Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs

Ursula Challita, Aidin Ferdowsi, Mingzhe Chen, and Walid Saad

Abstract

Cellular-connected UAVs will inevitably be integrated into future cellular networks as new aerial mobile users. Providing cellular connectivity to UAVs will enable a myriad of applications ranging from online video streaming to medical delivery. However, to enable reliable wireless connectivity for the UAVs as well as secure operation, various challenges need to be addressed such as interference management, mobility management and handover, cyber-physical attacks, and authentication. In this article, the goal is to expose the wireless and security challenges that arise in the context of UAV-based delivery systems, UAV-based real-time multimedia streaming, and UAV-enabled intelligent transportation systems. To address such challenges, ANN-based solution schemes are introduced. The introduced approaches enable UAVs to adaptively exploit wireless system resources while guaranteeing secure operation in real time. Preliminary simulation results show the benefits of the introduced solutions for each of the aforementioned cellular-connected UAV application use cases.

Introduction

Unmanned aerial vehicles (UAVs) will be ubiquitous and will play a vital role in various sectors ranging from medical and agricultural sectors to surveillance and public safety. Providing connectivity to UAVs is crucial for data collection and dissemination in such applications. Unlike current wireless UAV connectivity that relies on short-range communication technologies (e.g., WiFi, Bluetooth), cellular connectivity allows beyond line-of-sight (LoS) control, low latency, real-time communication, robust security, and ubiquitous coverage. In essence, cellular-connected UAVs will lead to many new application use cases, which we classify into three primary categories: UAV-based delivery systems (UAV-DSs), UAV-based real-time multimedia streaming (UAV-RMS) networks, and UAV-enabled intelligent transportation systems (UAV-ITS), as shown in Fig. 1.

However, to reap the benefits of cellular-connected UAVs for UAV-DS, UAV-RMS, and UAV-ITS use cases, various unique communication and security challenges for each of these applications need to be addressed. For instance, efficient handover and online path planning are more crucial for UAV-DS applications, while cooperative multi-UAV data transmission and secured consensus of UAV swarms are unique for UAV-ITS. In this scope, artificial intelligence (AI)-based solution schemes are regarded as a powerful tool for addressing the challenges of cellular-connected UAVs.[1] It is worthwhile noting that such challenges can also be addressed at different levels such as the physical layer and 3D coverage enhancement.[2] In this regard, AI-based schemes can assist in meeting the technical challenges of cellular-connected UAVs while yielding new improvements in the design of the network. Although many approaches exist for addressing the aforementioned challenges, we focus on machine learning solutions[3] due to their inherent ability to predict future network states, thus allowing UAVs to adapt to the dynamics of the network in an online manner. In particular, machine learning techniques allow UAVs to generalize their observations to unseen network states and can scale to large-sized networks, which therefore makes them suitable for UAV applications. Moreover, for such UAV-based applications, energy efficiency and computation capability are key design constraints. Consequently, the main scope of this work is to highlight the advantages that AI brings for cellular-connected UAVs under various constraints.

The current existing literature studied how the radio environment of cellular-connected UAVs changes with altitude and analyzed the corresponding implications on mobility performance [2]. Moreover, in [3], the authors provide an overview on the opportunities and challenges for the use of UAVs for wireless communication applications; however, the primary focus is on their use as base stations (BSs). The authors in [4] proposed a trajectory optimization scheme for cellular-connected UAVs while guaranteeing cellular connectivity. Although the works in [3, 4] discuss cellular-connected UAVs, they do not focus on the specifics of UAV-DS, UAV-RMS, and UAV-ITS applications; nor do they address AI or security challenges. Therefore, despite being interesting, none of the existing works propose and evaluate AI-based solutions for addressing both wireless and security challenges that arise in the context of cellular-connected UAVs. In essence, the state of the art does not study the potential of AI as a solution for integrating cellular-connected UAVs across various applications.

The main contribution of this article is to expose the major wireless and security challenges that arise in different UAV-based applications and suggest artificial neural network (ANN)-based solu-

[1] For more information, technical details related to the proposed AI techniques can be found in [1].

[2] Some existing surveys already discuss some of these issues [2, 3].

[3] The proposed machine learning techniques are mainly divided into two phases: a training phase followed by a testing phase. Therefore, although the training phase requires some heavy computation, it does not have any impact on the behavior of the UAVs during the testing phase, which refers to the actual execution time.

Digital Object Identifier:
10.1109/MWC.2018.1800155

Ursula Challita is with Ericsson Research (this work was done when Ursula Challita was at the University of Edinburgh); Aidin Ferdowsi and Walid Saad are with Virginia Tech; Mingzhe Chen is with Beijing University of Posts and Telecommunications.

