Deep Learning for Secure UAV-Assisted RIS Communication Networks

Umair Ahmad Mughal, *Student Member, IEEE*, Yazeed Alkhrijah, *Member, IEEE*, Ahmad Almadhor, and Chau Yuen, *Fellow, IEEE*

***Abstract*—Reconfigurable intelligent surfaces (RIS) represent an important advancement in metamaterial technology, enabling the control of electromagnetic waves to enhance wireless communications. However, integrating RIS with unmanned aerial vehicles (UAVs) introduces potential vulnerabilities that can significantly impact network performance. This research investigates the complexity of securing UAV-assisted RIS systems for next-generation communication networks. We present a deep machine learning framework, Long Short-Term Memory Deep Deterministic Policy Gradient (LSTM-DDPG), to robustly address security concerns and ensure reliable communication within UAV-assisted RIS networks by countering malicious threats. Simulation results confirm the efficacy of combining UAVs, RIS, and deep learning to mitigate attacks on UAV-RIS communication, with notable improvements compared to other baseline approaches. Finally, we discuss open research challenges and future directions in this rapidly progressing field.**

***Index Terms*—UAV, RIS, intrusion detection systems, LSTM, DDPG**

I. Introduction

The evolution of next-generation networks is set to reshape mobile networking through the integration of distributed network intelligence and the facilitation of sophisticated spectrum coexistence between an array of passive and active radio services. Unmanned Aerial Vehicles (UAVs), with their unique attributes such as enhanced positioning freedom, trajectory control, cost-effective deployment, and maintenance, along with the capability to establish unobstructed line-of-sight (LoS) links, are expected to be instrumental in the advancement of 5G and forthcoming communication and networking technologies [1].

In the context of the Third Generation Partnership Project (3GPP), UAVs can operate in various roles such as an aerial base station (ABS), an aerial relay (AR), or aerial user equipment (AUE). A variety of use cases have been identified for UAV-assisted wireless networks, promising significant enhancements in throughput, security, and reliability [2].

Emerging in this technological landscape is the concept of Reconfigurable Intelligent Surface (RIS), a transformative technology capable of creating novel wireless transmission patterns and controlling the communication channel. Comprising electronically tunable and energy-efficient analog processing elements, a RIS can manipulate various properties of passive reflecting elements in real time. This ability to control the direction of incident electromagnetic signals optimizes the effective channel gain [3]. The versatility of RIS allows its deployment on diverse surfaces, including buildings, vehicles, and indoor walls, with minimal expense and effort [4]. RISs are expected to see widespread use in the future, particularly in the enhancement of wireless or cellular communications, as demonstrated by their promising performance in various studies, including [5]. These surfaces can be installed on building facades and roadside billboards to passively enhance the radio propagation environment. This augmentation aims to improve communication link conditions and boost data rates. Recognizing the potential of RISs, it is both wise and essential to incorporate them into the design of UAV communication systems to develop resilient and forward-looking technical solutions.

RISs and UAVs hold the promise of playing a crucial role in fortifying cybersecurity within various scenarios such as vehicular-to-everything (V2X) communication, public safety networks, and Internet of things (IoT) networks. Intelligent reflectors, when employed as RISs, can enhance wireless communication and broaden network coverage. Through astute manipulation of the propagation environment, RISs can effectively alleviate signal interference, enhance signal quality, and bolster the overall reliability and security of UAV-assisted RIS communications. This capability proves especially valuable in V2X communication, public safety networks, and IoT networks, where numerous interconnected devices heighten vulnerability to potential attacks and security breaches [6]. Conversely, UAVs can function as mobile sensing and monitoring platforms within UAV-assisted RIS communication networks. They can integrate various sensors, cameras, and communication modules to identify and counteract cybersecurity threats. UAVs actively patrol designated areas of V2X networks, public safety networks, and IoT networks, recognizing anomalies and gathering real-time data on potential security breaches. Furthermore, UAVs play a role in swiftly implementing security measures in response to emerging threats,

U. A. Mughal is with the Department of Computer Science, College of Engineering, Tennessee Tech University, Cookeville, TN, 38501, USA (email: uamughal42 @tntech.edu)

Y. Alkhrijah is with the Department of Electrical Engineering, College of Engineering, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11564, Saudi Arabia. (email: Ymalkhrijah@imamu.edu.sa)

A. Almadhor is with the Department of Computer Engineering and Networks, College of Computer and Information Sciences, Jouf University, Saudi Arabia. (email: aaalmadhor@ju.edu.sa)

C. Yuen is with the School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Ave, Singapore (email: chau.yuen@ntu.edu.sg)

This research is supported by the Ministry of Education, Singapore, under its MOE Tier 2 (Award number MOE-T2EP50220-0019). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the Ministry of Education, Singapore.

including the deployment of RISs to fortify network security and resilience.

