Secure and resilient 6 G RAN networks: a decentralized approach with zero trust architecture

Hichem Sedjelmaci, Nesrine Kaaniche, Kamel Tourki

Secure and Resilient 6G RAN Networks: A Decentralized Approach with Zero Trust Architecture

Hichem Sdjelmaci
Ericsson R&D Security,
Massy,91300, France
hichem.sedjelmaci@ericsson.com

Nesrine Kaaniche
Samovar, Télécom SudParis,
Institut Polytechnique de Paris,
91120 Palaiseau, France
kaaniche.nesrine@telecom-sudparis.eu

Kamel Tourki
Ericsson S&T France,
Massy,91300, France
kamel.tourki@ericsson.com

***Abstract*—The upcoming sixth generation (6G) networks present significant security challenges due to the growing demand for virtualization, as indicated by their key performance indicators (KPIs). To ensure communication secrecy in such a distributed network, we propose an intelligent zero trust (ZT) framework that safeguards the radio access network (RAN) from potential threats. Our proposed ZT model is specifically designed to cater to the distributed nature of 6G networks. It accommodates secrecy modules in various nodes, such as the base station, core network, and cloud, to monitor the network while performing hierarchical and distributed threat detection. This approach enables the distributed modules to work together to efficiently identify and respond to the suspected RAN threats. As a RAN security use case, we address the intrusion detection issues of the 6G-enabled internet of drones. Our simulation results show the robustness of our ZT framework, which is based on distributed security modules, against potential attacks. The framework exhibits low detection time and low false positives, making it a reliable solution for securing 6G networks. Furthermore, the ZT model enables the accommodation of secrecy modules in various nodes and provides the needed enhanced security measures in the network.**

I. Introduction

As the fifth generation (5G) standardization getting matured, Release 19 shed lights on the the sixth generation (6G) design that enables the interoperability in hybrid systems. To improve the load balancing and provide the necessary resources, the 6G radio access network (RAN) should handle the heavy computation load on behalf of the devices with reduced capabilities, such as the internet of things (IoT) devices, to drastically reduce the communication latency.

As shown in Fig. 1, the flexibility granted to 6G RAN allows for a better computation load distribution, enabling extra resources to the devices, automotive and drones, to handle the needed quality of experience. Furthermore, lightening the computational load of the devices will allow for more data collection and faster communications with RAN. The later is being prepared to support new and emerging technologies, such as virtual and augmented reality, which require large bandwidth and reduced latency.

The development of 6G networks is also expected to bring significant improvements in terms of energy efficiency and sustainability. This is particularly important given the rapid growth of IoT devices and their associated energy consumption. The ability of 6G RAN to handle heavy computational loads will reduce the overall energy consumption of IoT devices, making them more sustainable and cost-effective in the long term. Furthermore, the new 6G requirements enabling for the interoperability of hybrid systems and supporting emerging technologies while improving the energy efficiency and sustainability open the doors for a promising area of research and development [1]. Moreover, the virtualization concept is ever inspiring, leading to new challenges on security. Threats such as jamming, false base station (BS) attacks, and denial of service attacks can pose a serious risk to RAN operations [2]. To address these threats, the security community has turned to Zero Trust Architecture (ZTA) as a cyber security solution that can accurately protect networks from known and unknown attacks, whether they originate from inside or outside the network.

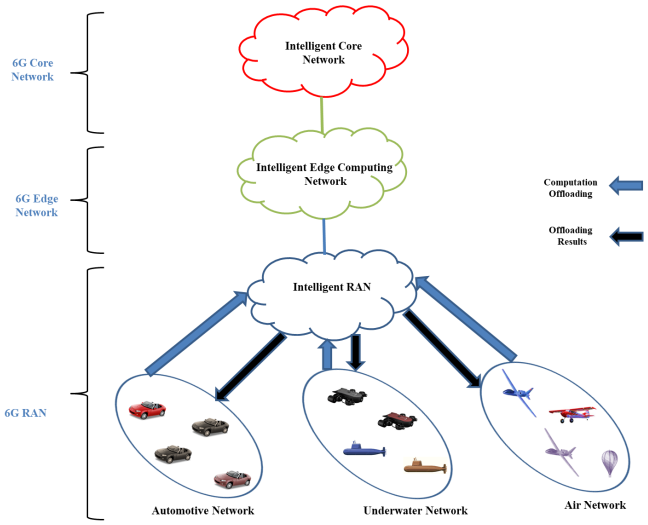

Fig. 1. 6G RAN-enabled computation offloading

The National Institute of Standards and Technology (NIST) has identified several key processes for securing critical infrastructure from cyber and network attacks. These processes include authentication, authorization, monitoring, and detection mechanisms, which are essential for ensuring the security and reliability of RANs to mitigate the security threats [3].

Implementing ZTA can provide several benefits for RAN security [4]. First, it can help to prevent unauthorized access to the network by requiring all users and devices to be authenticated before being granted access. Second, it can improve visibility into network activity, allowing for more effective monitoring and detection of potential threats. Third, it can enable more fine-grained access control, ensuring that each user or device is limited to the needed resources for their specific tasks.

Besides ZTA, there are other measures that can be taken to improve RAN security. These include encryption, regular security audits, and employee training to raise awareness about security best practices. By adopting a comprehensive approach to RAN security that includes both technological and human awareness, organizations can better protect themselves against cyber and network attacks. Thus, as virtualization continues to grow in popularity in 5G and beyond, it is becoming increasingly important to prioritize RAN security. ZTA, along with other security measures, can help to ensure that networks remain secure and reliable.

Contributions – This paper aims to address the attack detection and decision-making issues in 6G by proposing a robust zero trust framework. Our proposed framework complies with distributed architectures and applies a set of security modules at different nodes, including BS, core networks and cloud nodes, to ensure efficient secrecy RAN communication while considering internal and external threats. However, as the proposed framework is designed for hybrid inter-operable systems with multiple devices, comprising operating systems, network functions and security modules, it faces significant challenges.

To assess the performance of our proposed framework, we analyze the required attack detection time, false positive and decision-making metrics. Our simulation results show a significant decrease in false positive rates, while reducing the needed detection time to accurately overcome cyber threats. Specifically, the detection time required by our proposed framework does not exceed 15 seconds, which is a significant improvement over existing solutions. Moreover, we compare the performance of our framework with the state-of the art security frameworks, and showed that our proposed framework outperforms the existing works in terms of decision-making rate.

