Secure Target-Tracking by UAVs in O-RAN Environment

Seyed Ahmad Soleymani[*], Mohammad Shojafar[*], Chaun Heng Foh[*],
Shidrokh Goudarzi[†], and Wenwu Wang[‡]
[*] 5G& 6GIC, Institute for Communication Systems, University of Surrey, Guildford, UK
{s.soleymani, m.shojafar, c.foh}@surrey.ac.uk
[†] School of Computing and Engineering, University of West London, London, UK.
{shidrokh.goudarzi}@uwl.ac.uk
[‡] Centre for Vision, Speech and Signal Processing (CVSSP), University of Surrey, Guildford, UK
{w.wang}@surrey.ac.uk

***Abstract*—The paper presents a comprehensive investigation into a secure target-tracking system employing Unmanned Aerial Vehicles (UAVs) within urban environments. We introduce the Enhanced Multi-Agent Q-Learning (E-MAQL) algorithm designed to enhance target-tracking accuracy while minimizing energy consumption by UAVs. Additionally, we propose a robust security framework leveraging Deep Q-Networks (DQN) for Intrusion Detection Systems (IDS), alongside the implementation of Advanced Encryption Standard (AES) and Lightweight AES (LW-AES) protocols to ensure secure communication within the Open Radio Access Network (O-RAN) architecture. Our evaluations validate the effectiveness of E-MAQL in improving tracking performance and reducing energy consumption, while the proposed security framework demonstrates promising results in detecting and mitigating potential security threats within O-RAN-based systems. Furthermore, we measured the False Positive Ratio (FPR) of the IDS at 6%. Notably, our security framework significantly enhances the target-tracking system's accuracy by 33% when exposed to false injection data attacks, elevating accuracy from 53% to 86%.**

***Index Terms*—Target-tracking, UAVs, IDS, AES, O-RAN**

I. Introduction

Target-tracking is vital across various domains, with Unmanned Aerial Vehicles (UAVs) revolutionizing its efficacy [1]. Today, UAVs have a vital role in aerial surveillance, reconnaissance, and search and rescue operations, equipped with advanced sensors like cameras and radar systems. They enhance situational awareness crucial in military, law enforcement, and disaster response scenarios. Integrating UAVs in target-tracking expands applications, from precision agriculture to infrastructure inspection, highlighting their versatility. Studies like [2] focus on real-time tracking with deep learning, [3] enhances UAV control in dynamic environments, and [4] improves tracking coordination. Despite advancements, challenges persist in UAV-based target-tracking.

Current research on UAV-based target-tracking systems has primarily focused on enhancing tracking accuracy through collaborative efforts among UAVs and other network entities. However, there is a notable gap in addressing potential security threats, such as data manipulation, communication interference, or unauthorized access to system components, which can significantly impact tracking accuracy. As highlighted in [5], UAV security challenges encompass various domains, including sensors, hardware, software, and communication. Secure communication is especially vital, ensuring UAVs operate securely. In target-tracking scenarios, UAVs communicate wirelessly with each other and ground control stations, yet unstable communication links and the open nature of wireless communication expose UAVs to attacks compromising confidentiality, integrity, authenticity, and availability, potentially leading to inaccurate target-tracking.

In addressing these security challenges, [6] introduced a lightweight Intrusion Detection and Prevention System (IDPS) module tailored for UAVs, employing Deep Q-learning (DQN) within a Deep Reinforcement Learning (DRL) framework. This module enhances UAVs' ability to autonomously detect and respond to suspicious activities, thereby bolstering network security. In He et al. [7], a collaborative intrusion detection approach is proposed for UAV-based IoT networks, leveraging a Conditional Generative Adversarial Net (CGAN)-based algorithm with blockchain-enabled distributed federated learning to improve intrusion detection accuracy while ensuring data security and privacy. In [8] an Efficient and Secure Communication Mechanism (ESCM) is developed for UAV networks, featuring an ABC algorithm-based routing protocol and blockchain-enhanced security mechanisms to establish a static network environment, CyberUAV, ensuring efficient and secure communication despite high mobil-

978-3-903176-63-8/24/$31.00 ©2024 IEEE

ity. Despite these advancements, the security concerns in existing security schemes and protocols for UAV networks employed in target-tracking systems remain a significant challenge that needs to be fully addressed.

