Fortifying Lifelong Security for O-RAN Ecosystem: An Incremental Learning Framework for NextG Seamless Networking

[1]Mrityunjoy Gain, [2]Avi Deb Raha, [2]Apurba Adhikary, [2]Sheikh Salman Hassan, and [2]Choong Seon Hong
[1]Department of Artificial Intelligence, Kyung Hee University, Yongin-si, South Korea
[2]Department of Computer Science and Engineering, Kyung Hee University, Yongin-si, South Korea
Email: {gain, avi, apurba, salman0335, cshong}@khu.ac.kr

***Abstract*—Next-generation cellular networks are shifting towards cloud-based infrastructures emphasizing programmability, virtualization, and modular architectures. The open radio access network (O-RAN) paradigm is a promising approach to overcoming traditional RAN limitations by offering an open framework for data-driven optimization at the individual user level. However, this openness also introduces vulnerabilities, where malicious attacks or unauthorized requests can compromise user privacy, disrupt resource allocation, and degrade overall service quality. In addition, new user equipment (UEs) can be introduced with new attacks and vulnerabilities over time. To address these challenges, we propose a deep incremental learning framework designed for the O-RAN environment, aimed at managing and mitigating these cyber threats while ensuring optimal user experience and resource utilization. We formulate an optimization problem to learn new attacks or vulnerabilities while retaining the knowledge of previous threat knowledge. To solve the optimization problem, we propose an exemplar-based convolutional neural network (CNN) model, implemented within the non-real-time RAN intelligent controller (non-RT RIC), to effectively monitor traffic at the radio units (RUs). Experimental results demonstrate that our proposed framework secures the O-RAN ecosystem with over 91% accuracy, outperforming non-incremental methods by approximately 31% in distinguishing between benign and malicious traffic, thereby greatly enhancing network security and reliability for lifelong.**

***Index Terms*—O-RAN, incremental learning, RAN security, dynamic traffic, non-RT-RIC**

I. Introduction

Wireless communication is rapidly evolving, with a diverse array of new communication devices emerging to provide various services. Consequently, the volume of network traffic is increasing significantly, as different types of traffic require tailored services [1]. Traditionally, managing these diverse traffic types necessitated a wide range of hardware solutions, complicating network management. However, there is a shift towards a unified hardware approach that allows multiple services to operate on the same infrastructure. The radio access network (RAN) is a promising technology that addresses this need by decoupling the physical and logical layers of communication. This separation enables different logical layers to share the same physical layer, facilitating the delivery of multiple services while simplifying network management and enhancing efficiency.

Traditional RAN systems often struggle with vendor lock-in, inflexibility, and high costs due to tightly integrated hardware and software. In contrast, the open radio access network (O-RAN) is reshaping wireless telecommunications by promoting openness, disaggregation, and standardization. By decoupling hardware and software, O-RAN enables greater interoperability, innovation, and vendor-neutral ecosystems, leading to more competitive and cost-effective solutions. Its architecture, consisting of central units (CUs), distributed units (DUs), and radio units (RUs), facilitates 5G deployment and advanced network optimization [2]. As diverse traffic types emerge alongside various UEs, the likelihood of new and evolving threats increases significantly over time.

Despite the burgeoning interest in O-RAN, the domain of threat detection and security within this framework remains less explored. Existing studies have introduced some strategies for addressing network anomalies, such as TenaxDoS, which integrates federated learning with a replay memory-based continual learning method [3], and federated learning-based [4] anomaly detection in the O-RAN architecture, emphasizing data privacy preservation. Alves et al. [5] examined the feasibility of machine learning techniques for anomaly detection in O-RAN environments. Basaran et al. [6] developed a deep learning-based autoencoder to detect RF anomalies at the user equipment level, enhancing service continuity. However, static models in anomaly detection become less effective over time because they are trained on a fixed dataset and cannot adapt to new patterns or threats that emerge in a constantly changing environment like O-RAN. As new devices connect, traffic increases and network behaviors shift, the types of anomalies evolve, making it difficult for static models to maintain accuracy. Without the ability to learn from these changes, static models miss new types of anomalies or generate false alarms.

To address this issue, we propose an incremental deep-learning framework for the lifelong security of O-RAN by adapting evolving types of threats. Incremental learning can learn new patterns without forgetting previous patterns. It allows the model to update its knowledge as new data comes

[0]This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2022-00155911, Artificial Intelligence Convergence Innovation Human Resources Development (Kyung Hee University)), (No. RS-2024-00509257, Global AI Frontier Lab), and supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2023-00207816). *Dr. CS Hong is the corresponding author.