1536-1284/19/$25.00 © 2019 IEEE

tion approaches for addressing such challenges. In particular, we focus on three major use cases for cellular-connected UAVs: UAV-based delivery systems, UAV-based real-time multimedia streaming networks, and UAV-enabled intelligent transportation systems. For each one of these use cases, we introduce the main technical challenges in terms of wireless connectivity and security (Fig. 2), while outlining new AI-inspired solutions to address those challenges. The introduced AI solutions enable the UAVs to predict future network changes, thus adaptively optimizing their actions in order to efficiently manage their resources while securing safe operation. We also provide preliminary simulation results to showcase the benefits of the introduced solutions for each cellular-connected UAV application use case. Here, we restrict our attention to the security at higher communication layers since physical layer security issues and solutions have been discussed in [5].

The rest of this article is organized as follows. The following section presents the communication and wireless challenges in UAV-DS and proposes AI-based solution schemes for such challenges. After that, we highlight the main communication and security challenges in UAV-RMS applications and the corresponding proposed ANN-based solutions. Then we provide ANN-based solution schemes for the main communication and security challenges in UAV-ITS. Finally, conclusions are given in the final section.

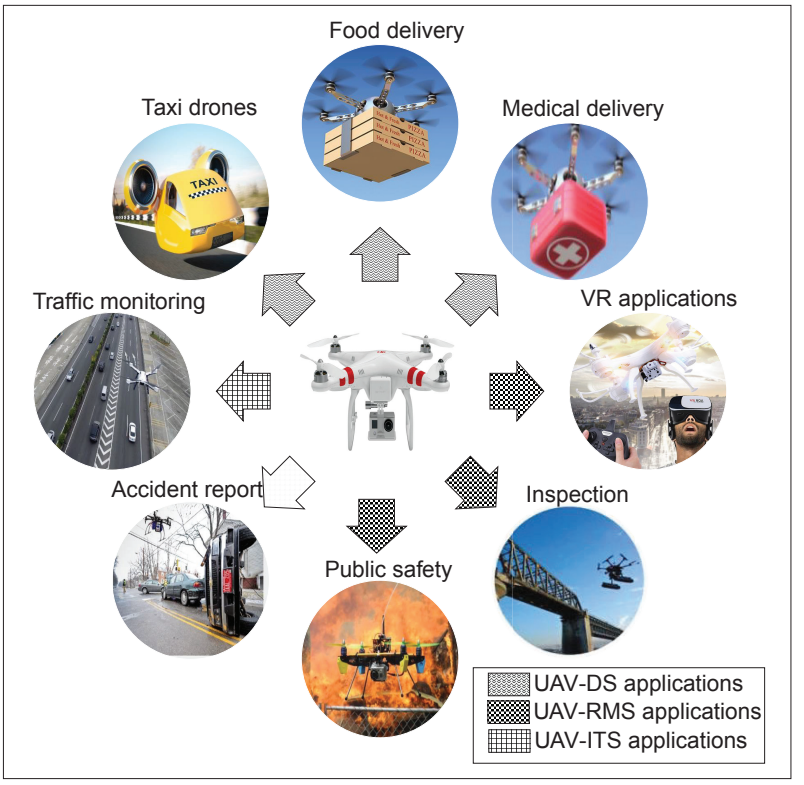

FIGURE 1. Cellular-connected UAV applications in UAV-based delivery systems, UAV-based real-time multimedia streaming networks, and UAV-enabled intelligent transportation systems.

UAV-Based Delivery Systems

Motivation

UAV-based delivery systems have received much attention recently for various applications such as postal and package delivery (e.g., Amazon prime), food delivery, transport of medicines and vaccinations, and drone taxis for delivery of people [6]. Compared to conventional delivery methods, UAV-DSs allow a faster delivery process at reduced cost. They can also provide mission-critical services reaching remote and inaccessible areas. To reap the benefits of UAV-DSs, it is important to provide cellular connectivity to the UAVs for control and signaling data transmission. In essence, providing cellular connectivity to delivery UAVs allows network operators to track their location and guarantee secure delivery of the transported goods. Therefore, to realize such benefits, it is important to address several wireless and security challenges related to cellular-connected UAV-DSs, ranging from efficient handover and path planning to cyber-physical attacks.