Motivation. Motivated by accuracy, power limitations, and security concerns, we present a secure target-tracking approach. This work aims to not only achieve precise target-tracking with minimal power consumption but also ensure secure communication among the entities involved in the network. To fulfill this objective, we design a network model comprising mobile ground-based sensor nodes (SNs), Multi-access Edge Computing (MEC) nodes, and UAVs, which will be elaborated further in the next section. Our network model leverages Open Radio Access Network (O-RAN) to enhance connectivity and communication between ground-level SNs, MECs, and UAVs. This integration optimizes data collection and transmission, increasing network efficiency, performance, and reliability [9], [10]. This paper has the following main contributions:

- We integrate O-RAN-enabled UAVs into the target-tracking system to optimize communication among ground-level SNs, MECs, and UAVs for enhanced network efficiency and reliability.
- We introduce an Enhanced Multi-Agent Q-Learning (E-MAQL)-based target-tracking algorithm utilizing UAVs, primarily focusing on enhancing accuracy and minimizing energy consumption within urban environments. This approach leverages Q-Learning (QL) to improve tracking efficiency in dynamic urban landscapes, addressing challenges such as obstacles and varied target trajectories.
- We develop a robust security framework comprising three integral components: an Deep Q-Network-based Intrusion Detection System (DQN-based IDS), the Advanced Encryption Standard (AES) protocol, and a LightWeight AES (LW-AES) protocol to ensure secure communication within the network. This framework prioritizes data integrity, authenticity, and confidentiality, implementing measures such as encryption and authentication to fortify the network against potential security threats.
- We assess the effectiveness of our proposed E-MAQL algorithm and security framework through multiple metrics including accuracy of target-tracking, accuracy of the security framework, power consumption, latency and False Positive Ratio (FPR).

The rest of the paper is structured as follows: Section II presents our proposed target-tracking architecture in O-RAN. It also outlines the threat model and security requirements. Section III presents proposed algorithms for E-MAQL, IDS, AES, and LW-AES. Section IV outlines how the performance of this work was evaluated using experimental results. Finally, Section V provides a conclusion and proposes outlooks.

II. Target-tracking Architecture in O-RAN

This section introduces the seamless integration of O-RAN-enabled UAVs within the target-tracking system.

A. Proposed System Model

The system aims to efficiently track moving ground targets, like vehicles, within urban environments, utilizing components such as mobile SNs, UAVs, MEC nodes, and intelligent controllers. As illustrated in Fig. 1, these components are interconnected within the O-RAN architecture, forming a robust network structure. The O-RAN deployment includes a microcell base station (mBS) and a network of MECs and small-cell base stations, enhancing network coverage and efficiency for optimal target tracking in urban environments. Communication occurs wirelessly through cellular networks technologies like LTE/5G and dedicated radio links, enabling seamless connectivity and efficient data exchange. This comprehensive architecture ensures smooth communication and collaboration, facilitating efficient data flow and robust decision-making capabilities. At its core, the O-RAN infrastructure acts as a backbone, managing communication channels among UAVs, MEC nodes, mobile SNs, and other network elements. Strategically positioned on the urban area, mobile SNs play a pivotal role in collecting real-time data on target movements. Utilizing the O-RAN's capabilities, these SNs swiftly detect specific targets, such as vehicles requiring monitoring, and relay their precise locations in real-time via messaging protocols. MEC nodes serve as intermediaries, facilitating seamless data exchange between SNs, UAVs, and the O-RAN infrastructure. MEC nodes analyze the data acquired from SNs and, taking into account the geographical location of the target node, choose an optimal set of UAVs for tracking. In this process, MECs assess factors such as the proximity of UAVs to the target and the remaining battery power of each UAV, ensuring efficient and effective tracking operations. The MEC nodes has a pivotal role in enhancing real-time decision-making and reducing latency by processing critical data closer to its source. Meanwhile, UAVs dynamically navigate the airspace to track the target, receiving instructions from MECs to optimize routes and collaboratively enhance tracking accuracy.

In scenarios where a mobile target traverses a predefined path on the ground, coordination between SNs, MECs, and UAVs is vital for tracking its trajectory

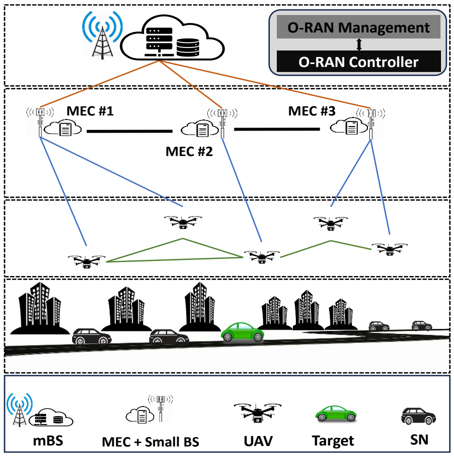

Fig. 1. O-RAN-based System Model.

effectively. As UAVs commence tracking, they continuously monitor the target's movements, dynamically adjusting their positions to maintain surveillance. Utilizing advanced sensing technologies, UAVs capture relevant data points and relay them to MECs for analysis, while bidirectional communication with MEC nodes enables UAVs to receive updates and adjust trajectory parameters as needed.

Moreover, UAVs monitor power levels to ensure uninterrupted operations, signaling MEC nodes when thresholds are reached for proactive management and seamless transitions. Secure communication among entities—MEC-UAV, UAV-UAV, and MEC-MEC—is essential to safeguard data integrity and confidentiality from potential threats. Robust encryption, authentication, and intrusion detection systems are crucial for maintaining the dependability of the target-tracking system amidst dynamic environments.