979-8-3315-0694-0/25/$31.00 ©2025 IEEE

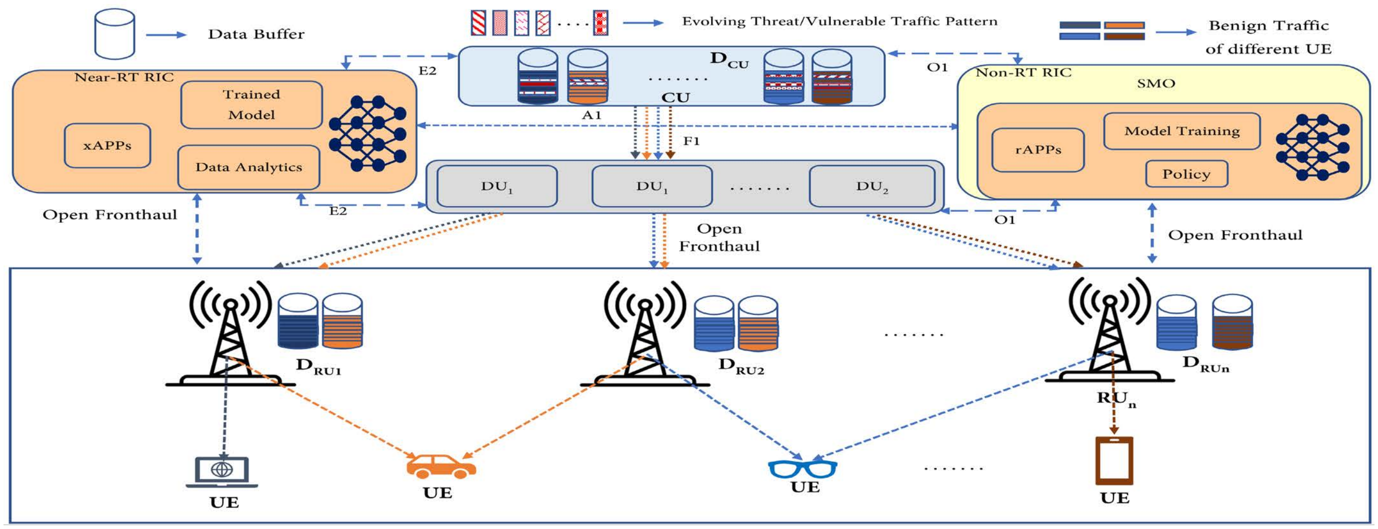


Fig. 1. System model for lifelong security in the O-RAN ecosystem.

in without needing to retrain from scratch, making the detection process more robust and adaptive. Our research aims to enhance the cohesiveness of the O-RAN ecosystem for real-time users for lifelong. The main contributions of our work include the development of an incremental deep-learning framework designed to manage malicious requests and ensure pervasive user services. We formulate an optimization problem to learn new knowledge without forgetting prior knowledge, specifically targeting dynamic changes and uncertainties related to attack requests. Furthermore, we propose an exemplar reply-based CNN model to solve this optimization problem effectively. Experimental results demonstrate that our approach successfully continually categorizes malicious network traffic, thus contributing to a more cohesive and secure O-RAN environment for lifelong. The main contributions of our proposed method are given below:

- We propose an incremental learning framework for the O-RAN environment that secures the O-RAN ecosystem handles any attacks or threat requests and provides pervasive services to the users.
- We formulate an optimization problem to learn new threats or vulnerability patterns without forgetting the knowledge of previously learned threats on dynamic changes and uncertainties, specifically targeting poisonous requests.
- We propose an exemplar replay-based incremental CNN model to solve the optimization problem, ensuring lifelong adaptive service in the O-RAN ecosystem amidst evolving threats and dynamic conditions.
- Experimental results demonstrate that our proposed method effectively classifies newly introduced malicious netquakes while retaining knowledge of prior threats, achieving an average accuracy of over 91% which is 31% higher than the non-incremental mechanism.

The rest of the paper is organized as follows. Section II discusses the literature review. In Section III and IV, we illustrated the system model and incremental O-RAN anomaly scenario respectively. Section V and VI represent the problem formulation and solution approach, respectively. Section VII presents the simulation settings and results, and finally, Section VIII concludes the paper.