Paper Organisation – This paper is organised as follows. Section II presents the related work. Sections III and IV introduce the proposed framework and detail the main procedures at different levels. Section V discusses the Internet of Drones (IoD) use case along with its performance assessment. Finally, we draw conclusions in Section VI.

II. Related Work

In this section, we provide an overview of the related works that have investigated or proposed ZTA. Recent works proposed zero trust frameworks for specific networks such as cloud computing, wireless sensor networks, and IoT. The authors in [5] proposed a zero trust security model for IoT that involves the use of multi-factor authentication, network segmentation, and traffic monitoring to prevent unauthorized access and data breaches. Moreover, more recent works have focused on the effectiveness of zero trust models in different contexts. The authors in [4] analyzed the zero trust approach for securing enterprise networks and showed that it can significantly improve security by enforcing strict access control policies. Moreover, the authors in [6] focused on heterogeneous networks in a multiuser context. To improve the security of the considered architecture, the authors proposed the use of ZTA to assist the mobility management. The simulation results showed that an improved version of ZTA, incorporating a dynamic trust model and a decentralized authentication process, can better mitigates the security risks (internal and external threats, including denial of service (DoS) and zero-day attacks) in such a distributed system. However, the authors did not considered external attacks from malicious wireless devices, which could seriously compromise the system trustworthiness. Therefore, further investigations are still needed to evaluate the effectiveness of the proposed ZTA scheme against such external attacks. In [7], Sedjelmaci et al. proposed a collaborative ZTA to secure the 6G edge computing from intruders targeting the IoT devices and edge servers. The proposed ZTA is based on a set of security agents activated at IoT and edge levels to monitor the network with a goal to detect the malicious device and malicious server. The attack detection techniques used by the security agents are using collaborative machine learning algorithms such as federated learning and reinforcement learning algorithms. To further increase the detection accuracy, specifically against the complex attacks such zero-day attacks, the authors develop a dynamic ZTA adapted to the 6G architecture. The dynamic ZTA based on a non-cooperative game concept switches from local detection to collaborative detection, and vice versa, to react efficiently against the suspected attacks. According to the simulation results, the proposed collaborative and dynamic ZTA approach exhibits a high accuracy detection while requiring low computation cost to achieve a high level of network security. However, more security components should be deployed within the 6G RAN to secure the network against attacks targeting the radio access, such as false BS attack.

Moreover, the authors in [8] included different AI-based techniques into their proposed 6G architecture to further enhance the security provided by their zero-trust system. By using unsupervised learning algorithms, the authors employed the k-nearest neighbors method to effectively detect any anomaly or attack that may occur within the system. The zero-trust framework implemented in the study aimed to accurately evaluate the trust level of the monitored target, thus ensuring that any potential threat would be timely detected and efficiently processed. However, the authors in [9] considered a different context and proposed hierarchical and cooperative attack detection framework to safeguard the 6G-enabled IoT from internal and external network attacks. The proposed framework relies on a federated learning algorithm, which

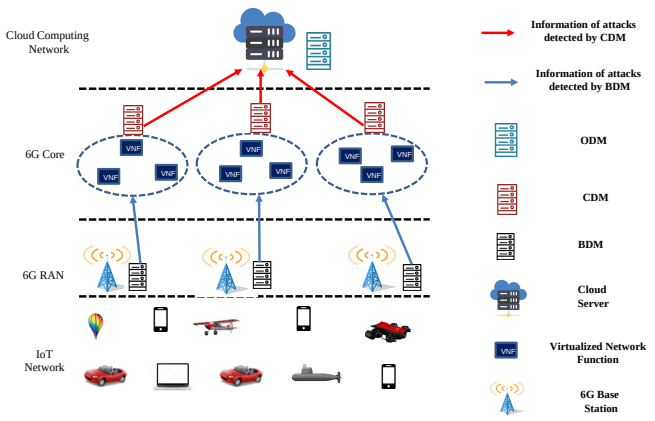

Fig. 2. Secure and resilient zero trust framework for 6G RAN.

considers 6G primary metrics, such as energy consumption, latency, end-to-end connectivity, and network latency. The simulation results showed high accuracy in attack detection under low computation overhead. Overall, both [8] and [9] did to consider the fooling actions that malicious security and monitoring agents could perform. This oversight leaves the system vulnerable to severe security breaches.

Table I showed that literature already investigated several promising zero trust architectures for different networks. However, some drawback still exist to be addressed to increase the 6G network trustworthiness. For example, more security components should be deployed within the 6G RAN to secure the network from attacks targeting the radio access. Moreover, the fooling actions, that malicious security and monitoring agents could perform, should be considered to prevent severe security breaches.

III. Cyber Defense for 6G Network

In this section, we present the 6G network architecture that we need to protect from the cyber-threats and intruders along with the cyber-attack model that is targeting the 6G infrastructure. Subsequently, we introduce the main cyber-defense modules, that constitute our ZTA, performing the defense monitoring and attack detection.

A. Network Architecture

A depicted in Fig. 2, we present a 6G network that consists of four layers: IoT, 6G RAN, 6G core network, and the cloud network. The IoT connects a huge number of devices, sensors, and machines such as smart thermostats, security cameras, and wearable devices. The 6G RAN, including small cells and advanced antenna technologies such as massive MIMO (mMIMO), provides wireless access to the 6G users (e.g smartphones, laptops, and tablets) [11].

The 6G core network is managing the network resources, services, and security using advanced technologies such as network slicing and artificial intelligence. Finally, the cloud network serves as a centralized control and management platform for the entire 6G network, enabling operators to monitor, optimize, and orchestrate the network performance and services using tools such as network management systems and orchestration platforms.

B. Attacker Model

In a 6G network, an attacker could potentially target any layer of the network, from the IoT devices to the cloud network.

For the IoT layer, an attacker is able to compromise devices such as smart thermostats or security cameras, which may have vulnerabilities that could be exploited to get access to the network [12]. Once inside the network, the attacker could launch various attacks, such as distributed denial of service (DDoS) attacks, which could overwhelm the network capacity and make it unavailable to legitimate users. At the 6G RAN layer, an attacker is able to target wireless communications by intercepting, modifying, or blocking data transmissions between devices and the network. For example, an attacker could use rogue base stations or jamming devices to disrupt communications or steal sensitive data.