B. Threat Model

In our UAV-based target-tracking system, we address a threat model where adversaries attempt to compromise tracking integrity by injecting false data into the network. Here, attackers aim to deceive the system by transmitting inaccurate location information or other falsified data, leading to erroneous tracking results and potential disruptions. The adversaries' goal is to undermine tracking accuracy and reliability without directly interfering with infrastructure or communication channels.

C. Security Requirements

Based on the outlined threat model, it is imperative to adhere to several security requirements to uphold the integrity and confidentiality of data exchange. These requirements encompass:

- **Secure Communication:** Implementing secure communication protocols among all parties involved, to prevent unauthorized access, data interception, or tampering.
- **Authentication:** Implementing robust authentication methods to verify the identities of communicating parties, preventing unauthorized entities from gaining access to the network.
- **Intrusion Detection:** Deploying intrusion detection systems to monitor network traffic and detect any suspicious or malicious activities, enabling timely responses to potential security threats.

By adhering to these security requirements, the target-tracking system can effectively mitigate potential security risks and ensure the reliability and trustworthiness of its operations.

III. The Proposed Algorithms

This study focuses on securing target-tracking using UAVs, MECs, and SNs within the O-RAN network architecture. Our main objective is to ensure precise tracking despite potential inaccuracies from faulty sensors or malicious data tampering. Considering the power limitations of UAVs, we also prioritize energy-efficient tracking methods.

In response to the above mentioned challenges, we propose a target-tracking approach that leverages the MAQL algorithm, considering both accuracy and UAV power constraints. Additionally, we integrate a security framework into our target-tracking algorithm, incorporating Lightweight Advance Encryption Standard (LW-AES) protocol and an IDS within the O-RAN architecture. This holistic approach addresses the dual objectives of achieving precise tracking while safeguarding against security threats. In the following sections, we comprehensively explain our MAQL-based algorithm for target-tracking. Additionally, we delve into the details of our security framework, which hinges on utilizing AES encryption and IDS technology. By elaborating on these components, we aim to thoroughly understand how our proposed approach effectively addresses the challenges of accurate target-tracking while ensuring robust security within the O-RAN framework.

A. Enhanced MAQL-based Algorithm (E-MAQL)

We aim to extend the research outlined in [11], which employed the standard Q-learning algorithm for target-tracking. In [11], a challenge exists where the utilized algorithm led to a zig-zag movement pattern for the UAVs, resulting in increased power consumption. To address this issue effectively, the current research endeavors to enhance the algorithm's performance and mitigate the occurrence of zig-zag

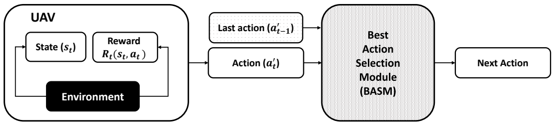

Fig. 2. E-MAQL Algorithm.

movement. By refining the algorithm used in [11], the aim is to achieve smoother UAV trajectories and optimize power utilization for more efficient target-tracking operations.

Q-learning operates within the Markov Decision Processes (MDPs) framework, as described in [12]. Within this framework, decisions are made based on the current state. Like other reinforcement learning algorithms, Q-learning considers the current state and selects the following possible action accordingly. Since targets can change direction continuously, UAVs must adjust their direction accordingly to track the target accurately. This dynamic nature often results in UAVs exhibiting a zig-zag movement pattern, leading to increased energy consumption and inefficiencies in monitoring performance.

As mentioned above, we have enhanced the algorithm used in [11] by incorporating additional considerations beyond the current state and subsequent action. Specifically, we now also consider the last action taken by the UAVs. This enhancement enables the algorithm to anticipate better and adapt to changes in the target's movement, thereby improving the efficiency and accuracy of the tracking process. By integrating this modification, we aim to mitigate the zig-zag movement pattern observed in previous iterations of the algorithm, ultimately enhancing the overall performance of our target-tracking system. Fig. 2 illustrates the E-MAQL based on this strategy.

B. Our Security Framework: DQN-based IDS and LW-AES

This section presents our security enhancement framework tailored for O-RAN-enabled UAVs within the target-tracking system developed in this study. Our framework comprises three primary components: an IDS, AES, and LW-AES. Using the AES and LW-AES protocols, we aim to ensure network security through IDS implementation and secure communication between UAV-UAV, MEC-UAV, and MEC-MEC interactions. As depicted in Fig. 3, we implement a centralized DQN-based IDS within the Near-RT RIC, utilizing AES for ensuring secure MEC-MEC communication, and LW-AES for securing UAV-UAV and MEC-UAV communications. We elaborate on each component in the subsequent sections:

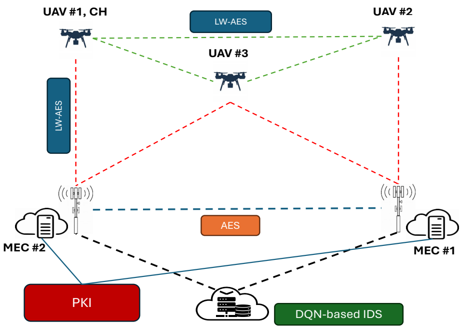

Fig. 3. High-level of Our Security Framework.