Wireless Challenges and AI Solutions

Ultra-Reliable and Low-Latency Communications (URLLC): In UAV-DSs, the UAVs must send critical control information while delivering goods to their destinations. This, in essence, requires latency of 1 ms or less and exceedingly stringent reliability with a target block error rate as low as 10^{-5} [7], especially in mission-critical scenarios such as medical delivery. Wireless latency encompasses both signaling overhead and data transmission. To achieve low signaling latency, channel estimation can be predicted in advance using AI, thus allowing proactive allocation of radio resources. This can be realized by incorporating a long-short term memory (LSTM) cell at the UAV level for learning a sequence of future channel states [8]. LSTMs are effective in dealing with long-term dependencies, which makes them suitable for learning a sequence of a time-dependent vector. Moreover, in a large network of UAVs, constantly communicating with a remote cloud can introduce substantial communication and signaling delays. To reduce such delays, one can rely on on-device machine learning or edge AI. As opposed to centralized, cloud-based AI schemes, on-device machine learning is based on a distributed machine learning approach, such as *federated learning* (FL), in which the training data describing a particular AI task (e.g., resource management or computing) is stored in a distributed fashion across the UAVs, and the optimization problem is solved collectively [9]. This in turn enables a large number of UAVs to collaboratively allocate their radio resources in a distributed way, thus reducing wireless congestion and device-to-cloud latency. Finally, it is important to note that transmission latency can be further reduced by improving wireless connectivity, as discussed later.

Efficient Handover: In UAV-DSs, the UAVs face frequent handovers and handover to distant cells resulting in a ping-pong effect. As opposed to ground user equipments (UEs), cellular-connected UAVs exhibit LoS links with multiple neighboring BSs simultaneously, which, along with dynamic channel variations, can result in a fluctuation in the quality of their wireless transmission. In this context, it is necessary to have complete and sequential information about the channel signal quality at different locations before and after the current

location of a particular UAV. As such, bidirectional LSTM cells (bi-LSTMs) are suited for addressing this challenge as they exploit both the previous and future contexts by processing the input data (i.e., channel quality) from two directions with two separate hidden layers. In particular, one LSTM layer processes the input sequence in the forward direction, while the other LSTM layer processes the input in the reverse direction [10]. Therefore, instead of accounting for the next time step only, this scheme enables each UAV to consider the channel quality at its previous and future sequence locations. This framework can hence be trained to allow the UAVs to update their corresponding cell association vector while avoiding frequent handovers based on previous and future channel signal quality.