II. Literature Review

In this section, we discussed the baseline works for O-RAN security. Alves et al. [5] propose some machine learning models to classify anomalies based on two 5G O-RAN datasets. Additionally, they propose a strategy to label anomalies using t-SNE on datasets with multiple KPIs, enabling clear identification of abnormal patterns. Başaran et al. [6] present a deep learning-based autoencoder for detecting RF anomalies at the UE side via xApps on the 5G near real-time RIC, ensuring improved and seamless service continuity. Rumesh et al. [7] propose a security architecture within a Network Digital Twin (NDT), aligned with O-RAN standards, for training machine learning models to enhance O-RAN security operations. They demonstrate a hierarchical Federated Learning (FL) anomaly detection algorithm across three traffic slices, with training data generated using the Colosseum emulation system. Attanayaka et al. [4] explore the use of FL for anomaly detection in the O-RAN architecture, emphasizing data privacy preservation. They propose a peer-to-peer (P2P) FL-based anomaly detection mechanism and conduct an in-depth analysis of four P2P FL variants. They evaluate their proposed models using simulations with the UNSW-NB15 dataset. Benzaïd et al. [3] introduce 'TenaxDoS', a framework that integrates FL with a replay memory-based CL strategy. This approach enables sustainable and cooperative network anomaly detection within the O-RAN environment beyond 5G networks. Mahrez et al. [8] analyze the handover process of a moving vehicle by comparing the effectiveness of different machine-learning techniques for anomaly detection within an O-RAN traffic steering module. Their goal is to improve handover prediction accuracy using these ML methods.

Given the promising potential of O-RAN, incremental learning can play a key role in ensuring a sustainable, long-term solution for securing the O-RAN ecosystem. Since continual learning is relatively underexplored in this context, it presents a valuable opportunity for further investigation.

III. System Model

The system model of our work is shown in Fig 1. We have one central Unit, represented as CU, M number of distributed units (DUs), denoted as DU_i, where $i = 1, 2, \dots, M$, and N number of radio units (RUs), denoted as RU_j, where $j = 1, 2, \dots, N$. The user equipment is denoted as UE. Each DU_i is connected to a subset of RUs, represented by the set $R_{DU_i} \subseteq \{RU_1, RU_2, \dots, RU_N\}$. The connection between the CU and DU can be modeled as a high-level control plane or backhaul link. For each DU_i, the link is represented as $L_{CU\to DU_i}$ where L represents the connection between units. The connection between each DU and the RUs under its control is denoted as $L_{DU_i \to R_{DU_i}}$ indicating that the DU_i controls the set of RUs in R_{DU_i}. Every UE is connected to a subset of RUs. Let $R_{UE} \subseteq \{RU_1, RU_2, \dots, RU_N\}$ be the set of RUs connected to the UE. The communication link between the UE and the connected RUs is represented as $L_{UE\to R_{UE}}$.

A. Wireless Channel Model

We represent the wireless channel as $h_j(t)$ between the UE and RU j. The received signal $y_j(t)$ at RU j is expressed as Eq. (1).

$$y_j(t) = h_j(t)x(t) + n_j(t), \tag{1}$$

where $x(t)$ is the transmitted signal from the UE, $h_j(t)$ is the channel gain (complex fading coefficient) for RU j, $n_j(t)$ is the additive White Gaussian Noise (AWGN) at RU j, typically $n_j(t) \sim \mathcal{N}(0, \sigma_n^2)$.

Multi-path Fading Model: We assume that the wireless channel consists of multiple paths between the UE and each RU. The wireless channel is expressed as Eq. (2).

$$h_j(t) = \sum_{l=1}^{L_j} \alpha_{j,l} e^{-j2\pi f_{j,l} t} e^{j\theta_{j,l}}, \tag{2}$$

where L_j is the number of multi-path components for RU j, $\alpha_{j,l}$ is the amplitude gain of the l-th path for RU j, $f_{j,l}$ is the doppler shift of the l-th path for RU j, dependent on the UE's velocity and direction, and $\theta_{j,l}$ is the phase shift of the l-th path for RU j.

Path Loss Model: We modelled the path loss between UE and RU j as Eq. (3).

$$PL_j = PL_0 + 10\eta \log_{10}(d_j), \tag{3}$$

where PL_j is the path loss for the link between UE and RU j, PL_0 is the path loss at a reference distance (usually 1 meter), η is the path loss exponent, which depends on the environment (urban, rural, indoor, etc.), and d_j is the distance between the UE and RU j.