*1) **The Proposed DQN-based IDS:*** Today, UAVs are increasingly utilized in various applications, including target-tracking systems. However, the vulnerability of UAV networks to cyber-attacks poses significant security challenges. We propose a DQN-based IDS designed for O-RAN-enabled UAV networks to address this. The proposed IDS operates within the Near-RT RIC framework, which serves as a centralized intelligence hub for managing and optimizing radio resources in UAV networks. Leveraging the capabilities of the RIC, our IDS uses DQN techniques to detect and mitigate potential intrusions in real time. This integration enables seamless coordination between network management and security functions, facilitating proactive threat response and ensuring the integrity of UAV operations.

Traditional rule-based IDS systems rely on predefined signatures and heuristic rules to identify known attack patterns. However, these approaches could be improved in adapting to evolving threat landscapes and detecting novel attack vectors. In contrast, our DQN-based IDS takes a dynamic and adaptive approach to intrusion detection, autonomously learning from network data to identify abnormal behavior indicative of security threats.

Algorithm 1 initializes a replay memory D to store experiences, sets up two Q-networks with random weights θ (the main Q-network) and θ' (the target Q-network), and initializes a feature selection algorithm. It then proceeds to train the DQN-based IDS over a fixed number of episodes (M), where the IDS interacts with the environment representing the monitored network for intrusions. At each episode's start, network features are collected to form the initial state s_1. During action selection at each time step within the episode, the IDS chooses an action a_t using an ϵ-greedy policy, balancing exploration and exploitation. This action corresponds to the IDS's decision on normal network activity or potential in-

Algorithm 1: DQN-based IDS with Feature Selection

```
Input: Network features, Replay memory capacity $N$, Number of episodes $M$, Maximum timestep $T$, Exploration parameter $\epsilon$, Discount factor $\gamma$, Update frequency $C$
Initialize replay memory $D$ to capacity $N$
Initialize Q-network with random weights $\theta$
Initialize target Q-network with weights $\theta' \leftarrow \theta$
Initialize feature selection algorithm (e.g., information gain)
for episode $= 1$ to $M$ do
    Initialize state $s_1$ by collecting network features
    for timestep $= 1$ to $T$ do
        Select action $a_t$ using $\epsilon$-greedy policy based on $Q(s_t, a; \theta)$
        Execute action $a_t$ and observe reward $r_t$ and new state $s_{t+1}$
        Preprocess $s_{t+1}$ to extract relevant features $f_{t+1}$
        Store transition $(s_t, a_t, r_t, s_{t+1})$ in $D$
        Sample random minibatch of transitions $(s_j, a_j, r_j, s_{j+1})$ from $D$
        Calculate target values $Q_{\text{target}} = r_j + \gamma \max_{a'} Q(s_{j+1}, a'; \theta')$
        Update Q-network parameters by minimizing the loss:
            $\mathcal{L} = \frac{1}{N} \sum_j (Q(s_j, a_j; \theta) - Q_{\text{target}})^2$
        Every $C$ steps, update target Q-network: $\theta' \leftarrow \theta$
    end for
    Update feature selection algorithm with observed states and rewards
end for
Output: Trained Q-network with weights $\theta$
```

trusion. After executing the selected action, resulting in a reward r_t and a new state s_{t+1}, the new state is preprocessed using a feature selection algorithm to extract relevant features f_{t+1} capturing crucial network behavior. These features are essential for optimizing tracking accuracy and operational efficiency in the target-tracking system. The algorithm then stores the transition (s_t, a_t, r_t, s_{t+1}) in the replay memory D, samples a random minibatch of transitions from D for training, calculates the target Q-values Q_{target}, and updates the Q-network parameters to minimize the loss function $\mathcal{L}$. Periodic updates of the target Q-network parameters θ' ensure alignment with the main Q-network θ. After each episode, the feature selection algorithm adapts the selected features based on observed states and rewards to enhance intrusion detection effectiveness.

*2) **AES with PKI**:* Our target-tracking system implements AES protocol for secure communication between MEC nodes (MEC-MEC). This setup is fortified by a robust PKI and an advanced session key generation mechanism, ensuring data transmission security. AES operates as a symmetric encryption algorithm, necessitating both MECs to possess a shared secret key for encryption and decryption. To establish secure communication channels, we adopt a hybrid encryption approach, combining AES with asymmetric encryption from PKI. The process begins with initiating a communication session, where the initiating node generates a temporary session key (K) using a cryptographic pseudorandom number generator (CSPRNG). This key is unpredictably generated and of a predetermined length. The initiating MEC node encrypts K using the recipient's public key (PK_r) from PKI, typically with an algorithm like RSA. The encrypted session key (K) and other necessary parameters are then transmitted to the recipient MEC node. Upon receipt, the recipient decrypts K using its private key (SK_r), ensuring only the intended recipient accesses the session key. With the session key exchanged, both MEC nodes utilize AES encryption for their communication, ensuring confidentiality and integrity of the exchanged data.