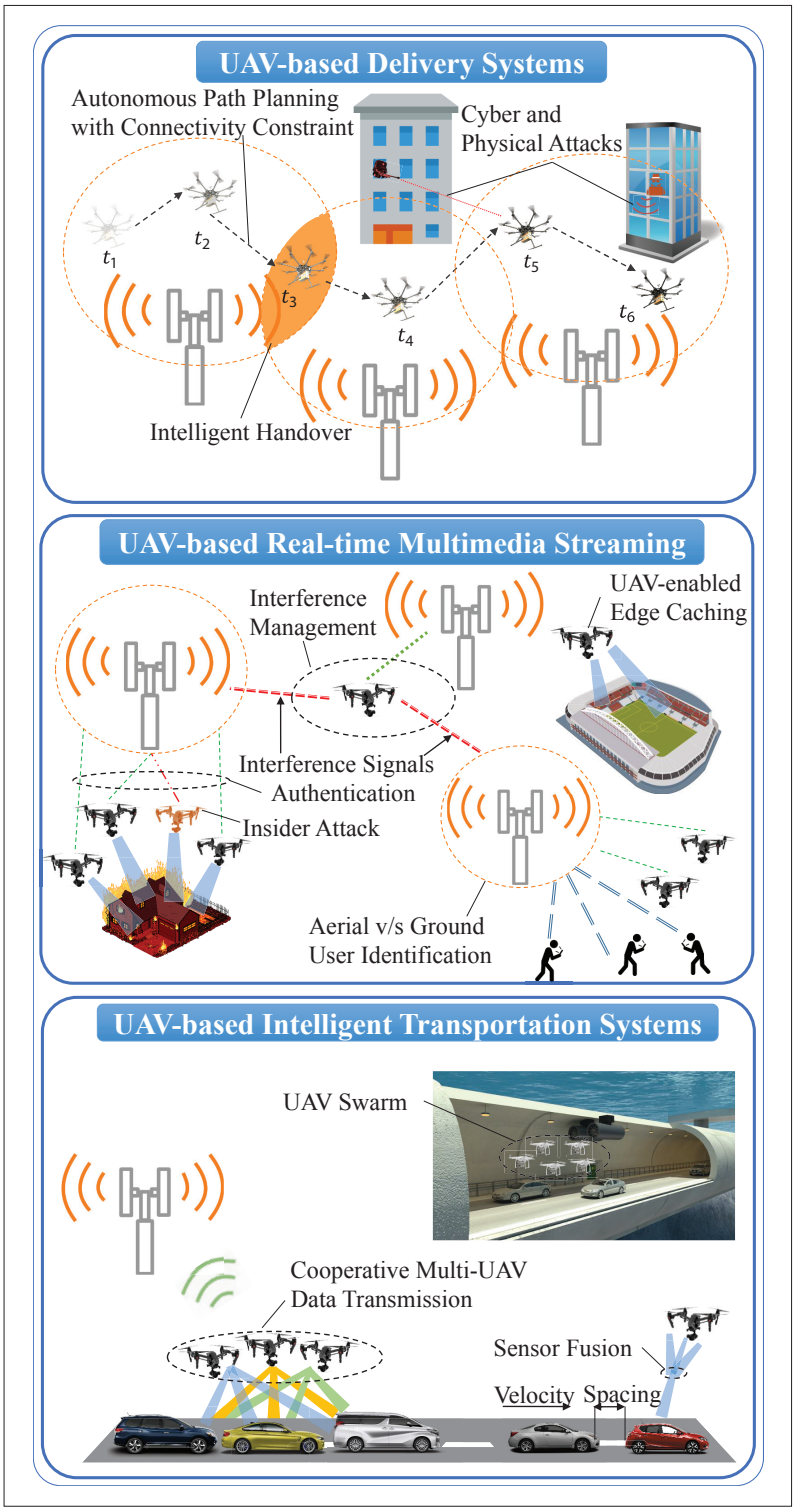

FIGURE 2. Examples of wireless and security challenges of cellular-connected UAVs in UAV-based delivery systems, UAV-based real-time multimedia streaming networks, and UAV-enabled intelligent transportation systems.

Autonomous Path Planning with Connectivity Constraints: A critical factor for UAV-DSs is to maintain reliable cellular connectivity for the UAVs at each time instant along their corresponding paths while also minimizing the total time required to accomplish their delivery mission. In essence, a delivery UAV must maintain a minimum signal-to-noise-plus-interference (SINR) ratio along its path to guarantee a reliable communication link for its control information. This naturally depends on the UAV's location, cell association vector, transmit power level, and the location of the serving ground BS. As such, a key challenge for UAV-DSs is to optimize the UAVs' paths so as to reduce their total delivery time while guaranteeing reliable wireless connectivity and thus an instantaneous SINR threshold value. Although a centralized approach can update the path plan of each UAV, this would require real-time tracking of the UAVs and control signals to be transmitted to the UAVs at all times. Moreover, a centralized approach incurs high round-trip latencies and requires a central entity to acquire full knowledge of the current network state. To overcome these challenges, *online* edge algorithms must be implemented individually by each UAV to plan its future path. In this regard, convolutional neural networks (CNNs) can be combined with a deep reinforcement learning (RL) algorithm based on a recurrent neural network (RNN) (e.g., an echo state network [ESN] or LSTM) at the UAV level, resulting in a CNN-RNN scheme. ESN exhibits dynamic temporal behavior and is characterized by its adaptive memory, which enables it to store necessary previous state information to predict the future steps of each UAV. Meanwhile, CNNs are mainly used for image recognition and thus can be used for identifying the UAV's environment by extracting features from input images. For instance, CNNs aid UAVs in identifying the location of ground BSs, ground UEs, and other UAVs in the network. These extracted features are then fed to a deep RNN, which can be trained to learn an optimized sequence of the UAV's future steps that would minimize its delivery time and guarantee reliable cellular connectivity at each time instant based on the input features.

In this regard, in [11], we proposed a deep RL framework based on ESN (D-ESN) for optimizing the trajectories of multiple cellular-connected UAVs in an online manner while minimizing latency and interference. For simplicity, we consider an input vector describing the locations of the neighboring ground BSs and other UAVs instead of extracting such features from a CNN. To highlight the gain of D-ESN for path planning, we compare the average values of the wireless latency per UAV, and rate per ground UE resulting from the proposed path planning scheme and the shortest path scheme, as shown in Fig. 3. Clearly, from Fig. 3, we can see that exploiting a D-ESN-based path planning scheme under connectivity constraints for cellular-connected UAVs results

in more reliable wireless connectivity and lower latency compared to a wireless-unaware shortest path scheme.