Complete Channel Model: The complete channel gain (including path loss and fading) between UE and RU j can then be written as Eq. (4).

$$h'_j(t) = \frac{h_j(t)}{PL_j} \tag{4}$$

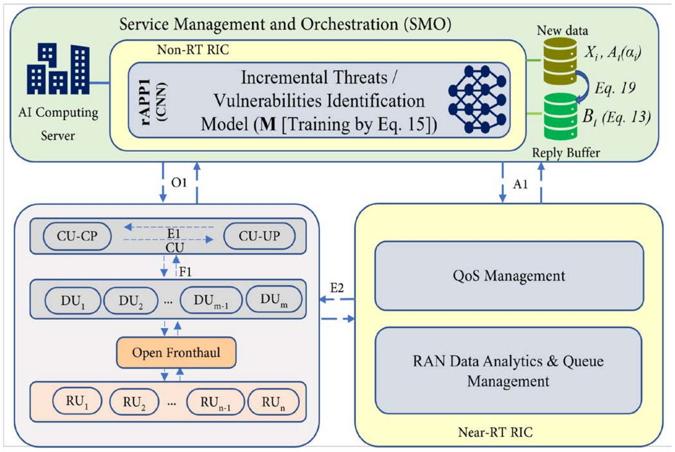


Fig. 2. Proposed solution approach for enhancing the incremental O-RAN security of the ecosystem.

IV. Incremental O-RAN Anomaly Scenario

We $U(t) = \{\text{UE}_1, \text{UE}_2, \dots, \text{UE}_{N(t)}\}$ represent the set of UEs at time t, where $N(t)$ is the number of UEs at time t. New UEs can be introduced dynamically over time. We $A_k(t) = \{A_k^1, A_k^2, \dots, A_k^{P_k(t)}\}$ represent the set of anomaly types for UE k, where $P_k(t)$ is the number of anomaly types observed in UE k at time t. When new UEs $\text{UE}_{N(t)+1}, \text{UE}_{N(t)+2}, \dots$ are introduced into the RAN, the system must handle their integration. Some UEs already in the system may experience the introduction of new anomaly types. For any $\text{UE}_k \in U(t)$, as new anomaly types are detected, we update the anomaly set $A_k(t)$ as Eq. (5).

$$A_k(t+1) = A_k(t) \cup \{A_k^{P_k(t)+1}, A_k^{P_k(t)+2}, \dots\} \tag{5}$$

This process continues as new anomalies evolve within the UE. When a new UE, $\text{UE}_{N(t)+1}$, is added at time t, its anomaly types evolve simultaneously, with the possibility of new types being introduced into the UE over time. The new user arises is represented as Eq. (6).

$$U(t+1) = U(t) \cup \{\text{UE}_{N(t)+1}\} \tag{6}$$

The set of anomaly types for $\text{UE}_{N(t)+1}$ will grow as Eq. (7).

$$A_{N(t)+1}(t+k) = A_{N(t)+1}(t+k-1) \cup \{A_{N(t)+1}^{P_{N(t)+1}(t+k-1)+1}, \dots\} \tag{7}$$

The loss function must now account for both the detection of new UEs and evolving anomalies within existing UEs. The total incremental anomaly detection loss function is expressed as Eq. (8).

$$L(t) = \sum_{k=1}^{N(t)} \left(L_\alpha(M(t), A_k(t)) + L_{\text{new-UE}}(M(t), \text{UE}_k(t)) \right), \tag{8}$$

where $L_\alpha(M(t), A_k(t))$ is the loss for detecting anomalies in UE_k. $L_{\text{new-UE}}(M(t), \text{UE}_k(t))$ is the loss associated with the detection of new UEs.

V. PROBLEM FORMULATION

We formulate the continual learning optimization problem as follows:

$$\begin{aligned}\min_{\theta_t} \Bigg(& \frac{1}{N_t} \sum_{i=1}^{N_t} \left[w(y_i) \ell(M(x_i; \theta_t, A_t), y_i) \right] \\ & + \frac{1}{K_t} \sum_{j=1}^{K_t} \left[\beta_t \ell(M(x_j(t); \theta_t, A_t), y_j(t)) \right] \Bigg),\end{aligned} \tag{9}$$

where N_t represents the number of new samples at time t. K_t represents the number of replay samples at time t. $w(y_i)$ is a weight function for the new sample labels y_i. $\ell(\cdot, \cdot)$ represents the loss function. $M(x; \theta_t, A_t)$ represents the model M at time t with parameters θ_t and anomaly set A_t. β_t is the weight for the replay samples. x_i, y_i are the new input data and labels at time t. $x_j(t), y_j(t)$ are the replayed input data and labels from previous time steps. The anomaly set A_t increases over time when new anomaly patterns come. The objective function is designed to balance learning from the new data N_t and replayed data K_t to maintain continual learning and anomaly detection performance over time.