*3) **LightWeight AES (LW-AES)**:* In this section, we detail the utilization of a lightweight version of the AES in conjunction with the EAX mode for ensuring secure UAV-UAV and UAV-MEC communications where EAX is a block-cipher mode of operation for solving the problem of Authenticated-Encryption with Associated-Data (AEAD) [13]. The LW-AES algorithm is optimized for efficient encryption and decryption operations on resource-constrained devices such as UAVs.

Considering the diverse array of sensors integrated into UAVs, leading to varying data lengths, it is clear that a flexible mode capable of accommodating dynamic data can be more suitable. In light of this requirement, the EAX mode is selected because of the adaptability to handle data of varying lengths efficiently. As an online algorithm, EAX processes data in real-time without prior knowledge of the data length. It operates seamlessly with inputs such as a nonce (N) of any length, a header (H) with variable length, and a message (M) with variable length. EAX ensures the confidentiality of M and the authenticity of both M and H, making it an ideal choice for securing communication in UAV networks where data lengths may vary unpredictably [14].

To utilize the EAX mode for AES encryption, we divide it into two main components: the encryp-

Algorithm 2: Encryption Algorithm

```
**Input:** $Key, H, N, M$
$CT \leftarrow$ BlockCipher$(EAX_{Enc}, Key, N) \oplus M$
$\tau \leftarrow$ MAC$(CT, H)$
**Output:** $CT, \tau$
```

Algorithm 3: Decryption Algorithm

```
**Input:** $Key, H, N, CT, tau$
$M \leftarrow$ BlockCipher$(EAX_{Dec}, Key, N) \oplus CT$
$\tau' \leftarrow$ MAC$(CT, H)$
**if** $\tau' \neq \tau$ **then**
    **Error:** Authentication failed
**end if**
**Output:** $M$
```

tion function (EAX_{Enc}) and the decryption function (EAX_{Dec}). The encryption function EAX_{Enc} operates as a symmetric encryption algorithm, typically employing AES, denoted as $EAX_{Enc} : Key \times \{0,1\}^n \rightarrow \{0,1\}^n$. It takes a key (of length n) and a plaintext block as inputs and produces a ciphertext block of the same length. Similarly, the decryption function (EAX_{Dec}) reverses this process, decrypting ciphertext blocks back to their original plaintext form. Additionally, the EAX mode incorporates a tag length parameter (τ) denoted as $\tau \in [0 \cdots n]$, which determines the length of the authentication tag generated during encryption. This tag serves to ensure the integrity and authenticity of the encrypted data and is typically chosen to be between 0 and the block size n of the block cipher.

These parameters, EAX_{Enc}, EAX_{Dec}, and τ, are chosen before initiating a specific session that will employ the EAX mode. It's crucial to fix these parameters consistently across all participants in the communication session to ensure interoperability and security.

In the context of secure communication between two UAVs, the EAX mode scheme denoted as $EAX[EAX_{Enc}, EAX_{Dec}, \tau]$. This scheme ensures both the confidentiality and authenticity of the transmitted data. The encryption algorithm operates with the signature $Key \times H \times N \times M \rightarrow CT$. Upon receiving the ciphertext, the decryption algorithm, with the signature $Key \times H \times N \times CT \rightarrow M$ verifies the authenticity of the ciphertext and recovers the original plaintext message where Key is the shared secret key known only to the communicating UAVs. Here, N, H, M, and CT represent binary strings $\{0,1\}^*$, with N as the nonce, H as the header, M as the message, and CT as the resulting ciphertext.

In Algorithm 2 and 3, the Message Authentication Code (MAC) used in the EAX mode algorithm is a cryptographic hash function applied to the ciphertext and the header. It ensures the integrity and authenticity of the ciphertext and the associated header. In EAX mode, the MAC is computed using a secure cryptographic hash function, such as Hash-based Message Authentication Code (HMAC), to generate a fixed-size tag based on the input data. This tag is then used to verify the integrity of the received ciphertext and header during decryption. If the computed tag matches the received tag, it confirms that the ciphertext and header have not been tampered with, assuring the message's integrity and authenticity.

IV. Numerical Results

This section presents simulation results for our target-tracking system, evaluating tracking accuracy, UAV power consumption, latency, and security framework resilience.