The combination of RISs and UAVs in V2X networks, public safety networks, and IoT networks offers several advantages for cybersecurity. Firstly, RISs contribute to enhanced signal coverage and quality, thereby reducing the vulnerability of devices to unauthorized access or malicious interference. Secondly, UAVs function as agile and adaptable security agents, capable of promptly identifying and responding to security threats in real time. They excel at conducting surveillance, detecting intrusions, and deploying countermeasures to safeguard the integrity of RIS-assisted networks. Lastly, the mobility and flexibility of UAVs enable them to effectively address security challenges in diverse and dynamic environments such as V2X networks, public safety networks, and IoT networks including remote or hard-to-reach locations. The integration of RISs and UAVs in dynamic environments such as V2X networks, public safety networks, and IoT networks holds significant potential for strengthening cybersecurity. RISs improve wireless communication and network coverage, while UAVs provide mobile sensing and monitoring capabilities. Together, they enhance threat detection, response time, and overall network security, thereby contributing to the protection of devices and data from cyber threats.

The UAV-assisted RIS offers a comprehensive analysis of the environment to ensure the efficient safeguarding of an extensive perimeter. It performs surveillance in areas susceptible to threats, dynamically adjusting its surface orientation to limit coverage in non-critical zones. Emphasizing security and reliability as primary considerations, we have incorporated these fundamental aspects into the design of the UAV-assisted RIS wireless network, proposing potentially effective solutions. Figure 1 illustrates the specified reliability and security requirements for the UAV-assisted RIS.

The combination of RIS and UAV technologies can profoundly enhance multiple aspects of communication and networking, from network coverage to massive multiple access, and physical layer security [2]. However, as we explore these applications, we must consider the potential vulnerabilities that could be exploited by malicious actors and lead to various types of cyber attacks. The normal operation scenario of the RIS-aided UAV is presented in Fig. 2a. However, the ability to program the wireless channel offered by RIS has its downside. While it can enhance the resilience and dependability of next-generation wireless networks, it also opens up potential avenues for launching destructive over-the-air attacks. The affordability and low-power consumption of RISs make it possible to deploy illegitimate devices or compromise genuine ones.

Motivated by the aforementioned challenges, this paper suggests a secure and efficient deep machine learning framework designed for UAV-assisted RIS communication. The proposed framework aims to ensure secure communication in dynamic practical environments such as V2X communication, public safety, and IoT networks.

The notable contributions of this article are emphasized as follows.

- This paper delves into the potential adversarial implications of integrating RIS with UAV communication frameworks. We examine a variety of RIS-assisted attacks, including those previously discussed in the literature [3], [4] and potential new threats. From the perspective of an attacker, we explore the characteristics of RIS that render it susceptible to adversarial misuse and consider potential countermeasures.
- We present the LSTM-DDPG framework designed for secure communication in UAV-assisted RIS communication. The LSTM-based actor-network and critic network are meticulously developed to capture temporal correlations in state features, thereby improving the overall state representation capability.
- Simulation results indicate that the proposed LSTM-DDPG algorithm exhibits strong convergence performance and surpasses state-of-the-art methods in terms of training time, energy consumption, and security.

