranganathan, and S. Capkun, "V-range: Enabling secure ranging in 5g wireless networks," in *NDSS 2022, San Diego, California, USA, April 24-28, 2022*. The Internet Society, 2022.

[14] O. Lasierra, G. Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez, "European 5g security in the wild: Reality versus expectations," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 13–18.

[15] I. Palamà, F. Gringoli, G. Bianchi, and N. Blefari-Melazzi, "Imsi catchers in the wild: A real world 4g/5g assessment," *Computer Networks*, vol. 194, p. 108137, 2021.

[16] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the lte control plane," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1153–1168.

[17] "TR 21.917, Technical Specification Group Services and System Aspects," in *3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Release 17*, 2023.

[18] "Positioning in 5g networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 38–44, 2021.

[19] W. Feller, *An introduction to probability theory and its applications, Volume 2*. John Wiley & Sons, 1991, vol. 81.

[20] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1251–1258.

[21] S. Woo, J. Park, J.-Y. Lee, and I. S. Kweon, "Cbam: Convolutional block attention module," in *Proceedings of the European conference on computer vision (ECCV)*, 2018, pp. 3–19.

[22] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. Alemi, "Inception-v4, inception-resnet and the impact of residual connections on learning," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 31, no. 1, 2017.

[23] L. Bonati, P. Johari, M. Polese, S. D'Oro, S. Mohanti, M. Tehrani-Moayyed, D. Villa, S. Shrivastava, C. Tassie, K. Yoder *et al.*, "Colosseum: Large-scale wireless experimentation through hardware-in-the-loop network emulation," in *2021 DySPAN*. IEEE, 2021, pp. 105–113.

[24] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srslte: An open-source platform for lte evolution and experimentation," in *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, 2016, pp. 25–32.

[25] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New privacy issues in mobile telephony: fix and verification," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 205–216.

[26] T. Fei and W. Wang, "Lte is vulnerable: Implementing identity spoofing and denial-of-service attacks in lte networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[27] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, "5g suci-catchers: Still catching them all?" in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 359–364.

[28] D. Abodunrin, Y. Miche, and S. Holtmanns, "Some dangers from 2g networks legacy support and a possible mitigation," in *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2015, pp. 585–593.

[29] R. Borgaonkar and S. Udar, "Understanding imsi privacy," in *Vortrag auf der Konferenz Black Hat*, 2014.

[30] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "Imsi-catch me if you can: Imsi-catcher-catchers," in *Proceedings of the 30th annual computer security applications Conference*, 2014, pp. 246–255.

[31] M. S. A. Khan and C. J. Mitchell, "Trashing imsi catchers in mobile networks," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 207–218.

[32] R. Borgaonkar, A. Martin, S. Park, A. Shaik, and J.-P. Seifert, "White-stingray: Evaluating imsi catchers detection applications," in *Proceedings of the 11th USENIX Conference on Offensive Technologies*, ser. WOOT'17. USA: USENIX Association, 2017, p. 21.

[33] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4g and 5g cellular paging protocols using side channel information," *Network and Distributed Systems Security (NDSS) Symposium2019*, 2019.

[34] D. Rupprecht, K. Jansen, and C. Pöpper, "Putting {LTE} security functions to the test: A framework to evaluate implementation correctness," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.

[35] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "Lte security disabled: misconfiguration in commercial networks," in *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*, 2019, pp. 261–266.

[36] B. Michau and C. Devine, "How to not break LTE crypto," in *ANSSI Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, 2016.

[37] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *2013 16th international symposium on wireless personal multimedia communications (WPMC)*. IEEE, 2013, pp. 1–9.

[38] M. T. Raza, F. M. Anwar, and S. Lu, "Exposing LTE security weaknesses at protocol inter-layer, and inter-radio interactions," in *Security and Privacy in Communication Networks: 13th International Conference, SecureComm 2017, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13*. Springer, 2018, pp. 312–338.

[39] S. Park, A. Shaik, R. Borgaonkar, and J.-P. Seifert, "Anatomy of commercial imsi catchers and detectors," in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, 2019, pp. 74–86.

[40] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.

[41] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on {LTE}," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 55–72.

[42] N. Ludant and G. Noubir, "Sigunder: a stealthy 5G low power attack and defenses," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 250–260.

[43] S. Erni, M. Kotuliak, P. Leu, M. Roeschlin, and S. Capkun, "Adaptover: adaptive overshadowing attacks in cellular networks," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 2022, pp. 743–755.