A. Dataset Description and Preprocessing

The dataset is generated by simulating the movement of UAVs and the target in a virtual environment using MATLAB. Trajectories of the UAVs and the target are recorded over time, capturing their positions and velocities at regular intervals. The attacker UAV injects false location data into the network by broadcasting incorrect position information. In the preprocessing stage, several steps are undertaken to prepare the dataset for training the DQN-based IDS: (I) Normalization is applied to ensure uniform scaling of the trajectories and velocities of the UAVs across different features. (II) Relevant features, such as the positions and velocities of the UAVs, are extracted from the dataset to construct the input features for the IDS. Each data point in the dataset is then labeled based on whether it represents normal behavior or an attack by the malicious UAV. Subsequently, the dataset is partitioned into training and testing sets to assess the IDS's performance. (III) A portion of the dataset is allocated for testing the IDS's robustness against false data injection.

B. Simulation Setup

We conducted simulations using MATLAB on a laptop with an 11th Gen Intel(R) Core(TM) i7-1165G7 processor and 16.0 GB of RAM to evaluate a target-tracking system employing the E-MAQL algorithm. The system includes one target and multiple UAVs tracking it, along with two MEC nodes and 10 SNs deployed in an environment featuring 100 cylindrical obstacles. The UAVs' speed ranges from 0 to 5 m/s, while the target's trajectory spans from coordinates

TABLE I
SIMULATION SETUP PARAMETERS

Parameter	Value
Number of UAVs	2 - 4
Number of MECs	2
Number of SNs	10
Target Start Coordinates	(10,60)
Target End Coordinates	(300,150)
Number of Obstacles	100
UAV Speed Range	0 - 5 m/s
Target Average Velocity	3 m/s
Action Space for UAVs	8
UAV Mass	4kg

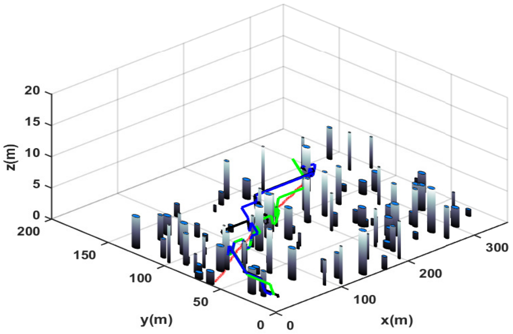

Fig. 4. The 3D urban environment with obstacles.

(10,60) to (300,150), with an average speed of 3 m/s. Each UAV weighs 4kg, and the E-MAQL algorithm operates with an action space of 8 distinct actions. In a threat scenario, one UAV acts as an attacker aiming to inject falsified data, threatening network integrity. Additionally, we compared the system's performance under two network architectures: traditional RAN, characterized by a monolithic structure, and O-RAN, featuring distributed architecture with virtualized MEC nodes. Table I presents the parameters used in the simulation setup.

To implement the DQN-based IDS, we utilized the TensorFlow framework for its robust features in constructing and training deep learning models. Additionally, for AES and LW-AES encryption in MATLAB, we employed the Java libraries `javax.crypto.Cipher` and `javax.crypto.spec.SecretKeySpec`.

C. Performance Results

To assess the accuracy of the proposed E-MAQL algorithm in the target-tracking system, we investigated the impact of varying the number of UAVs on system performance and resource allocation. We conducted a thorough evaluation under different configurations, utilizing 2, 3, and 4 UAVs for tracking a target along a specified trajectory (see Fig. 4). This analysis offers insights into how our system adapts to different team sizes and assesses scalability and effectiveness. For statistical robustness, we averaged localization error over 100 Monte Carlo experiments.

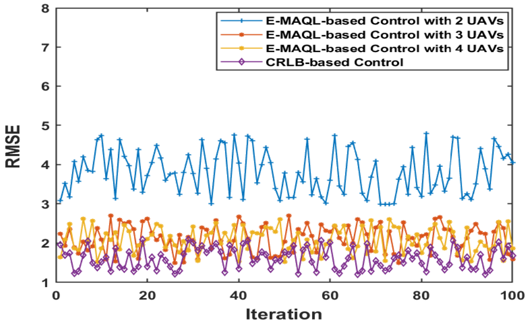

Fig. 5. Comparison of RMSE between the CRLB-based control and E-MAQL with 2, 3, and 4 UAVs across 100 Monte Carlo experiments.

Fig. 5 depicts the Root Mean Square Error (RMSE) between the actual location value and the prediction made from the proposed E-MAQL during target-tracking. We conducted a comparative analysis, benchmarking our E-MAQL control approach against a Cramér-Rao Lower Bound (CRLB)-based method. Notably, the RMSE of the CRLB-based control consistently decreases faster throughout the time steps compared to other methods. This can be attributed to UAVs dynamically adjusting their positions to minimize the CRLB. While RMSE values exhibit slight fluctuations across control schemes, results indicate that E-MAQL-based control with three and four UAVs achieves tracking performance comparable to the optimal CRLB-based control.

$$\text{RMSE} = \sqrt{\frac{1}{T}\sum_{t=1}^{T}(TN_t - \hat{TN}_t)^2} \qquad (1)$$

where TN_t is the actual position of target m at time t, $\hat{TN}_t$ refers to the estimated target position, and T is the total time of target-tracking.