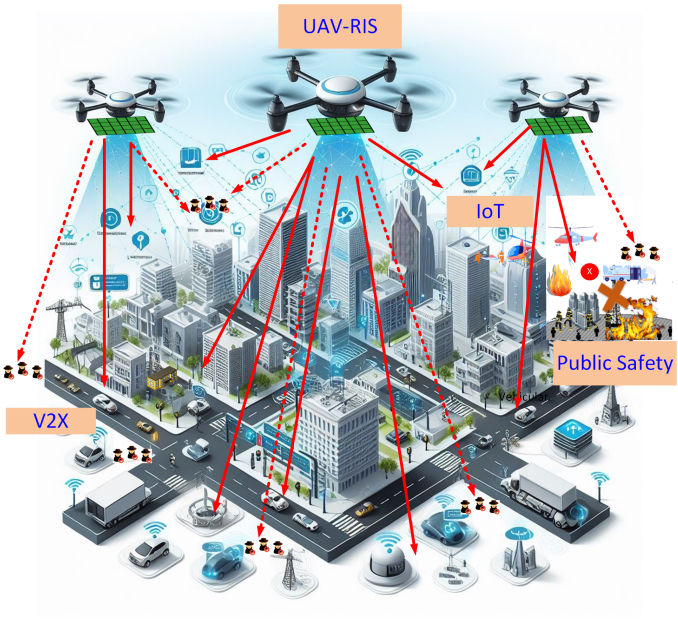
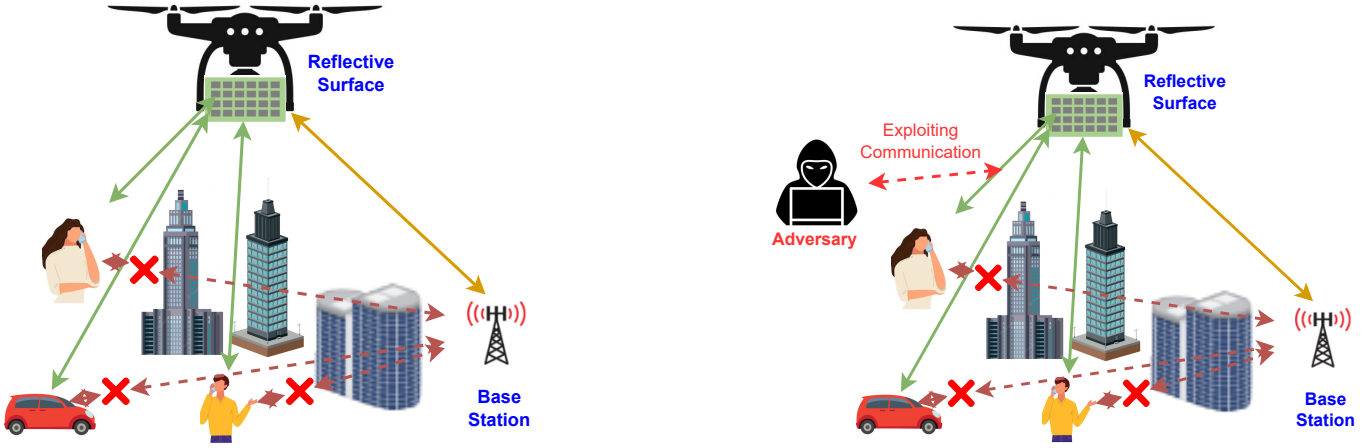


Figure 1. UAV-assisted RIS: Ensuring secure and reliable perimeter protection.

II. RIS-Enabled UAV Communications: Applications and Security Implications

A. Extended Coverage through UAV-assisted RIS Communications

UAVs fitted with Intelligent Omni-surfaces (IOS), a variant of RIS, can extend coverage and enhance spectral efficiency in cellular networks. With the ability to control signal direction without blind spots, the IOS can extend the signal reach of a base station into dead zones, providing 360-degree coverage. Despite these advantages, this setup is susceptible to spoofing attacks [5]. A malicious actor could utilize a rogue UAV-assisted RIS setup to redirect communication, potentially creating network disruption or intercepting sensitive data.



(a) Normal operation

(b) Under adversarial exploitation

Figure 2. UAV-assisted RIS communication

B. Increased Capacity via UAV-assisted RIS Communications

UAV-assisted RIS systems can significantly improve network throughput and capacity. By controlling the phase shifts of the RIS elements, the system can cancel interference, assuming known Channel State Information (CSI) at the RIS controller. Despite these advantages, this scenario also presents a potential avenue for jamming attacks as shown in Fig. 2b.

C. Massive Multiple Access through UAV-assisted RIS Communications

UAV-assisted RIS systems can address the massive access challenges posed by the growing number of IoT devices. By steering indoor wireless channels in favor of specific users, these systems can enhance system capacity [7]. Yet, they are vulnerable to DoS attacks, where an attacker could potentially overload the network with illegitimate access requests, causing service disruptions.

D. Spectrum Sharing in UAV-assisted RIS Communications

RIS technology can enable efficient spectrum sharing by reducing interference. However, this feature presents an opportunity for adversaries to launch spoofing attacks. An attacker could manipulate the RIS phase shifters to disrupt the network's spectrum sharing, causing interference and affecting network performance.

E. Physical Layer Security (PLS) in UAV-assisted RIS Communications

UAV-assisted RISs can improve the PLS of terrestrial cellular networks by establishing dominant Line-of-Sight (LoS) links between aerial and ground nodes. However, the same LoS advantage could be exploited by eavesdroppers to intercept data. The RIS could also be manipulated to create a destructive reflected signal, diminishing the received SNR at specific locations and limiting eavesdropping chances. Despite these measures, persistent and sophisticated attackers could still find ways to compromise these systems, underscoring the need for robust security protocols.