The 6G core network layer is managing the network resources, services, and security. An attacker targets this layer by exploiting vulnerabilities in the network infrastructure, such as routers or servers, or by compromising the software used to manage the network services. This could allow the attacker to gain unauthorized access to sensitive data or to manipulate network resources for their own purposes.

Finally, the cloud network serves as a centralized control and management platform for the entire 6G network. An attacker targets this layer by compromising the cloud infrastructure or exploiting vulnerabilities in the software used to manage the network. This could allow the attacker to gain access to sensitive information or to manipulate the network performance and services.

We aligned our view with Dolev and Yao model [13] and we distinguish two main adversaries, where each of them may target any layer of the network to get unauthorized access, disrupt communications, steal sensitive information, or manipulate the network resources. The attacker is then able to Read, Drop and Send valid messages. A Read activity alludes to getting or capturing messages. In the mean time, a Send activity alludes to producing and replaying messages. A Drop activity alludes to separating.

Below, we detail the considered attackers:

- *External adversaries* — malicious actors may attempt to compromise the main security properties of a 6G network, such as data confidentiality, integrity, and network service availability [14]. In addition, they may attempt to degrade the 6G network key performance indicators (KPIs) by increasing latency, exhausting network resources, generating overhead, or altering signal strength intensities, among other methods. These attacks could take various forms, such as DoS, man-in-the-middle attacks, black hole attacks, eavesdropping, and poisoning. The attacks could target various components of the 6G network, including

TABLE I
COMPARISON OF RECENT RELATED WORKS ON ZERO TRUST ARCHITECTURES

Solution	Network Type	Security Features	Weaknesses
Mehraj et al. [4], [5], [10]	IoT networks	Multi-factor authentication, Network segmentation, Traffic monitoring	Not specifically designed for 6G networks.
Chen et al. [6]	Heterogeneous networks	ZTA on top of the management layer, DoS and zero-day attack mitigation,	Does not consider external attacks from malicious wireless devices.
Sedjelmaci et al. [7]	6G edge computing	Collaborative and dynamic ZTA , High accuracy detection, Low computation cost	Does not consider attacks targeting the radio access.
Bao et al. [8]	6G architecture	K-nearest detection method, Accurate trust level evaluation	Does not consider the fooling actions of malicious agents.
Sedjelmaci et al. [9]	6G-enabled IoT	Hierarchical framework, High accuracy detection, Low computation overhead	Does not consider the fooling actions of malicious agents.

virtualization functions, network configuration modules, and artificial intelligence algorithms for quality of service (QoS) management. Protecting against such attacks will be critical for ensuring the security and performance of 6G networks.

- *Internal adversaries* — these include malicious network equipment and edge servers. Once infected, these devices can target network and machine learning (ML) configurations [15]. Additionally, they may engage in misbehavior such as dropping neighbor's packets and injecting malicious messages into the network. Defending against these internal adversaries is critical for maintaining the integrity and security of the whole network.

Both internal and external adversaries, may implement known or unknown attack methods. Known attacks involve previously identified security threats that are recognized within the security community and can be detected by their attack signatures. These attacks can take various forms, including traditional attack vectors such as malware, phishing, DoS attacks, and ransomware. In contrast, unknown attacks, also known as zero-day exploit attacks, are novel or previously unreported attacks that are more difficult to defend against since there is no existing knowledge of them. Protecting against unknown attacks requires proactive measures for identifying and responding to security incidents. By incorporating both known and unknown attack types into the security model, we can establish a comprehensive approach to securing the network against potential threats.

C. Proposed ZTA: Defense Monitoring and Attack Detection

The proposed ZTA framework aligns with the NIST guidelines [3], which recommend incorporating features such as trust evaluation, target monitoring and attack detection, data integrity, and protection against both internal and external attacks. Our proposal consists of three distinct cyber defense modules, depicted in Fig. 2. These modules are responsible for ensuring comprehensive security monitoring at various points in the 6G RAN architecture. The first module, called the BS Defense Module (BDM), monitors security at the base station. The second module, referred to as the Core Defense Module (CDM), focuses on security in the core network. Finally, the Cloud Defense Module (ODM) monitors security at the cloud server. By collaborating effectively, these defense modules can accurately detect internal and external attacks targeting the 6G RAN. Furthermore, these modules can also identify and prevent suspicious activities that originate from BS or within the core network to identify the malicious BDM and CDM. In the following, we will provide more details on each of these defense modules.

- ***BDM***. This proposed defense module, acts as a monitoring agent responsible for supervising the behaviors of target IoT devices that fall within the radio communication range of the BS. These devices include drones, underwater vehicles, and sensors. Given the large amounts of data processed within the 6G RAN network, the sensor-enabled nodes and devices are vulnerable and require continuous monitoring [16]. Therefore, the BDM plays a critical role in ensuring the security and trustworthiness of the network by detecting any suspicious activities or behavior that could potentially compromise the system integrity. In a nutshell, the BDM serves as the first line of defense against internal attacks .
  It is important to note that the signal intensity distribution can be a significant feature to identify distributed jamming attacks [17], and false BS. This is because jamming attacks and false BS aim to disrupt the wireless communication by broadcasting a high-intensity signal, leading to the reduction of the signal quality at the receiver side. By monitoring the signal intensity, the BDM can identify if a distributed jamming attack and/or false BS are occurring, and take appropriate measures to prevent it.
- ***CDM***. This second defense module is responsible for detecting and mitigating various types of attacks on the network. For this purpose, CDM operates a multi-class-based attack detection module that takes as input the attack features delivered by the BDM. These attack features are generated by the malicious IoT device. To ensure a more robust filtering process, CDM employs a Reinforcement Learning (RL) algorithm [18] that continuously learns from the network data and improves the accuracy of the new attack detection mechanism, even for zero-day attacks. This is especially important in a dynamic network such as an Internet of Drones where new types of attacks can emerge frequently. Moreover, CDM verifies whether the attack features delivered by the BDM correspond to a network attack or not. The module monitors the trustworthiness of the BS where BDM is activated. The objective is to ensure that the BDM is not compromised, and the attack features are genuine. This is crucial as a false alarm could result in the disruption of legitimate network activities.
- ***ODM***. This third defense module collects information from both the CDM list of detected malicious IoT devices and the BDM list of malicious devices and blacklisted BDMs. The ODM module employs a collaborative RL algorithm that enhances the robustness and efficiency of making final decisions regarding the detected attacks in the RAN,

building upon the processing of both BDMs and CDMs. The final decision-making process determines whether the suspicious IoT devices exhibit malicious behavior or whether the monitoring BDM and/or CDM should be categorized as malicious agents.