VI. SOLUTION APPROACH

To solve the formulated problem, we propose an exemplar-reply-based deep incremental framework within the non-RT-RIC, illustrated in Fig. 2. We propose a low-level and high-level [9] feature fusion-based CNN model as the backbone for our incremental learning framework as shown in Fig. 3. The CNN extracts both low and high-level patterns [10] from all RU traffic, analyzes them, and filters out unauthorized packets to ensure secure operation across all UEs. Our proposed exemplar reply-based method is able to adapt new knowledge without forgetting the previous knowledge. We have detailed our proposed approach sequentially in this section. The model structure with anomaly classes is shown in Eq. (10).

$$M(x_{i,k}, \theta_t, A_t) = \hat{y}_{i,k}, \quad A_t = \{\alpha_1, \alpha_2, \ldots, \alpha_{A_t}\} \tag{10}$$

where $M(x_{i,k}, \theta_t, A_t)$ is the CNN model parameterized by θ_t at time t, processing input $x_{i,k}$ from the k-th RU of the i-th UE. The output $\hat{y}_{i,k}$ is the predicted anomaly class from A_t, the set of known anomalies at time t, with A_t total anomaly types.

We use weighted cross-entropy loss as our loss function. The loss for the current task is shown in Eq. (11).

$$L_{\text{current}}(\theta_t) = \frac{1}{N} \sum_{i=1}^{N} \left[w(y_i) \cdot \ell(M(x_i; \theta_t, A_t), y_i) \right] \tag{11}$$

where $w(y_i)$ is a dynamic weight function assigning higher weight to rare anomaly types, and $\ell(\cdot)$ is the cross-entropy loss. y_i is the true anomaly class for the i-th UE data x_i.

To store the representative samples from the previous task, we use a reply memory buffer. The memory buffer with time decay is shown in Eq. (12).

$$\begin{aligned} B_t &= \{(x_j(t), y_j(t), \alpha_j(t))\}_{j=1}^{K_t} \\ \text{with time-decay:} \, B_t &\leftarrow \beta_t \cdot B_{t-1} \end{aligned} \tag{12}$$

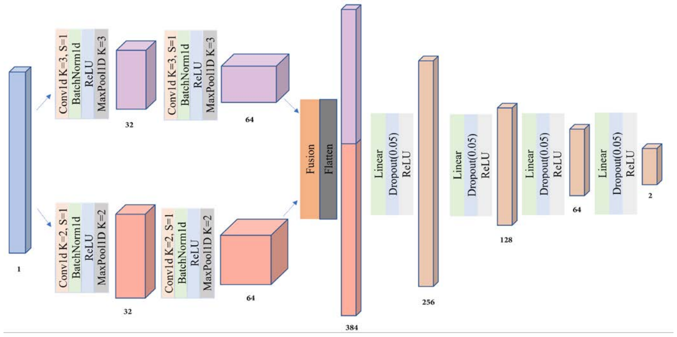


Fig. 3. Proposed CNN model for our framework.

where B_t is the buffer at time t, storing previous data $(x_j(t), y_j(t), \alpha_j(t))$ of K_t samples, and β_t is the decay factor ensuring older data loses importance as t increases. To keep the previous knowledge, we need to train the representative samples of the previous samples at the time of training the new task. We define the loss of the representative samples of the previous task as replay loss with decay, shown in Eq. (13).

$$L_{\text{replay}}(\theta_t) = \frac{1}{K_t} \sum_{j=1}^{K_t} \left[\beta_t \cdot \ell(M(x_j(t); \theta_t, A_t), y_j(t)) \right] \tag{13}$$

where the time-decayed memory buffer reduces the importance of past samples.

We combine the current loss and reply loss and make a trade-off to balance both plasticity and elasticity. The combination of loss with the current and replay is shown in Eq. (14).

$$L_{\text{total}}(\theta_t) = \lambda_t L_{\text{current}}(\theta_t) + (1 - \lambda_t) L_{\text{replay}}(\theta_t) \tag{14}$$

where λ_t dynamically adjusts the importance of new data versus replayed data, balancing between anomaly detection and generalization to older examples.