III. Potential Vulnerabilities and Attacks in UAV-Aided RIS-Assisted Systems

Emerging research is illuminating a range of potential attack vectors in Reconfigurable Intelligent Surface (RIS)-assisted communication systems, particularly those involving Unmanned Aerial Vehicles (UAVs). Such attacks take advantage of the unique reflective properties of RIS and can be launched by an adversary who has either compromised an existing RIS controller or deployed their own RIS. Herein, we explore the nature and potential impact of these attacks, drawing upon both existing and emerging research.

A. Signal Cancellation

A signal cancellation attack in a RIS-assisted system doesn't follow the typical approach of a conventional jammer, which seeks to increase interference at the receiver and thereby decrease the signal-to-interference-and-noise ratio (SINR) [8]. Instead, the adversary aims to generate a signal that mirrors the original one in phase but in the reverse direction. This signal, once it reaches the receiver, destructively interferes with the original signal, effectively canceling it out. In a UAV-aided system, the UAV could be manipulated to position the RIS optimally for such an attack, or could itself be used to relay the phase-reversed signal.

B. Exploiting Beamforming

Beamforming is a crucial aspect of coverage in high-frequency systems that utilize large antenna arrays, and in UAV-aided RIS-assisted systems, it is of paramount importance [9]. These systems estimate the appropriate beamforming vectors from the Channel State Information (CSI) derived from transmitted pilot sequences. However, an adversarial RIS could introduce phase manipulations during pilot sequence transmissions, leading to beam vectors calculated from the manipulated CSI. The UAV could be used to transmit these manipulated pilot sequences, thereby disrupting the beamforming process.

C. Exploiting Beam Management

Within analog beamforming systems, such as those applicable in UAV-aided RIS-assisted systems, the transmission beam is derived from a predefined set of beam vectors, as mentioned in [9]. These beam vectors are employed iteratively to scan the cell area. An adversarial RIS possesses the capability to adjust its reflection coefficients deliberately, generating a scattered signal that varies in accordance with the sweeping beam. If this manipulated scattered signal is directed towards the receiver, it has the potential to distort the received power measurements, leading to the selection of a sub-optimal beam pair. This form of attack could be particularly potent, especially if the RIS can optimize its phase shifts based on either full or partial channel state information (CSI).

D. Physical Layer Authentication (PLA) Manipulation

Physical Layer Authentication (PLA) stands out as an emerging security technique that associates a wireless transmitter's identity with its specific location and channel attributes, which can be discerned by receivers, as outlined in [10]. In a UAV-aided RIS-assisted system, an adversarial RIS has the potential to undermine PLA by introducing rapid and random adjustments to the phase shifts. This manipulation can induce oscillations in performance indicators crucial for authentication, such as received signal strength or SNR. Executing this attack requires synchronization with the network and operates at a sub-symbol level. In cases where highly accurate channel estimates are available, there exists the possibility of exploiting them to arbitrarily disguise the identity of a node.

E. RIS-Aided Noise Injection

A RIS can be employed to assist an active jammer, in a way that the jammer transmits noise towards the RIS, which in turn "relays" the noise along with the legitimate signal. This undermines the RIS's effectiveness, as the added noise hampers the legitimate signal. In a UAV-aided RIS-assisted system, the UAV could be manipulated to position the RIS optimally for such an attack, or could itself be used to relay the noise. This attack necessitates active transmission towards the RIS and can target any legitimate RIS. In the presence of impinging noise, the SNR of the legitimate link scales linearly with the size of the RIS, contrasting with the quadratic scaling in the absence of an attack.

F. Exploiting RIS for Covert Surveillance

Given the reflective capabilities of RIS, an adversary could strategically position a UAV to eavesdrop on the communication between legitimate users, exploiting the RIS as a kind of 'mirror' to intercept the signals. This would necessitate a deep understanding of the RIS properties and the communication system, but it is a plausible threat that needs to be considered. In [11], a machine learning-based beamforming policy for UAV-assisted RIS was enhanced to improve the performance of communication channels. The DDPG algorithm provides an effective means to learn the optimal trajectory for Unmanned Aerial Vehicles (UAVs) and configure Reconfigurable Intelligent Surfaces (RIS) efficiently in an online setting [12]. [13] introduced an extended DDPG algorithm incorporating multi-dimensional rewards. However, it is noteworthy that DDPG with fully connected deep neural networks lacks the representational capacity needed for precise state inference. In [14], the authors introduced a secure UAV communication strategy to counteract smart jammers. This approach employed a knowledge-based reinforcement learning (RL) method, utilizing domain information to decrease the state space and expedite the convergence of the RL algorithm. Conventional optimization methods are not well-suited for trajectory planning in real-time scenarios. [15].