In the target-tracking system, the power consumed by UAVs is a critical challenge owing to their restricted power capacity. Our E-MAQL approach tackles this issue by mitigating the zig-zag movement pattern observed in UAVs during target-tracking, significantly reducing power consumption. This improvement is particularly significant as most UAV power usage is associated with their mobility or flight. To evaluate the effectiveness of E-MAQL, we conducted a comparative analysis with the algorithm used in [11] when employing 3 UAVs for target-tracking.

Fig. 6 compares the average power consumed by UAVs when employing two different algorithms, QL

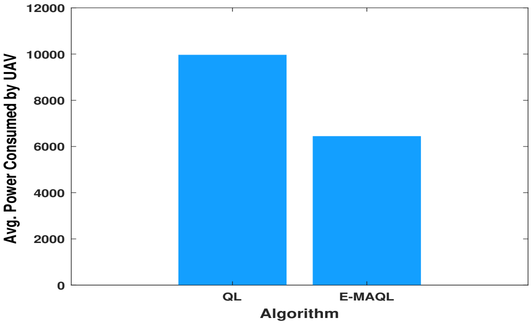

Fig. 6. Comparison of average power consumption by UAVs using QL and E-MAQL algorithms with 3 UAVs.

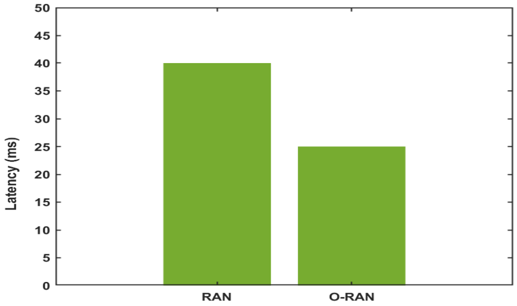

Fig. 7. Comparison of latency between traditional RAN and O-RAN.

and E-MAQL, with a total of 3 UAVs involved in the target-tracking system. This substantial reduction in power consumption observed with E-MAQL highlights its efficiency in optimizing UAV movements during target-tracking. The E-MAQL algorithm mitigates the zig-zag movement pattern typically associated with QL, resulting in smoother and more energy-efficient trajectories for the UAVs. Consequently, this improvement in power consumption with E-MAQL demonstrates its effectiveness in enhancing the energy efficiency of the target-tracking system, contributing to prolonged UAV operation and mission duration.

In our comparative analysis focusing on latency, we evaluated the performance of two network architectures: traditional RAN and O-RAN. Latency encompasses propagation delay, transmission delay, processing delay, and queueing delay. The simulation results demonstrate that O-RAN consistently outperforms traditional RAN in terms of latency across various scenarios. This is mainly because O-RAN's decentralized architecture with distributed radio units (RUs) and virtualized baseband units (BBUs) minimizes propagation delays by reducing data travel distance compared to centralized processing in traditional RAN. In additon, O-RAN's use of open interfaces and standardized protocols optimizes transmission processes, while its flexibility allows for advanced transmission technologies, such as beamforming, further reducing transmission delays. Moreover, O-RAN's virtualized architecture enables efficient processing resource allocation, reducing processing delays compared to fixed-function hardware in traditional RAN. Finally, O-RAN's support for network slicing and edge computing minimizes queueing delays by prioritizing traffic and dynamically allocating resources. Fig. 7 illustrates the latency comparison between traditional RAN and O-RAN, highlighting the significant latency reduction achieved with O-RAN.

TABLE II
PERFORMANCE METRICS OF DQN-BASED IDS

Metric	Value
Precision	76.19%
Recall	80.50%
F-measure	0.78
Accuracy	92.49%

We evaluated the proposed DQN-based IDS by measuring its FPR (see Eq. 2). The recorded FPR for our IDS reveals that 6% of the instances flagged as malicious were actually benign. This indicates a 6% chance of the IDS incorrectly identifying normal behavior as an attack. While a lower FPR is preferred to reduce false alarms and enhance system efficiency, the 6% FPR suggests that the IDS effectively distinguishes between normal and malicious behavior. However, there is still room for improvement in the IDS algorithm to minimize false positives and improve accuracy in detecting genuine threats while keeping false alarms to a minimum. Further analysis and refinement of the IDS model may be necessary to optimize its performance and achieve a lower FPR.

$$\text{FPR} = \frac{FP}{FP + TN} \tag{2}$$

where FP represents the number of false positives (instances incorrectly classified as attacks), and TN represents the number of true negatives (instances correctly classified as non-attacks).

The performance of our IDS is assessed based on four crucial classification metrics: Accuracy, Precision, Recall, and F1-score. Table II illustrates the recorded values for the total instances, where 1042 instances were considered. Among these, 800 instances were allocated for training, 200 for testing, and 52 were identified as false data instances.