Security Challenges and AI Solutions

Due to the UAVs' altitude limitations and the LoS communication link with the ground BS, UAV-based delivery systems are vulnerable to *cyber-physical* (CP) *attacks* in which an adversary aims at compromising a delivery UAV, taking over its control, and ultimately destroying, delaying, or stealing the transported goods. To thwart such CP attacks, the UAV can create a CP threat map in which the adversaries' locations can be categorized based on the environmental objects where the UAVs can be physically attacked as well as the communication network where the cyber attacks can be imposed on the communication link. Even though prior works assume that a threat map is predetermined [12], it is important to create such a map in an online manner in order to account for real-time changes in the environment and to overcome the memory limitation of UAVs for storing a large-scale map. To realize this, a CNN can be trained for classifying the high-risk locations by taking as input the images of the UAV's surrounding environment along each position of its path. From the operator's perspective, it is also important to detect any potential attack by identifying any abnormal or undesirable behavior in the UAVs' motion. Therefore, given their capability of dealing with time-series data, RNNs can be adopted for capturing the UAV's motion characteristics by feeding them with the UAV's dynamics such as its position, speed, acceleration, and destination location. In this case, the RNN's output will be the predicted UAV's normal motion, and thus, using this output the operator can distinguish UAV's abnormal motion which is resulted from a CP attack.

UAV-Based Real-Time Multimedia Streaming Applications

Motivation

One key use case for cellular-connected UAVs is to provide various real-time multimedia streaming applications such as online video streaming and broadcasting, UAV-enabled virtual reality (VR), online tracking and localization of mobile targets, and surveillance. In essence, providing cellular connectivity to UAVs enables online transmission of data and low-latency wireless communication, which are essential factors for multimedia streaming applications. To enable effective delivery of such real-time multimedia using cellular-connected UAVs, several wireless and security challenges need to be addressed, ranging from interference management to authentication.

Wireless Challenges and AI Solutions

Interference Management: For UAV-RMS applications, UAVs will mainly transmit data in the *uplink*. Nevertheless, the ability of cellular-connected UAVs to establish LoS connectivity with multiple ground BSs can lead to substantial mutual interference among them as well as to ground users. To address this challenge, new improvements in the design of future cellular networks, such as advanced receivers, cell coordination, 3D frequency reuse, and 3D beamforming, are needed. For instance, due to their ability to recognize and classify images, CNNs can be implemented on each UAV in order to identify several features of the environment such as the location of UAVs, BSs, and ground UEs. Such an approach will enable each UAV to adjust its beamwidth tilt angle so as to minimize the interference on the ground UEs. Moreover, in streaming scenarios, UAV trajectory optimization is also essential. In particular, physical layer solutions such as 3D beamforming can be combined with an interference-aware path planning scheme to guarantee more efficient communication links for both ground and aerial users. Such a path planning scheme (e.g., the one we proposed in [11]) allows the UAVs to adapt their movement based on the rate requirements of both aerial UAV-UEs and ground UEs, thus improving the overall network performance.

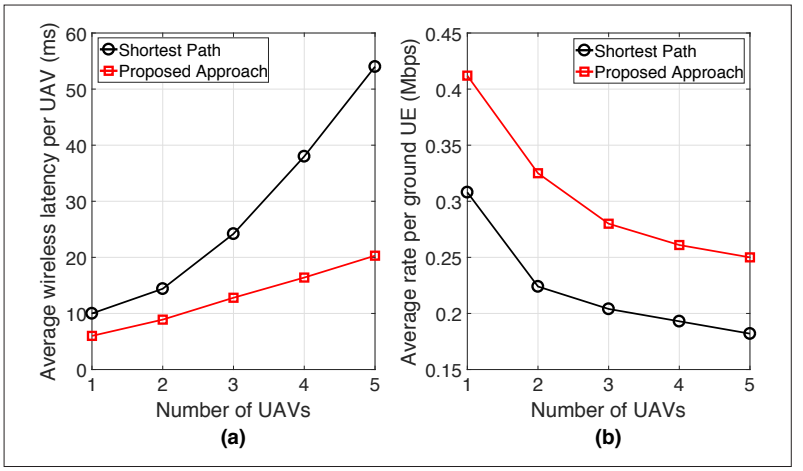

FIGURE 3. Performance assessment of the proposed deep ESN-based path planning algorithm in terms of average: a) wireless latency per UAV; b) rate per ground UE compared to the shortest path approach for different numbers of UAVs [11].