G. Manipulation of UAV-assisted RIS Link

The link between the UAV and the RIS is another potential point of vulnerability. An adversary could aim to disrupt this link, either by jamming the communication or by injecting false information. This could result in the UAV being unable to control the RIS effectively, or in the worst-case scenario, the UAV could be tricked into executing malicious commands.

H. RIS-aided UAV Swarm Exploitation

If multiple UAVs are used in the system, possibly in a swarm configuration, an adversary might attempt to exploit the interactions between the UAVs. They could try to compromise one UAV in the swarm and use it to disrupt the others, or they could inject false information into the swarm's communication to cause confusion and disruption.

The listed vulnerabilities underscore the need for robust security protocols in UAV-aided RIS-assisted systems. Further research is required to develop countermeasures against these threats and to continually monitor the system for any signs of intrusion or interference. The incorporation of advanced security features like artificial intelligence and machine learning could help bolster the system's defenses, enabling it to detect and respond to threats more effectively. As the field of RIS-assisted communication continues to evolve, the focus on security will remain a crucial aspect, ensuring the reliability and integrity of these advanced communication systems.

IV. Proposed DDPG-LSTM Framework for Intrusion Detection System

In this section, we present the LSTM-DDPG framework designed for intrusion detection for UAV-assisted RIS communication. To improve signal quality at the designated receiver and reduce the likelihood of eavesdropping, we employ the DDPG-LSTM framework within UAV-assisted RIS systems. This framework is specifically crafted to optimize security considerations, ensuring reliable communication within the domain of UAV-integrated RIS communication systems, thereby effectively preventing potential malicious threats.

The proposed LSTM-DDPG algorithm is outlined in Figure 3, with distinct components such as actor and critic networks, both incorporating LSTM architecture. Each network, actor, and critic, is composed of online and target counterparts.

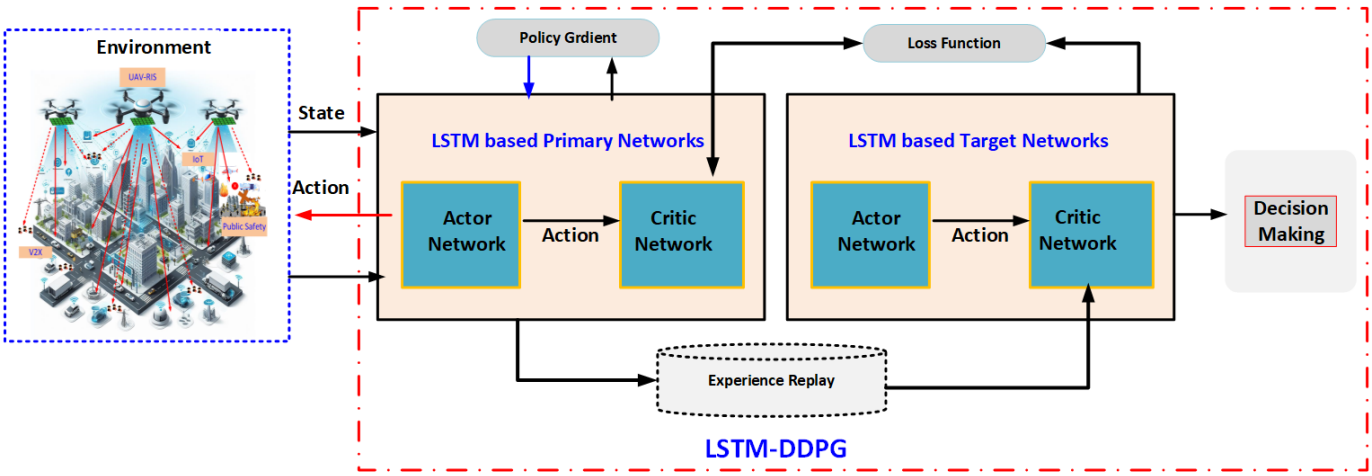


Figure 3. Proposed LSTM-DDPG Framework for Intrusion Detection in UAV-assisted RIS Communication

The actor-network employs the policy gradient method to derive a deterministic action based on observed environmental states. The critic network collaborates with the actor-network, employing a loss function to minimize and accurately evaluate the actor-generated action through knowledge of the Q-function. To enhance training efficiency and stability, duplicate target actor and critic networks are employed. Additionally, a historical transition tuple is maintained in the experience replay buffer, from which a random mini-batch of transitions is selected to train the neural networks, effectively minimizing data correlation.

A. LSTM-based Actor-Critic Network

The standard DDPG algorithm adheres to an actor-critic framework, consisting of an actor-network and a critic network. In this configuration, both the actor and critic networks employ fully connected deep neural networks (DNNs) to extract features from states and actions. However, the shortcomings of fully connected DNNs become evident as they struggle to capture temporal patterns inherent in environmental dynamics, such as user mobility and the time-varying nature of UE tasks. This inadequacy results in inaccuracies in state inference.