IV. An Adaptive ZTA to Harden the Security of 6G RAN

This section details the main security functions of the proposed adaptive trust architecture enforced at each layer. The adaptive trust monitors the network, targets to detect misbehavior executed by the attacker, and proactively acts before they execute an attack, i.e., zero-day attack. With an adaptive trust architecture, the proposed ZTA is continuously evaluating the vulnerabilities, detecting and reacting automatically using AI against the suspected malicious behaviors.

A. Collaborative AI Techniques for ZTA

As highlighted in subsection III-C, the cyber defense systems, BDM, CDM and ODM running within the ZTA, rely on collaborative AI techniques that use RL algorithms to secure the 6G RAN against the cyber threats.

1) BDM's AI Detection: Rules-based Game Approach: In the following, we outline the BDM-based process of our proposed ZTA framework. To identify both known and unknown attack features, the BDM adopts a rules-based non-cooperative game approach that models two competitor players: security and attack players. Each player aims to maximize its own utility function while minimizing the utility function of the other player [19]. By adopting this approach, the BDM can effectively detect potential attacks and accurately assesses the trustworthiness of the IoT devices within its radio communication range. Additionally, this approach allows the BDM to differentiate between intentional attacks and unintentional anomalies, which can further improve the overall security of the 6G RAN.

The game involves two players: the security player X_i, representing the BDM, and the attack player Y_j, representing the suspected IoT device. The sets of players are denoted as $X_i|i = 1, ..., n$ and $Y_j|j = 1, ..., m$, where n is the number of BDMs in the 6G RAN and m is the number of suspected IoT devices connected to the BS. We assume that all X_i players are activated. The strategies of the security and attack players are represented by the sets $\gamma^1_{\text{Security}} = \gamma^1_1, ..., \gamma^1_L$ and $\gamma^2_{\text{Attack}} = \gamma^2_1, ..., \gamma^2_F$, respectively. Here, F is the number of attacks executed by the malicious IoT device Y_j, while L is the number of attacks detected by the BDM X_i. Suppose we have a security game involving a security player X_i and an attack player Y_j. Let ϕ^1_i be the probability that X_i detects the known attack features, and ϕ^2_i be the probability that X_i detects the unknown attack features. The probability that X_i provides a false detection of the attack features is represented by the complement of ϕ_i, which is $(1 - \phi_i)$.

Similarly, let ω^1_j be the probability that Y_j launches a known attack, and ω^2_j be the probability that Y_j launches a new attack. A known attack is detected using the known attack features, while a new attack is detected using the unknown attack features. Thus, the complement of ω_j is the probability that Y_j did not launch an attack, which is $(1 - \omega_j)$.

The expected utility functions of X_i and Y_j depend on the probabilities $\phi^1_i, \phi^2_i, \omega^1_j, \omega^2_j, (1 - \phi_i)$ and $(1 - \omega_j)$, as defined by Eqs. 1 and 2, where $\phi^1_i, \phi^2_i, \omega^1_j, \omega^2_j, \phi_i$ and ω_j are all in the range $[0, 1]$. Note that the expected utility functions of both players depend on the probabilities of the other player, which creates a non-cooperative environment for the game, given by

$$U_{\text{Security}}(\gamma^1_{\text{Security}}, \gamma^2_{\text{Attack}}) = \omega^1_j \phi' + \omega^2_j \phi'' + (1 - \omega_j), \quad (1)$$

$$U_{\text{Attack}}(\gamma^2_{\text{Attack}}, \gamma^1_{\text{Security}}) = \phi^1_i \omega' + \phi^2_i \omega'' + (1 - \phi_i), \quad (2)$$

where $\phi' = \frac{\phi^1_i}{\phi^1_i + \omega^1_j}$, $\phi'' = \frac{\phi^2_i}{\phi^2_i + \omega^2_j}$, $\omega' = \frac{\omega^1_j}{\phi^1_i + \omega^1_j}$, and $\omega'' = \frac{\omega^2_j}{\phi^2_i + \omega^2_j}$.

In this non-cooperative game, the objective of each BDM is to identify the relevant attack features carried out by the malicious IoT devices and subsequently forward them to CDM for further detection. On the other hand, each malicious IoT device aims to launch an attack against the RAN while deceiving the BDM. The Nash equilibrium corresponds to the max-min functions given by Eqs. 3 and 4 as follows:

$$U^*_{\text{Security}}(\gamma^{1*}_{\text{Security}}, \gamma^{2*}_{\text{Attack}}) = \max_{\phi^1_i, \phi^2_i} \min_{(1-\omega_j)} U_{\text{Security}}(\gamma^1_{\text{Security}}, \gamma^2_{\text{Attack}}) \quad (3)$$

$$U^*_{\text{Attack}}(\gamma^{2*}_{\text{Attack}}, \gamma^{1*}_{\text{Security}}) = \max_{\omega^1_j, \omega^2_j} \min_{(1-\phi_i)} U_{\text{Attack}}(\gamma^2_{\text{Attack}}, \gamma^1_{\text{Security}}) \quad (4)$$

The functions U^*_{Security} and U^*_{Attack} represent the expected utility functions of the BDM and the malicious IoT device, respectively in the Nash equilibrium state.

After reaching an equilibrium, we can observe that the payoff for the attack player, Y_j, is the same whether they launch an attack using strategy γ^2_{Attack} or a different strategy $\gamma^{2*}_{\text{Attack}}$. Similarly, the payoff for the security player, X_i, is the same whether they activate strategy $\gamma^1_{\text{Security}}$ or a different strategy $\gamma^{1*}_{\text{Security}}$ and categorize Y_j as a malicious IoT device. As a result, X_i sends a list of attack features used by Y_j to the CDM for further detection and analysis. In the following section, we describe the processing carried out by the CDM.

2) CDM's AI Detection: RL Approach: The CDM utilizes BDM delivery provided by attack features made by Y_j as its input. As highlighted in subsection III-C to enhance the filtering process and improve the accuracy of detection, CDM employs a RL algorithm. Additionally, the CDM module verifies whether the delivered attack features correspond to a network attack or not, and monitors the trustworthiness of the BS where BDM is activated.