UAV-Enabled Edge Caching: For various real-time multimedia streaming applications, cellular-connected UAVs must generate videos from data files collected using sensors and cameras. For instance, in UAV-enabled VR applications, the UAVs will generate 360° videos for each user. However, each UAV can only collect a limited number of data files, which might not be sufficient for generating all the requested videos. Meanwhile, cache-enabled UAVs can store common data files related to popular content or for generating videos that users may request in the future, thus reducing the number of data files that UAVs need to collect when a request is made [13]. For instance, for UAV-enabled VR applications, cache-enabled UAVs can directly store a 360° video and send a rotated version of this stored video according to each user's viewing perspective. Moreover, for game broadcast applications, cache-enabled UAVs can store the environment of the game and thus would only need to track the motions of the players for updating the cached data. Here, CNNs can once again be adopted for allowing cache-enabled UAVs to store popular videos or common data files. In particular, CNNs can extract and store the common features of the data files that are requested by different users or by each user at different time slots. Furthermore, CNNs can be used to record the

In essence, DBNs are deep architectures that consist of a stack of restricted Boltzmann machines (RBMs), thus having the benefit that each layer can learn more complex features than the layers before it. In essence, a pre-training step is done in DBNs thus overcoming the vanishing gradient problem. This is then followed by fine-tuning the network weights using conventional error back propagation algorithm.

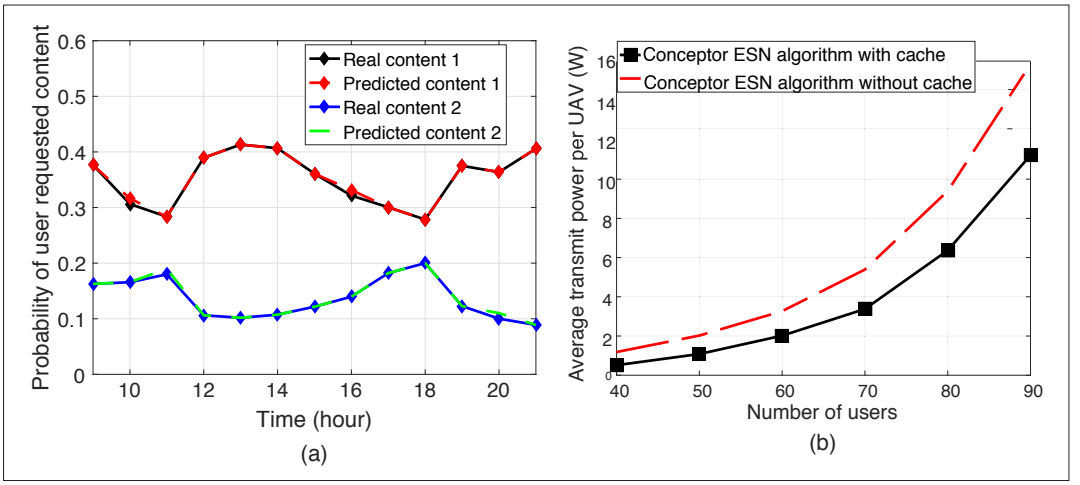

FIGURE 4. a) Comparison of the content request probability predictions for the proposed conceptor ESN algorithm with the real data; b) the average UAV transmit power as a function of the number of users in the network for the proposed conceptor ESN algorithm with and without caching [13].

features of each UAV's surrounding environment. Consequently, when the UAVs need to collect data in a new environment, they would only need to collect new features that are not already recorded by the CNNs. In this context, RNNs can also be employed for predicting users' video requests. In fact, the context requests of users can be correlated over time, and thus, RNNs can enable the UAVs to cache in advance the predicted future requests or other popular multimedia files.

Based on our work in [13], we introduce an ESN-based algorithm for predicting the user's content request distributions. The input to the proposed framework is the users' context information such as age, gender, and job, and the output of the ESN-based algorithm is the distribution of the users' content requests. Therefore, based on the users' content request distributions, the UAVs can determine the contents to store at the UAV cache and thus transmit the cached contents to the users without the need for backhaul connections. Using real data from *Youku*, Fig. 4a shows that the ESN-based algorithm can accurately predict the content request distribution of a given user. Figure 4b shows the average transmit power per UAV of cache-enabled UAVs as a function of the number of users. In Fig. 4, we can see that the proposed ESN algorithm for cache-enabled UAVs yields a considerable reduction in transmit power compared to a baseline without caching.