To address this limitation and better exploit the temporal patterns of states, allowing for continuous adaptation to environmental dynamics, we introduce the LSTM-based state characterization layer within actor-critic networks. Serving as a modified type of recurrent neural network, LSTM incorporates a memory cell to capture long-term dependencies from input sequence data. Consequently, LSTM has proven successful in handling various sequential tasks, including time series prediction and translation.

To overcome this constraint and more effectively leverage the temporal patterns inherent in states, facilitating continuous adaptation to environmental dynamics, we propose the integration of an LSTM-based state characterization layer within actor-critic networks. Operating as a modified form of a recurrent neural network, LSTM incorporates a memory cell to capture long-term dependencies present in input sequence data. As a result, LSTM has demonstrated success in addressing a variety of sequential tasks, ranging from time series prediction to translation.

The hidden state at the last time step, derived from the LSTM layer, serves as the output and is directed into fully connected neural networks (dense layers). This process further extracts state features to achieve an effective fitting effect. Subsequently, the actor-network employs output layers with different activation functions to generate corresponding policies. Finally, the results from these output layers are concatenated using the "$\oplus$" operator to produce the action.

The final hidden state obtained from the last time step through the LSTM layer functions as the output and is fed into fully connected neural networks, specifically dense layers. This step facilitates the extraction of state features, contributing to an effective fitting effect. Following this, the actor-network utilizes output layers with distinct activation functions to generate respective policies. Ultimately, the outcomes from these output layers are combined using the "" operator to yield the final action.

V. Performance Evaluation

In this section, first, we discuss the environment setup of the UAV-assisted RIS communication network. Then, we emulate the attacks and discuss the results.

A. UAV-Assisted RIS Environment Setup

In the context of UAV-aided RIS-assisted communications, our focus is to devise mechanisms that can effectively safeguard against various attacks such as Signal Nullification, Noise Injection, UAV-assisted RIS Link Exploitation Attack, and UAV Swarm Exploitation. To this end, we employ deep learning for detecting and counteracting these attacks. Our approach begins with the design and execution of a testbed to emulate the potential attacks. This step involves manipulating the RIS and UAV systems to simulate various attacks, resulting in the creation of datasets containing both normal and attacked instances. This data forms the basis for training our machine-learning models.

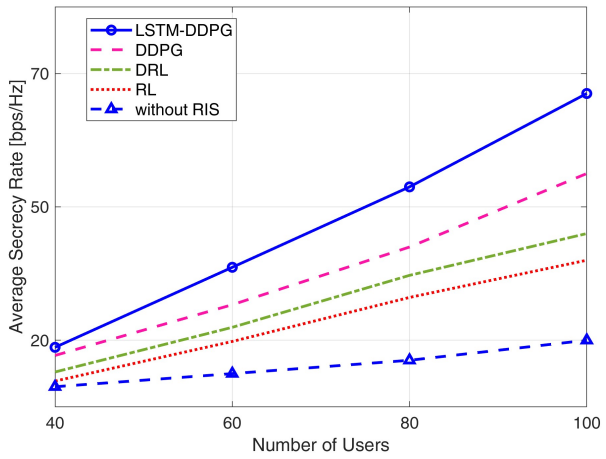


Figure 4. Average secrecy rate versus the number of users.

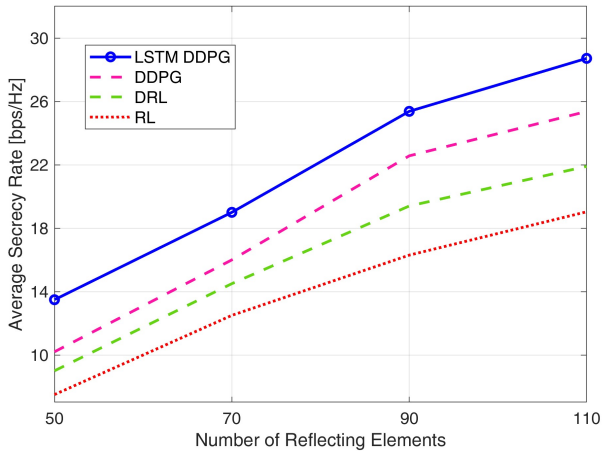


Figure 5. Average secrecy rate versus the number of reflecting elements.