Based on the total loss, we update the gradient of the model. The gradient update for continual learning is shown in Eq. (15).

$$\theta_{t+1} = \theta_t - \eta_t \nabla_{\theta_t} L_{\text{total}}(\theta_t) \tag{15}$$

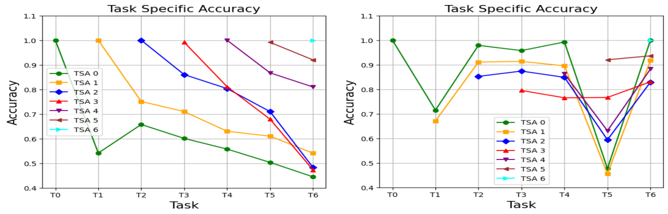
where η_t is the learning rate at time t, and $\nabla_{\theta_t} L_{\text{total}}(\theta_t)$ is the gradient of the total loss with respect to the model parameters. After learning the current task, we store some representative samples of the current task in the reply buffer. These samples will be used in further training when a new task comes. The memory buffer update is shown in Eq. (16).

$$B_{t+1} = B_t \cup \{(x_i(t+1), y_i(t+1), \alpha_i(t+1))_{\text{new}}\}^{N_{t+1}} \tag{16}$$

where $\{(x_i(t+1), y_i(t+1), \alpha_i(t+1))_{\text{new}}\}$ represents the newly detected samples from time $t+1$. When a new UE comes, we expand the UE set. New UE has a high probability of introducing new anomaly types. The UE set expansion is shown in Eq. (17).

$$U_{t+1} = U_t \cup \{u_i\}_{\text{new}}^{U_{t+1}} \tag{17}$$

where U_{t+1} represents the number of new UEs added at time $t+1$.



(a) Non-incremental CNN (b) Proposed Method

Fig. 4. Task-specific sccuracy of our proposed method compared to conventional non-incremental CNN method.

If a new UE introduces some new anomaly, we expand the anomaly set along with the UE track. This new anomaly is trained in a continual learning manner without forgetting the previous anomaly-type knowledge. The anomaly set expansion is shown in Eq. (18).

$$A_{t+1} = A_t \cup \{\alpha_k\}_{\text{new}}^{A_{t+1}} \tag{18}$$

where A_{t+1} is the number of new anomaly types detected at time $t+1$.

VII. Simulations Settings and Results

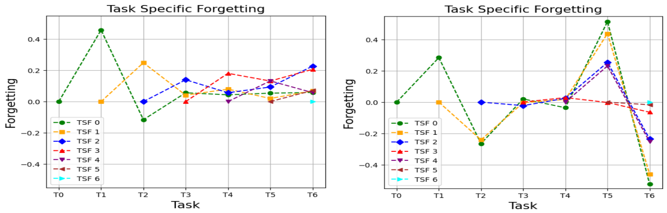
A. Dataset and Environment Settings

For our experiment, we utilize the O-RAN anomaly detection dataset, as outlined in [11]. This dataset comprises 10,000 traffic data samples, each with 23 numerical features. The dataset includes both benign and malicious O-RAN traffic, spanning over 20 distinct pieces of user equipment. 3 train passengers, 10 waiting passengers, 4 cars, and 3 pedestrians. We divide the UEs into 7 sequential tasks. The data is divided into two subsets: 80% of the samples are used for training, while the remaining 20% are set aside for testing the model's performance on unseen data. we stored 500 exemplars from each task in the reply buffer, maintaining a fair contribution of each UE. We set up our computational environment using Python 3.10 and PyTorch as the deep learning framework. For model optimization during training, we used the Adam optimizer [12]. We set the learning rate to 0.0001 to ensure gradual updates to the model weights, preventing large jumps that might destabilize the learning process. We used batch size 128 and λ_t = 0.5 throughout training.

B. Experimental Results

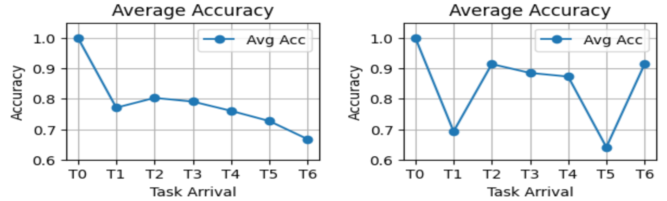
In this section, we present the results of our proposed exemplar-based CL method compared to non-incremental settings. To evaluate the performance, we took task-specific accuracy, task-specific forgetting, average accuracy, average forgetting, backward transfer, and forward transfer [13]. These metrics are the baseline metrics for evaluating incremental learning.