Identification of Aerial and Ground Users: As shown in [2], the radio propagation environment experienced by cellular-connected UAVs differs from that experienced by ground users. Consequently, to maximize the total network performance, a network operator must allocate its radio resources differently between airborne and ground users, especially for UAV-RMS applications. To realize this, network operators should be capable of differentiating an airborne user from a ground one, which cannot be achieved by solely relying on self-reporting due to the possibility of a faulty report. Instead, network operators can utilize wireless cellular radio measurements such as reference signal received power (RSRP), received signal strength indicator (RSSI), and reference signal received quality (RSRQ) for user classification. These features can essentially act as input to a deep belief network (DBN), which can be trained for classifying an airborne user from a ground one. In essence, DBNs are deep architectures that consist of a stack of restricted Boltzmann machines (RBMs), thus having the benefit that each layer can learn more complex features than the layers before it. In essence, a pre-training step is done in DBNs, thus overcoming the vanishing gradient problem. This is then followed by fine-tuning the network weights using a conventional error back propagation algorithm.

Security Challenges and AI Solutions

In UAV-RMS applications, an attacker can disrupt the UAV's data transmissions by forging the identities of the transmitting UAVs and sending disrupted data using their identities. This type of *insider attack* becomes particularly acute in a large-scale UAV system. In particular, the BS must process the received multimedia files from all the UAVs and allocate computational resources for authenticating the UAVs. However, in large-scale networks, authenticating all the UAVs at once exceeds the BS's computational resources, thus incurring delay in processing the received files.

To avoid this delay, the BS can authenticate only a fraction of the UAVs at each time step. To realize this, the BS could implement a deep RL algorithm based on LSTM in order to learn what signals to authenticate at each time step of its authentication process. In particular, this framework takes as an input a sequence of previous security states of each UAV indicating whether a UAV was previously vulnerable to attacks, and learns a sequence of future authentication decisions for each UAV. LSTMs are suitable for this application since they can learn the interdependence of UAVs' vulnerability at the past time steps, memorize the importance of UAVs to the BS, and map the past sequence of UAV states to a future decision sequence.

To analyze the performance of the LSTM-based deep RL method for authentication, based on [14], we consider a network of 1000 UAVs that transmit multimedia streams to a BS. We analyze different

scenarios in which different proportions of available UAVs are vulnerable to cyber attacks.Figure 5 assesses the performance of the LSTM-based deep RL framework compared to two baseline authentication scenarios. From Fig. 5, we can see that the proposed algorithm performs the same as the two other baselines in the low range of proportion of vulnerable UAVs. However, as the number of vulnerable UAVs increases the LSTM-based deep RL outperforms the two other baselines and reduces the proportion of compromised UAVs in the network.

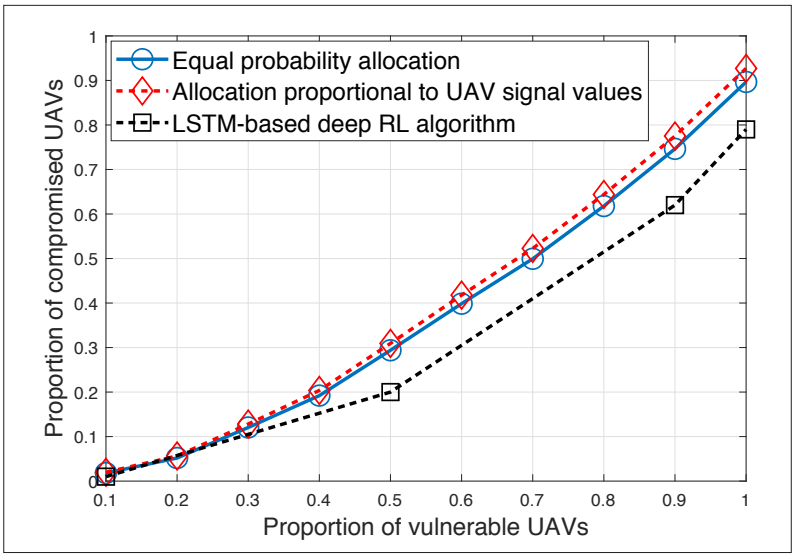

FIGURE 5. The proportion of compromised cellular-connected UAVs as a function of the proportion of vulnerable UAVs in large-scale UAV system authentication [14].

UAV-Enabled Intelligent Transportation Systems

Motivation

Integrating UAVs in an ITS would control road traffic, monitor incidents, and enforce road safety. For instance, UAVs can provide a quick report in case of an accident and can act as flying roadside units, speed cameras, and dynamic traffic signals. Moreover, for vehicular platoons, to reduce wireless network congestion, a cellular-connected UAV can send control and network related information to one of the vehicles only, and this vehicle can share the information with other vehicles in the platoon via dedicated short-range communication links. UAVs can also track the behavior of a platoon, thus detecting any compromised vehicle. Therefore, to reap the benefits of UAV-ITS, several wireless and security challenges need to be addressed ranging from cooperative multi-UAV data transmission and multimodal data integration to secured consensus of UAV swarms.