In our simulation setup, we integrate the dynamics of Reflective RIS into our UAV-aided communication scenario. A user is modeled to move at a constant speed along a predefined trajectory, passing two eavesdroppers. A UAV, equipped with RIS, is available for relaying data from the base station to the user. These base stations are strategically placed at designated coordinates. The RIS-augmented UAV follows the user's path at an altitude of 20 meters, adjusting its reflective properties to optimize the communication link. We adopt an air-to-ground channel model that incorporates Line-of-Sight (LoS) signals, non-line-of-sight (non-LoS) signals, and multiple reflected components leading to multipath fading. The inclusion of RIS in this model is crucial, as it adds a degree of freedom in signal propagation, reflecting the incident signals from the UAV towards the legitimate user.

The secrecy rate, which serves as a measure of system confidentiality against eavesdropping, is calculated for the downlink along with cyber and physical features. It represents the difference between the data rate achieved at the legitimate user from the base station or RIS-enhanced UAV relay and the maximum rate achieved at the two eavesdropper nodes. The cyber feature represents the communication channels associated with RIS-aided UAVs, whereas, the physical feature represents the physical dynamic and control system features.

B. Results

This section presents a comprehensive set of experiments aimed at assessing the efficacy of our proposed LSTM-DDPG framework. The primary focus is on addressing security concerns and ensuring reliable communication in the context of UAV-integrated RIS communication systems. These experiments are designed to effectively counteract potential malicious threats and validate the robustness of the proposed approach.

We analyze the relationship between the average aggregate secrecy rate and the number of users in Figure 4. The results show that our proposed LSTM-DDPG mechanism consistently surpasses all other algorithms, demonstrating superior performance. It is clear that as the number of users increases, the

TABLE I
INTRUSION DETECTION AGAINST MALICIOUS THREATS.

Models	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	AUC (%)
RL	96.51	96.74	95.31	95.05	96.43
DRL	97.91	97.41	97.35	97.10	97.22
DDPG	98.71	97.45	97.48	97.85	98.73
LSTM-DDPG	99.10	98.84	98.61	98.22	99.11

LSTM-DDPG consistently outperforms alternative schemes in terms of secrecy rate. When compared to DDPG, deep reinforcement learning (DRL), RL, and without RIS, our proposed scheme consistently exhibits higher levels of secrecy. This highlights the inherent capability of the proposed algorithm to effectively safeguard sensitive information, even in scenarios with a larger user base. Specifically, the average secrecy rate of our proposed algorithm is 28%, 35%, 45%, and 65% higher than DDPG, DRL, RL, and without RIS, respectively.

Figure 5 shows the average aggregate secrecy rate in relation to the quantity of reflecting elements. The outcomes reveal the efficacy of the proposed LSTM-DDPG method in comparison to various other machine learning algorithms. It is evident that, with an increasing number of reflecting elements, the proposed algorithm consistently outshines alternative approaches in achieving a higher secrecy rate.

In addition, the various standard metrics for classification performance are employed to assess and contrast the models. These metrics encompass accuracy, precision, recall, F1 score, and the area under the receiver operating characteristic (ROC) curve (AUC). Table I presents the classification outcomes on crucial metrics for the proposed LSTM-DDPG framework in comparison to other AI models, including RL, DRL, and DDPG algorithms. The proposed framework consistently attains significantly higher values for accuracy, precision, recall, F1-score, and AUC when compared to any individual base model across all metrics.

VI. CONCLUSIONS AND RESEARCH OPPUTUNITES

In this paper, we have highlighted potential vulnerabilities in UAV-assisted reconfigurable intelligent surface (RIS) com-

munication networks that could be exploited by malicious attackers. Threats such as signal cancellation attacks, pilot sequence poisoning, and beam management poisoning pose risks to the secure functionality of these systems. To address these concerns, we have proposed a long short-term memory deep deterministic policy gradient (LSTM-DDPG) framework for detecting and countering malicious threats. Extensive experiments have demonstrated the efficacy of LSTM-DDPG framework in improving security and enabling reliable communications in UAV-RIS networks. Our approach introduces innovative machine learning solutions that outperform existing optimization techniques for this application.

As research on UAV-RIS communication systems continues, maintaining a focus on security will be crucial. The success of advanced machine learning techniques, like our LSTM-DDPG framework, underscores their potential for addressing the complex security challenges in these emerging networks. Our work paves the way for future efforts on developing more sophisticated machine learning models and protocols to match the evolution of threats targeting UAV-RIS systems. As this field continues advancing, research contributions like ours that prioritize reliability and integrity will be vital. There are significant opportunities for impactful research on ensuring robust and secure UAV-RIS communications.

REFERENCES

[1] S. Li, B. Duo, X. Yuan, Y.-C. Liang, and M. Di Renzo, "Reconfigurable intelligent surface assisted unmanned aerial vehicles communication: Joint trajectory design and passive beamforming," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 716–720, 2020.