At the beginning of training process, the security experts interact with the RL algorithm by providing a relevant information related to new attack behaviors with goal to allow the machine learning algorithm to classify the new incoming data as normal or malicious. The RL algorithm relies on three security parameters: states, actions, and a payoff function. The RL states corresponds to attack features used by RL algorithm to model the normal and malicious behaviors during the training process and classify the suspected device as normal device or an intruder. The RL actions is the decisions initiated by CDM about the behaviors of BS and the monitored IoT device, such as detecting the BDM (activated at the BS) as malicious agent that provides false verdict against the monitoring target, and identifying an IoT device launching a cyber attack. The CDM computes an RL payoff, ψ_i' for each monitored BDM and associated BS, where the payoff functions depends on the following security parameters, θ^C, θ^F and θ^T as showed in in Eq.5. θ^C and θ^F are the correct and false identification rates, respectively and θ^T is the attack identification cost. Here, $i' = 1, \ldots, n'$, where n' is the total number of activated BDMs to monitor the RAN segment.

$$\psi_i' = \alpha_1 \theta^C - (\alpha_2 \theta^F + \alpha_3 \theta^T) \tag{5}$$

where $\theta^C \in [0, 1]$ is computed as the number of attacks correctly identified by the monitoring CDM (by using as inputs the attacks features provided by $BDM_{i'}$) over the number of BDMs, attached to the CDM. The coefficients α_1, α_2, and $\alpha_3 \in [0, 1]$ weight these parameters differently. Specifically, α_1 emphasizes the importance of correct identification, while α_2 and α_3 penalize false identification and identification costs, respectively. The values of these coefficients may vary depending on the specific context of the attack identification task. Similarly, $\theta^F \in [0, 1]$ is computed as the number of false detection (i.e., false positive and false detection) provided by $BDM_{i'}$ against the legitimate target and identified by CDM over the number of deployed BDMs. We define $\theta^T \in [0, 1]$ as the average time required by $BDM_{i'}$ to compute and collect the relevant features of monitored attacks occurring within the RAN segment. Notably, θ^T approaches 1 when a high computation time is needed to determine the relevant attack features. Conversely, θ^T approaches 0 when a low computation time is needed.

CDM monitors the payoff function ψ_i' for each monitored $BDM_{i'}$ over time and makes the first decision regarding the trustworthiness of $BDM_{i'}$ at the end of each iteration. Specifically, if $BDM_{i'}$ has a false identification rate θ^F that is much higher than its correct identification rate θ^C, as determined by the inequality $\alpha_2 \theta^F \gg \alpha_1 \theta^C$, then $BDM_{i'}$ is categorized as an untrusted defense system; otherwise, it is categorized as a trusted defense system.

Once the trusted defense system $BDMs$ have been determined, the RL algorithm transitions to an unsupervised training process (i.e., without the intervention of security experts), using the relevant attack features provided from these trusted sources as input. CDM computes the total payoff function as the average of the ψ_i' values for all K iterations, denoted as $(\sum_{g=1}^{K} \psi_i' g)/K$, and makes the final decision regarding the monitored $BDMi'$. If the false detection rate of the selected $BDMs$ is much higher than their correct detection rate, as determined by the inequality $(\alpha_2 \sum_{g=1}^{K} \theta_g^F)/K \gg (\alpha_1 \sum_{g=1}^{K} \theta_g^C)/K$, then CDM blacklists $BDM_{i'}$, preventing it from participating in the attack detection process.

3) ODM AI Detection: Hybrid Learning Approach: The collaborative RL executed by ODM is based on a hybrid RL processing, which involves a combination of a local RL process and a multi-agent RL process, which will be further elaborated hereafter.

*a) **Local RL process —**:* The local RL algorithm is trained in a supervised manner, with input provided by the operator or security expert in the central cloud computing who periodically feeds the algorithm with relevant features related to the new attack behavior. The primary aim is to accurately detect new types of attacks, including zero-day attacks that exhibit an unknown malicious behaviors. To this end, the ODM performs further detection against the suspected IoT devices detected by BDM and CDM as malicious devices. In this local RL approach, ODM evaluates the trustworthiness of monitoring CDM. Furthermore, only trusted CDMs, which have shown a high level of accuracy in detecting attacks, are allowed to be one of the defense agent that cooperate in the multi-agent RL process. The ODM calculates a reputation score for each CDM, based on $\beta_1 \mu^C - \beta_2 \mu^F$, where β_1 and β_2 are weight parameters that fall within the range [0,1]. The reputation score is based on the fraction of correctly detected attacks by the CDM that are confirmed by the ODM over the number of interactions between CDM and ODM (μ^C), as well as the fraction of false positives generated by the CDM that are detected by the ODM over the number of interactions between those defense modules (μ^F). If the product of β_1 and μ^C is significantly greater than the product of β_2 and μ^F, the monitored CDM is classified as a trusted defense agent. Otherwise, it is deemed to be an untrusted defense agent.

*b) **Multi-agent RL process —**:* The trusted CDMs feed ODM with features related to detected attacks (defined as RL's states), the decision-making processes employed by CDMs to handle malicious BSs and IoT devices (defined as RL's actions) and the results of a number of an accurate detection provided by the BDM against the monitored devices (defined as RL's payoffs). During the training process, the ODM uses as an inputs these information to build a global training model by aggregating the RL's states related to each malicious IoT devices, while taking into account the RL's payoffs associated with each BDM that identifies cyber attack occurred within the RAN. During the attack detection process, the ODM selects the CDMs that provide the same detection as ODM, i.e., ODM confirms the attacks executed by the monitored targets identified by CDMs. Furthermore, ODM requests the CDMs that persist on providing false detection to switch from multi-agent RL process to local RL process. To reduce further the false positive and false negative that could be generated by the ODM, the

cyber security experts update the global training model of ODM with new attack features.