To evaluate the efficacy of the proposed security framework, encompassing IDS, AES, and LW-AES, we conducted comprehensive tests to measure the accuracy of the target-tracking system across various scenarios. These assessments were crucial for understanding the system's performance in the presence of attackers who injected false data into the network. To this end, we measured the accuracy of target-tracking both with and without the presence of attackers (see Eq. 3). Without any attackers, the accuracy of the tracking system is notably high, at 95%, indicating its robust performance under normal conditions. However, when one UAV acts as an attacker, the accuracy drops to 53%, demonstrating malicious entities' disruptive impact on the tracking system. With two UAVs as attackers, the accuracy decreases further to 41%, highlighting the compounding effect of multiple attackers on system performance.

Our deployed security framework effectively mitigated attackers' impact, notably improving tracking accuracy. In scenarios with one UAV acting as an attacker, accuracy increased to 86%, showcasing the framework's effectiveness. With two UAVs as attackers, accuracy further rose to 80%, highlighting the robustness and reliability of our security measures in enhancing the target-tracking system.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

where TP represents the number of true positives (instances correctly classified as attacks), TN represents the number of true negatives (instances correctly classified as non-attacks), FP represents the number of false positives (instances incorrectly classified as attacks), and FN represents the number of false negatives (instances incorrectly classified as non-attacks).

V. Conclusion

In this study, we developed E-MAQL, an algorithm enhancing target-tracking accuracy while minimizing energy usage. Additionally, we introduced a comprehensive security framework for secure target-tracking with UAVs in urban environments within the O-RAN architecture. Our framework integrates IDS and secure communication protocols like AES and LW-AES to mitigate threats such as data manipulation and communication interference. Through extensive simulations, we validated our approach's effectiveness in ensuring data integrity, authenticity, and confidentiality between UAVs and ground-based entities like MEC nodes. Our experiments demonstrated the framework's robustness against false data injection attacks, showcasing significant improvements in accuracy and FPR. These findings underscore the importance of proactive security measures in UAV-based communication systems within the O-RAN architecture, fostering advancements in secure target-tracking technologies.

Acknowledgment

This work was partially supported by Horizon Europe Marie Skłodowska-Curie Actions under the project TRACE-V2X (grant agreement ID 101131204) and by the U.K. Department for Science, Innovation, and Technology under Projects 5G MoDE (Mobile oRAN for highly Dense Environments) and HiPer-RAN (Highly Intelligent, Highly Performing RAN).

References

[1] L. Zhou, S. Leng, Q. Liu, and Q. Wang, "Intelligent UAV swarm cooperation for multiple targets tracking," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 743–754, 2021.

[2] T. Keawboontan and M. Thammawichai, "Towards real-time UAV multi-target tracking using joint detection and tracking," *IEEE Access*, 2023.

[3] B. Li, Z.-p. Yang, D.-q. Chen, S.-y. Liang, and H. Ma, "Maneuvering target tracking of uav based on mn-ddpg and transfer learning," *Defence Technology*, vol. 17, no. 2, pp. 457–466, 2021.

[4] M. Doostmohammadian, A. Taghieh, and H. Zarrabi, "Distributed estimation approach for tracking a mobile target via formation of uavs," *IEEE Transactions on Automation Science and Engineering*, vol. 19, no. 4, pp. 3765–3776, 2021.

[5] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," *Computer Networks*, vol. 224, p. 109626, 2023.

[6] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. Al Ridhawi, "Lightweight ids for UAV networks: A periodic deep reinforcement learning-based approach," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021, pp. 1032–1037.

[7] X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, "CGAN-based collaborative intrusion detection for uav networks: A blockchain-empowered distributed federated learning approach," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 120–132, 2022.

[8] H. Luo, Y. Wu, G. Sun, H. Yu, and M. Guizani, "Escm: an efficient and secure communication mechanism for UAV networks," *IEEE Transactions on Network and Service Management*, 2024.

[9] "O-RAN alliance, O-RAN.WG11.Security-Near-RT-RIC-xApps-TR.0-R003-v05.00," Tech. Rep., February 2024, r003.

[10] "O-RAN alliance, O-RAN.WG11.Security-Protocols-Specification.O-R003-v08.00," Tech. Rep., February 2024, r003.

[11] S. A. Soleymani, S. Goudarzi, X. Liu, L. Mihaylova, W. Wang, and P. Xiao, "Multi-target tracking using a swarm of uavs by Q-learning algorithm," in *2023 Sensor Signal Processing for Defence Conference (SSPD)*. IEEE, 2023, pp. 1–5.

[12] Y.-J. Chen, D.-K. Chang, and C. Zhang, "Autonomous tracking using a swarm of uavs: A constrained multi-agent reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 702–13 717, 2020.

[13] M. Bellare, P. Rogaway, and D. Wagner, "The EAX mode of operation," in *Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*. Springer, 2004, pp. 389–407.

[14] N. Cecchinato, A. Toma, C. Drioli, G. Oliva, G. Sechi, and G. L. Foresti, "Secure real-time multimedia data transmission from low-cost UAVs with a lightweight aes encryption," *IEEE Communications Magazine*, vol. 61, no. 5, pp. 160–165, 2023.