[2] Y. Xu, H. Xie, Q. Wu, C. Huang, and C. Yuen, "Robust max-min energy efficiency for reconfigurable intelligent surface-aided hetnets with distortion noises," *IEEE Transactions on Communications*, vol. 70, no. 2, pp. 1457–1471, Feb. 2022.

[3] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "Irs-based wireless jamming attacks: When jammers can attack without power," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1663–1667, 2020.

[4] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE transactions on wireless communications*, vol. 18, no. 8, pp. 4157–4170, 2019.

[5] K. Zhi, C. Pan, H. Ren, K. K. Chai, and M. Elkashlan, "Active reconfigurable intelligent surface versus passive reconfigurable intelligent surface: Which is superior with the same power budget?" *IEEE Communications Letters*, vol. 26, no. 5, pp. 1150–1154, 2022.

[6] U. A. Mughal, J. Xiao, I. Ahmad, and K. Chang, "Cooperative resource management for c-v2i communications in a dense urban environment," *Vehicular Communications*, vol. 26, p. 100282, 2020.

[7] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, "Message integrity protection over wireless channel: Countering signal cancellation via channel randomization," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 106–120, 2017.

[8] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Communications*, vol. 29, no. 3, pp. 131–138, 2022.

[9] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE journal on selected areas in communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[10] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2219–2230, 2020.

[11] I. Ahmad, R. Narmeen, Z. Becvar, and I. Guvenc, "Machine learning-based beamforming for unmanned aerial vehicles equipped with reconfigurable intelligent surfaces," *IEEE Wireless Communications*, vol. 29, no. 4, pp. 32–38, August 2022.

[12] S. Hu, X. Chen, W. Ni, E. Hossain, and X. Wang, "Distributed machine learning for wireless communication networks: Techniques, architectures, and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1458–1493, 2021.

[13] Y. Yu, J. Tang, J. Huang, X. Zhang, D. K. C. So, and K.-K. Wong, "Multi-objective optimization for unmanned aerial vehicles-assisted wireless powered internet of things networks based on extended ddpg algorithm," *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6361–6374, September 2021.

[14] Z. Li *et al.*, "Uav networks against multiple maneuvering smart jamming with knowledge-based reinforcement learning," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12,289–12,310, Aug. 2021.

[15] S. Hu, X. Yuan, W. Ni, and X. Wang, "Trajectory planning of cellular-connected uav for communication-assisted radar sensing," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6385–6396, Sep. 2022.

Umair Ahmad Mughal received a B.S. in electrical engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2015, and a Master degree in electrical and computer engineering from INHA University, Korea, in 2020. Currently, he is pursuing a Ph.D. degree in Computer Science from Tennessee Technological University, USA, and working with the Cybersecurity Education Research and Outreach Centre.

His research interests include machine and deep learning for the cybersecurity of multi-UAVs networks, Cellular Vehicle-to-Everything (C-V2X) with 5G communications, and underwater acoustic communication. He is a recipient of the Jungseok International Scholarship to pursue his M.S. studies at Inha University due to his excellent academic career.

Yazeed Alkhrijah received the B.S. degree in electrical engineering (communication and electronics) from King Saud University, Riyadh, Saudi Arabia, the M.S. degree in electrical and computer engineering from The University of Tennessee Knoxville, TN, USA, and the Ph.D. degree in electrical and computer engineering with Southern Methodist University, Dallas, TX, USA. In 2022, he is the director of Engineering Research Center and an Assistant Professor with Imam Muhammad Ibn Saud Islamic University, Riyadh.

Ahmad Almadhor received the B.S.E. degree in computer science from Aljouf University (formerly Aljouf College), Aljouf, Saudi Arabia, in 2005 and the M.E. degree in computer science and engineering from University of South Carolina, Columbia, SC, USA, in 2010 and the Ph.D. degree in electrical and computer engineering at the University of Denver, Denver, CO, USA, in 2019. Dr. Almadhor's awards and honors include University of Denver's Profiles of Excellency, Jouf's Patents Award, Aljouf's Governor Award for excellency and several others.

Chau Yuen (S02-M06-SM12-F21) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. Dr. Yuen received IEEE Marconi Prize Paper Award in Wireless Communications (2021), and EURASIP Best Paper Award for JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING (2021). He serves as an Editor-in-Chief for Springer Nature Computer Science, Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.

He is a Distinguished Lecturer of IEEE Vehicular Technology Society, Top 2% Scientists by Stanford University, and also a Highly Cited Researcher by Clarivate Web of Science. He has 3 US patents and published over 500 research papers at international journals or conferences