B. Collaborative cyber resilience based on GAN approach

The Trustworthy defense systems, BDMs and CDMs that ODM selects as described in subsection IV-A3, will collaborate together during the cyber-resilience process to secure the 6G RAN against new incoming threats. The cyber resilience layer aims to further enhance the security of the whole system and prevent the critical attacks to reach the RAN components. The trusted BDMs and CDMs with ODM run a hierarchical GAN algorithm [20] to further enhance the cyber security of the proposed adaptive ZTA. The proposed GAN algorithms are based on a two-tiered security system, with two security components, a generator and a discriminator. The first security component, the generator, provides suspected inputs to the discriminator. The second security component, the discriminator, categorizes this latter as normal, attack, or anomaly. In the first GAN algorithm, the BDMs play the role of the generator, while the CDMs play the role of the discriminator. In the second GAN algorithm, the CDMs play the role of the generator, while the ODMs play the role of the discriminator.

The process of training and classification performed by the generators and discriminators is highlighted in Algorithm 1 and detailed as follows:

- The generator is responsible for generating synthetic data that resembles the real data. This data is then provided to the discriminator for classification.
- The discriminator is responsible for classifying the data as real or synthetic. If the discriminator is able to correctly classify the data, then the generator is updated to generate more realistic data.

This process is repeated until the generator is able to generate data that is indistinguishable from real data. The discriminator is then used to classify the suspected inputs as normal, attack, or anomaly. The two-tiered security system provides a number of advantages over traditional security systems. First, it is more robust to adversarial attacks. Adversarial attacks are designed to fool the discriminator into classifying synthetic data as real data. However, the two-tiered security system is able to detect and mitigate these attacks efficiently. While the traditional security systems require a large amount of data to train the discriminator, the two-tiered security system only requires a small amount of data to train the generator. This is due to the generator that was able to learn the distribution of the real data from the CDMs. Furthermore, the two-tiered security system is more scalable while the traditional security systems can be difficult to scale to large datasets. However, the proposed system is able to scale to large datasets by training multiple generators and discriminators in parallel.

During the training process, in the first GAN algorithm, a CDM's discriminator uses as input the attack features (related to the malicious IoT devices, Y_j) detected by BDMs and confirmed by CDM. Specifically, the CDM's discriminator, which is based on a RL algorithm, considers those attack features as the main state to increase its utility function. Furthermore, each BDM sends to the attached CDM its rule weight $\mathcal{W}_k$, $k \in 1, ..., L$, where L is the total number of trustworthy BDMs that activate their generators. Afterwards, the CDM's discriminator aggregates all the rules weights which is computed as $\frac{\sum_{k=1}^{L}(W_k)}{K}$ and CDM sends back the aggregation results to the BDMs' generators. Similarly as the first algorithm, in the second GAN algorithm the CDMs' generators and ODM's discriminator collaborate between each other on sharing the learning parameters and enhance the global training model. $\mathcal{W'}_{k'}$ represents the training parameter of RL algorithm executed by CDM generator k', $k' \in 1, ..., L'$, where L' is the total number of CDM generators. ODM discriminator aggregates the training parameters send by CDM and send the aggregation results which is equal to $\frac{\sum_{k'=1}^{L'}(W'_{k'})}{K'}$ to the distributed CDMs' generators.

During the classification process, the discriminators' components activated at CDM and ODM levels collaborate with the security experts to refine the classification (i.e., decrease the false positive), and they categorize the new attacks detected by the generators' components as an attacks, normal or anomaly, based on training models and parameters obtained during the training process, $\mathcal{W}_k$ and $\mathcal{W'}_{k'}$. Furthermore, in case when the suspected attacks are detected as an anomaly or normal node by the discriminators, these latter request the generators, that provide the false detection, to update their training process considering the new attacks' features provided by the security experts.

V. Use Case Study: Internet of Drones

This section, we first define the considered use case under study. Then, we discuss the different conducted experiments' results.

A. Use Case: Internet of Drones

The development of 6G-based Internet of Drones (IoD) networks is expected to revolutionize various industries by enabling fast, reliable, and autonomous drone-based services [21]. However, the dynamic characteristics of the IoD network, such as the dynamic topology, mobility, and heterogeneity of devices, pose significant security challenges that require novel security modules to address. In an IoD network, security is a crucial factor in ensuring the reliable and safe operation of drones. As drones are expected to perform various critical tasks, such as surveillance, inspection, and delivery, any security breach could result in significant consequences, such as data leakage, loss of control, or physical harm. Furthermore, the IoD network KPIs, such as latency, reliability, and throughput, are closely dependent of the employed security measures. For instance, encryption and authentication protocols can significantly affect the network latency, while intrusion detection and prevention systems can improve the network reliability and throughput.

Algorithm 1 Cyber Resilience Layer Processing

Require: $bdms$: A list of trusted BDMs,
$cdms$: A list of trusted CDMs,
odm: The ODM,
$epochs$: The number of epochs
Ensure: Aggregated tuples and classification results

BDM vs CDM training process
Initialize the discriminator and generator models.
for epoch in range(epochs) **do**
  for CDM in $cdms$ **do**
    Get the attack features Y_j detected by BDMs.
    Train the CDM's discriminator on the attack features.
  end for
  for BDM in $bdms$ **do**
    Set L to the total number of trustworthy BDMs that activate their generators.

    for $k \in 1, ..., L$ **do**
      BDM sends its rule weights $\mathcal{W}_k$to the attached CDM.
    end for
  end for
  for CDM in $cdms$ **do**
    Compute $Agg = \frac{\sum_{k=1}^{L}(W_k)}{K}$
    Send Agg to the BDMs.
  end for
end for

CDM vs ODM training process
for epoch in range(epochs) **do**
  Get the attack features Y'_j detected by CDMs.
  Train the ODM's discriminator on the attack features.
  for CDM in $cdms$ **do**
    Set L' to the total number of associated CDM.

    for $k' \in 1, ..., L'$ **do**
      CDM sends $\mathcal{W'}_{k'}$ to ODM.
    end for
  end for
  Compute $Agg' = \frac{\sum_{k'=1}^{L'}(W'_{k'})}{K'}$
  Send Agg' to the CDMs.

  Detection process
  for CDM in $cdms$ **do**
    Set IN to the incoming attack features.
    Apply Agg on IN and set out to the classification result.
    Apply Agg' on IN and set out' to the result.

    if $out \neq out'$
    Update the discriminator models
    end if
  end for
end for

RETURN $\mathcal{W}_k$, $\mathcal{W'}_{k'}$ and out.