In Fig. 4, we compare the task-specific accuracy of our exemplar replay-based method to a categorical non-incremental deep learning approach across seven sequential tasks. As shown in Fig. 4(a), the non-incremental method suffers a significant accuracy drop for all previous tasks with each new task introduction. Notably, during task 3, task 1's accuracy slightly improves due to similar malicious traffic patterns. In contrast, our proposed method shows negligible accuracy drops when new tasks are introduced and can recover minor losses during future task training, effectively minimizing forgetting as demonstrated in Fig. 4(b). Although some forgetting occurs during tasks 2 and 5, the model successfully restores this knowledge in subsequent tasks, maintaining satisfactory performance. In Fig. 5, we compare the task-specific forgetting of our exemplar replay-based method with the non-incremental deep learning approach across seven sequential tasks. Positive values indicate forgetting, negative values reflect knowledge restoration, and zero represents no forgetting. Fig. 5(a) shows the non-incremental method consistently forgets previous tasks, with slight restoration during task 3 due to similarities with task 1. In contrast, our method exhibits minimal forgetting, with only small positive values as shown in Fig. 5(b). It also restores knowledge during later tasks, as shown by negative values, ensuring strong overall performance throughout the sequence.



(a) Non-incremental CNN (b) Proposed Method

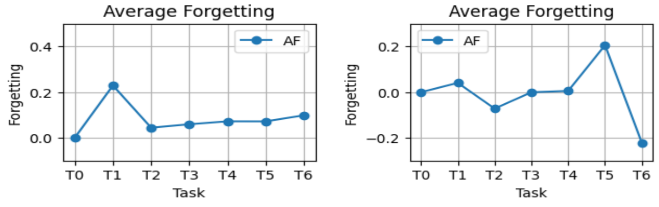
Fig. 5. Task-specific forgetting of our proposed method compared to conventional non-incremental CNN method.



(a) Non-incremental CNN (b) Proposed Method

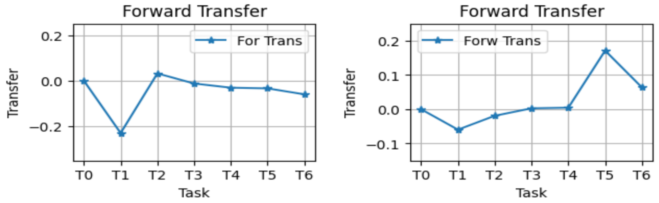
Fig. 6. Average accuracy of our proposed method compared to conventional non-incremental CNN method.

In Fig. 6, we compare the average accuracy of our proposed method with the conventional non-incremental approach, showing how accuracy evolves as new tasks are introduced. Fig. 6(a) displays the conventional method's average accuracy, which consistently declines with each new task, indicating a failure to retain previously learned knowledge. In contrast, Fig. 6(b) illustrates our proposed method's performance, which effectively restores lost accuracy during training on new tasks, demonstrating its ability to recover and maintain overall performance despite sequential learning. In Fig. 7, we compare the average forgetting of our proposed method with the conventional non-incremental approach, showing how task accuracy changes as new tasks are introduced. Positive values indicate forgetting, negative values reflect knowledge restoration and zero values signify no forgetting or restoration. Fig. 7(a) shows the average forgetting of the conventional non-incremental method, with consistently positive values indicating forgetting with each new task, highlighting its inability



(a) Non-incremental CNN (b) Proposed Method

Fig. 7. Average forgetting of our proposed method compared to conventional non-incremental CNN method.

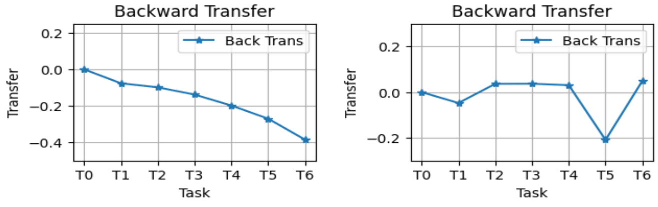


(a) Non-incremental CNN (b) Proposed Method

Fig. 8. Forward transfer of our proposed method compared to conventional non-incremental CNN method.

to retain previously learned knowledge. In contrast, Fig. 7(b) illustrates our proposed method's performance, with values close to zero or negative, signifying effective mitigation of forgetting. Even when some forgetting occurs, the model can restore lost knowledge during subsequent task training, demonstrating resilience and capacity for continual learning without significant degradation.