Compared to the IoT, the IoD network has some unique security challenges due to its dynamic and heterogeneous nature. The mobility of drones, which can fly at high speeds and access remote locations, makes them vulnerable to physical attacks, such as interception and jamming. Moreover, the drones' small size and limited processing power can make them vulnerable targets for cyber-attacks, such as spoofing and denial-of-service attacks. On the other hand, compared to the Internet of Vehicles (IoV), the IoD network poses some different security challenges due to the drones' unique characteristics. For instance, drones operate in three-dimensional space, which requires different security measures than vehicles that operate on two-dimensional roads. Moreover, drones can operate autonomously, which increases the risk of malfunction and misbehavior due to hardware or software failures.

In terms of security requirements, the IoD network has some specific KPIs that need to be considered. For instance, the latency requirement for drone-based services is much lower than that of traditional IoT devices due to the real-time nature of drone operations. Furthermore, the reliability is critical for drones, as any security breach could result in significant consequences, such as loss of control or physical harm. Therefore, the security mechanisms employed in the IoD network need to be highly efficient and capable of addressing the unique security challenges of this network. These mechanisms should provide end-to-end security, including secure communication, secure storage, and secure processing, to safeguard the drones and their data from various threats and attacks. Furthermore, the security mechanisms should be highly adaptable to the dynamic and heterogeneous nature of the IoD network, allowing for fast and efficient security updates and upgrades.

B. Performance Assessement

In this section, we evaluate the performance of the proposed ZTA framework for the IoD use case by analyzing its detection efficiency and false positive metrics.

The detection efficiency, denoted as E, measures the average time it takes to monitor the security modules to detect malicious targets within its proximity. To calculate E, we consider the total number of security modules located within the malicious targets neighborhood. The security modules include drones equipped with sensors, control stations, and operation systems that collaborate to detect and face the potential threats. On the other hand, the false positive metric, referred to as F, measures the number of false detection generated by the security modules and detected by the higher security modules over the total number of security modules detecting false positives. False positives can occur due to various reasons, such as environmental noise, faulty sensors, or errors in the algorithms used to detect malicious behavior.

We carried out simulations and presented E and F metrics as a function of the iterations involving the collaborative efforts of drones, control stations, and operation systems in

detecting attacks. In the proposed robust ZTA, we assume that some security modules may be compromised and act as malicious agents. Thus, we compare the obtained results either considering the eventual security modules acting as malicious agents or not. The proposed framework provides an additional layer of protection against potential attacks and ensures that the system can operate even if some security modules are compromised. We depict the robust trust framework in Figs 3 and 4. Under the weak trust framework, we assume that all security modules are trusted agents and do not behave as malicious agents. This framework may be suitable for low-risk environments where the probability of malicious attacks is low.

There are various attack datasets available in the literature, specifically for IoT systems. In this study, we leverage the IoT attack datasets proposed in [22] to assess the security performance of our proposal in the context of IoD. These datasets comprise normal traffic as well as malicious traffic related to network attacks such as denial of service. The data is categorized into two classes, which allows us to evaluate how well our system can detect and respond to potential attacks within the IoD ecosystem. By using these datasets, we can evaluate the effectiveness of the proposed security solution and validate its performance in simulated attack scenarios.

Fig. 3 displays the detection efficiency of our proposed zero trust framework for IoD increases as function of the number of iterations. It is note that, when the number of iterations increases, the accuracy of attack detection increases, specifically when the number of iterations reaches 40 iterations. Fig. 3 shows that a weak trust framework demands a higher detection efficiency to protect the wireless network as compared to a robust ZTA. This is due to the collaborative detection process executed by trusted security modules such as BDMs, CDMs, and ODM. In this process, only trusted security modules are permitted to participate. When untrusted security modules, such as malicious BDMs and/or CDMs, are incorporated in the final decision-making process performed by ODM against suspicious IoD devices, the detection efficiency increases, particularly when the number of malicious IoD devices is high. The untrusted security modules aim to deceive the system by providing false attack detection, i.e., wrongly categorize the legitimate target as an attacker and vice versa. This mischief is intended to force ODM to perform multiple verification on the suspicious IoD devices, leading to the increase of detection efficiency. This emphasizes the importance of our proposed robust zero trust framework in ensuring the security of IoD systems by detecting and responding to potential attacks, even in the presence of malicious security modules.

In Fig. 4, we demonstrate that the proposed ZTA framework for IoD shows a lower false positive rate than the weak trust framework. This outcome is achieved by utilizing a non-cooperative security game among BDMs to identify the most distinguishable attack features. These features are then forwarded to trusted CDMs for further attack detection. The collaboration between trusted CDMs and ODM aims to detect and eliminate any malicious BDMs and CDMs, which can contribute to the occurrence of false positives. By identifying and eliminating these malicious security modules, our proposed framework ensures a higher level of security for IoD systems and minimizes the probability of false alarms, which can be detrimental to the performance of these systems.

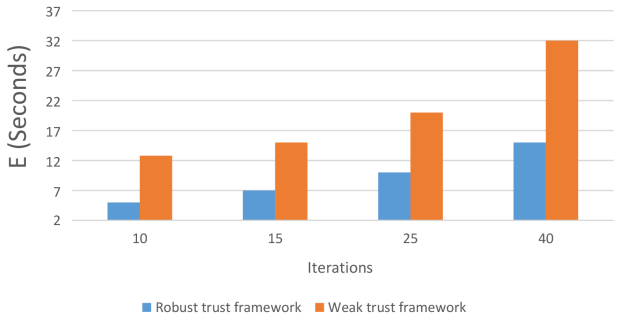

Fig. 3. Efficiency detection

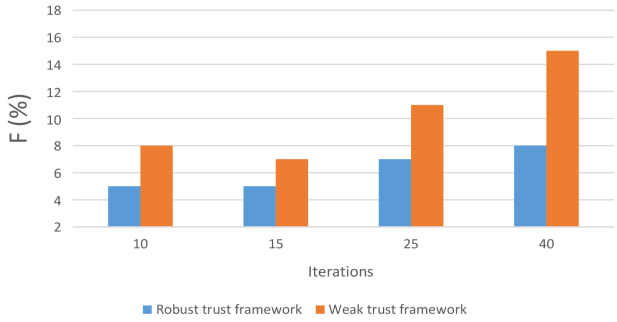

Fig. 4. False positive

In Fig. 5, we analyze the decision-making rate accuracy (denoted by M), which are computed as the number of attacks correctly detected by the distributed defense agents (in our case, BDMs and CDMs) and confirmed by centralized defense agent (in our case ODM) over the total number of defense agents. We vary the number of defense agents from 25 to 70 agents and compute the decision-making rate generated by our adaptive ZTA. Furthermore, we compare the security performance of the proposed ZTA, with current ZTAs [6], [7] conceived to secure the 5G beyond and 6G networks. As shown in Fig. 4, our adaptive ZTA and current zero trust framework [7] exhibit a high decision-making rate as compared to the zero trust framework [6], specifically when the number of defense agents increase. This is due to the fact that, in [6], the authors do not consider the fact that the security agents could be hacked by the attacker and could behave as malicious agents. Therefore, in [6], the number of false positive could increase

promptly. However, Fig. 5 shows that, when the number of defense agents is equal or greater than 50 agents, the adaptive ZTA shows a little improvement as compared to [7]. This result is achieved thanks to the cyber resilience approach executed by the defense agents, BDMs, CDMs and ODM to improve the accuracy of attack detection. Furthermore, the defense agents run the collaborative GAN algorithm during the resilience process to prevent the new attacks on executing an intrusion against the 6G RAN.

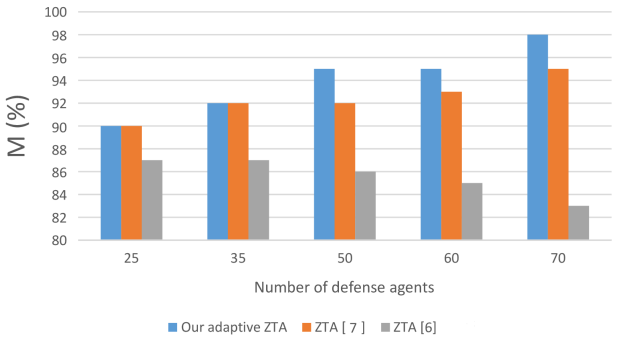

Fig. 5. Accuracy decision-making

VI. Conclusion

Cybersecurity is a critical aspect for the future 6G wireless network, and advanced detection and prevention mechanisms must be deployed to address the heterogeneity of devices in the 6G architecture and the increasing complexity of cyber-attacks. ZTA has been identified as a promising security architecture to safeguard critical network infrastructure from external and internal cyber threats. This paper introduces a new distributed and hierarchical zero trust framework that aims to protect the 6G RAN from network attacks attempting to penetrate the core network. The proposed security framework is based on distributed security modules deployed at base stations, core network functions, and cloud servers to monitor the radio access network and prevent external attacks from executing internal attacks remotely. Simulation results demonstrate that our proposed security framework achieves a low detection time and a very low false positive rate.

Our future research perspective is to consider other 6G KPIs during the experimental phase, we cite the network coverage, throughput and connectivity's degree.

Acknowledgment

This work is an extended and enhanced version of the conference paper that has been presented at 6TH IEEE International Workshop on Intelligent Transportation and Autonomous Vehicles Technologies in Florida [23].

Author Contributions All authors contributed to this work.

Funding Not applicable.

Data Availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no competing interests.

Ethical Approval Not applicable.

References

[1] S. Talwar, N. Himayat, H. Nikopour, F. Xue, G. Wu, and V. Ilderem, "6g: Connectivity in the era of distributed intelligence," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 45–50, 2021.

[2] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran," *Computer Networks*, p. 109358, 2022.

[3] S. Rose, O. Borchert, A. Mitchell, and S. Connelly, "Zero trust architecture, nist special publication 888-207," *NIST, Aug/2020.[online]. Available: https://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST. SP*, vol. 800207, 2020.

[4] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57 143–57 179, 2022.

[5] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in cloud computing environment," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2020, pp. 1–6.

[6] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6g security," *arXiv preprint arXiv:2203.07716*, 2022.

[7] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6g edge computing," *IEEE Network*, pp. 1–13, 2023.

[8] S. Bao, W. Sun, and H. Xu, "A native intelligent and security 6g network architecture," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. IEEE, 2022, pp. 395–400.

[9] H. Sedjelmaci, N. Kheir, A. Boudguiga, and N. Kaaniche, "Cooperative and smart attacks detection systems in 6g-enabled internet of things," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 5238–5243.

[10] C. Dong, F. Jiang, S. Chen, and X. Liu, "Continuous authentication for uav delivery systems under zero-trust security framework," in *2022 IEEE International Conference on Edge Computing and Communications (EDGE)*. IEEE, 2022, pp. 123–132.

[11] F. A. P. de Figueiredo, "An overview of massive mimo for 5g and 6g," *IEEE Latin America Transactions*, vol. 20, no. 6, pp. 1548–0992, 2022.

[12] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[13] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[14] M. Xu, D. Thai Hoang, J. Kang, D. Niyato, Q. Yan, and D. In Kim, "Secure and reliable transfer learning framework for 6g-enabled internet of vehicles," *IEEE Wireless Communications*, vol. 29, no. 4, pp. 132–139, 2022.

[15] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627.

[16] S. Soltani, M. Shojafar, R. Taheri, and R. Tafazolli, "Can open and ai-enabled 6g ran be secured?." *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 11–12, 2022.

[17] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif, and M. Rajarajan, "Securing the lorawan join procedure using blockchains," *Cluster Computing*, vol. 23, pp. 2123–2138, 2020.

[18] W. Qiang and Z. Zhongli, "Reinforcement learning model, algorithms and its application," in *2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC)*. IEEE, 2011, pp. 1143–1146.

[19] L. An, A. Chakrabortty, and A. Duel-Hallen, "A stackelberg security investment game for voltage stability of power systems," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3359–3364.

[20] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *International Conference on Information Processing in Medical Imaging*. Springer, 2017, pp. 146–157.

[21] G. Raja, S. G. Senthivel, S. Balaganesh, B. R. Rajakumar, V. Ravichandran, and M. Guizani, "Mlb-iod: Multi layered blockchain assisted 6g internet of drones ecosystem," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2511–2520, 2023.

[22] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108–116.

[23] H. Sedjelmaci and K. Tourki, "A distributed zero trust framework for 6g ran," in *6TH International Workshop on Intelligent Transportation and Autonomous Vehicles Technologies*. IEEE, 2013.