In Fig. 8, we compare the forward transfer of our proposed method with the conventional non-incremental approach, illustrating how learning previous tasks affects subsequent ones. Positive values indicate that prior knowledge aids in learning new tasks more effectively, while negative values suggest that earlier knowledge hinders the acquisition of new information. Fig. 8(a) shows the forward transfer of the conventional non-incremental method, where consistently negative values indicate that prior knowledge hinders the learning of new tasks, highlighting the method's limitation in integrating new information. In contrast, Fig. 8(b) presents our proposed method, with values close to zero or positive, signifying the successful leveraging of prior knowledge to facilitate learning of new tasks. This demonstrates that our approach avoids interference from past tasks and enables more efficient learning of future ones. In Fig. 9, we compare the backward transfer of our proposed method with the conventional non-incremental approach, showing how learning new tasks affects performance on previously learned tasks. Positive values indicate that learning new tasks enhances earlier task performance, while negative values indicate performance degradation. Fig. 9(a) shows the non-incremental method with consistently negative values, highlighting its failure to retain prior knowledge when learning new tasks. In contrast, Fig. 9(b) demonstrates that our method maintains or improves performance on earlier tasks, with values near zero or positive. Although there is slight interference during task 5, the model quickly recovers, showing that our method effectively balances learning new tasks without forgetting previous ones.



(a) Non-incremental CNN (b) Proposed Method

Fig. 9. Backward transfer of our proposed method compared to conventional non-incremental CNN method.

VIII. Conclusion

In this paper, we propose a deep learning-based continual learning framework tailored for the O-RAN system, effectively addressing the dynamic nature of cyber threats and malicious traffic. The proposed exemplar replay-based CNN model enables real-time traffic analysis and adaptive learning, allowing the system to detect and respond to both new and previously known attacks. This continual learning approach ensures that the model evolves with the network, maintaining its ability to protect user privacy, optimize resource allocation, and uphold high-quality service in the face of emerging vulnerabilities. The framework not only segregates malicious from benign traffic but also adapts to the ever-changing landscape of network threats. With over 91% average accuracy in distinguishing between legitimate and harmful traffic, the experimental results highlight the model's robustness and effectiveness, making it a valuable solution for enhancing the security, reliability, and overall performance of the O-RAN ecosystem in a rapidly evolving threat environment.

References

[1] M. Gain *et al.*, "Cohere o-ran ecosystem: Towards ensuring nextg seamless networking infrastructure," *in KCC*, pp. 1417–1419, 2024.

[2] M. Gain, A. D. Raha *et al.*, "Cognize metaverse service requests: Towards ensuring pervasive service in the metaverse," *in KSC*, pp. 1229–1231, 2023.

[3] C. Benzaïd *et al.*, "A federated continual learning framework for sustainable network anomaly detection in o-ran," in *in WCNC*, 2024, pp. 1–6.

[4] D. Attanayaka *et al.*, "Peer-to-peer federated learning based anomaly detection for open radio access networks," in *in ICC*, 2023, pp. 5464–5470.

[5] P. V. Alves *et al.*, "Machine learning applied to anomaly detection on 5g o-ran architecture," *Procedia Computer Science*, vol. 222, pp. 81–93, 2023, iNNS DLIA 2023.

[6] O. T. Başaran, *et al.*, "Deep autoencoder design for rf anomaly detection in 5g o-ran near-rt ric via xapps," in *in ICC Workshops*, 2023, pp. 549–555.

[7] Y. Rumesh *et al.*, "Federated learning for anomaly detection in open ran: Security architecture within a digital twin," in *EuCNC/6G Summit*, 2024, pp. 877–882.

[8] Z. Mahrez *et al.*, "Benchmarking of anomaly detection techniques in o-ran for handover optimization," in *IWCMC*, 2023, pp. 119–125.

[9] M. Gain *et al.*, "A novel unbiased deep learning approach (dl-net) in feature space for converting gray to color image," *IEEE Access*, vol. 11, pp. 78 918–78 933, 2023.

[10] M. Gain, A. D. Raha *et al.*, "Ccc: Color classified colorization," *arXiv preprint arXiv:2403.01476*, 2024.

[11] M. Rimmer, "Anomaly detection use case," 2022. [Online]. Available: https://wiki.o-ran-sc.org/display/RICP/Anomaly±Detection±Use±Case

[12] A. D. Raha *et al.*, "Advancing ultra-reliable 6g: Transformer and semantic localization empowered robust beamforming in millimeter-wave communications," *arXiv preprint arXiv:2406.02000*, 2024.

[13] M. Gain *et al.*, "Open ran embracing continual learning: Towards nextg adaptive traffic analysis," in *in NOMS*. IEEE, 2024, pp. 1–7.