Wireless Challenges and AI Solutions

Cooperative Multi-UAV Data Transmission: In UAV-ITS, each UAV is generally equipped with multiple sensors such as LiDAR and GPS, and therefore needs to send different types of multimedia files and/or big data (e.g., 3D map representation of the environment) to either other UAVs, vehicles, or the infrastructure simultaneously. In such scenarios, it would be essential for different UAVs in a given geographical area to coordinate their data transmission. In other words, instead of each UAV transmitting the whole data file (e.g., an area map) to its corresponding vehicle, each UAV will transmit a different part of the data file to all of the vehicles in a given geographical area, resulting in faster data transmission and lower power consumption per UAV. In this regard, deep spectral clustering (DSC) learning can be adopted for grouping the UAVs into several clusters for data transmission based on their location, the type of sensors they encompass, data files they need to transmit, and the location and number of vehicles in the network. In essence, DSC learns a map that embeds this input data into the eigenspace of their associated graph Laplacian matrix and clusters them accordingly. Consequently, DSC endows the UAVs with the capability of transmitting correlated data in a cooperative and distributed manner to the vehicles. This would essentially result in faster data transmission to the vehicles, thus allowing them to make real-time decisions for safe navigation among the surrounding traffic. DSC can be combined with cooperative game theory for further analysis of cooperative swarms of UAVs. Moreover, the presence of high mobility in ITS along with cooperative UAV swarms requires revisiting the interference and resource management schemes above to handle the more dynamic and cooperative ITS environment.

Multimodal Sensor Fusion: In UAV-ITS, UAVs must transmit each of their sensor readings to other network nodes, resulting in cellular network congestion in the case of dense UAV deployment. However, energy consumption and bandwidth allocation are important factors that determine the maximum operation time of the UAVs. As such, to reduce the power and bandwidth allocated for transmitting the sensor readings, a UAV can integrate its heterogeneous sensor readings into one vector, resulting in fewer data transmissions over the UAV-vehicle links while also providing a more comprehensive assessment of the environment. Nevertheless, there are differences between sensors ranging from sampling rates to the data generation model, making UAV-based ITS sensor integration challenging. In this regard, multimodal RBMs (m-RBMs) are a suitable tool for combining different perspectives captured in signals of multimodal data for a system with multiple sensors [15]. An m-RBM can be implemented at the UAV level, thus identifying nonintuitive features largely from cross-sensor correlations, which can yield accurate estimation. From the UAV's perspective, this approach enables each UAV to have a better assessment of its environment. For instance, a system trained simultaneously to detect an accident, a high-speed vehicle, and an anomalous vehicle does better than three separate systems trained in isolation since the single network can share information among the separate tasks. From the wireless network perspective, multimodal sensor fusion improves the UAV's energy efficiency and results in fewer data transmissions over the UAV-vehicle links, thus reducing wireless congestion and enabling a larger number of UAVs to be served simultaneously.

Wireless and security challenges	UAV-based applications			ANN-based solutions								
	UAV-DS	UAV-RMS	UAV-ITS	FL	bi-LSTM	CNN-RNN	D-ESN	CNN	ESN	DBN	LSTM	DSC	m-RBM
URLLC	✓			✓									
Efficient handover	✓				✓								
Autonomous path planning	✓					✓	✓						
Interference management		✓						✓					
UAV-enabled edge caching		✓						✓	✓				
Identification of aerial and ground users		✓								✓			
Cooperative multi-UAV data transmission			✓									✓	
Multimodal sensor fusion			✓										✓
Cyber-physical attacks	✓							✓					
Authentication of UAVs		✓									✓		
Secured consensus of UAV swarms			✓	✓									

TABLE 1. Cellular-connected UAV use cases, challenges, and ANN-based solution schemes.

Security Challenges and AI Solutions

For UAV-ITS, a swarm of coordinated UAVs has the capability of performing missions compared to single UAVs. Swarming UAVs communicate with each other while in flight to reach a consensus on their defined task, and can respond to changing conditions autonomously. A good analogy would be a dense flock of starlings reacting to a sudden threat like a hawk. Nevertheless, this data sharing scheme among a swarm of UAVs is generally prone to *adversarial machine learning* attacks in which an attacker can join the swarm and alter their shared data, which results in non-harmonious movements as well as collisions. To overcome this challenge, federated learning can be adopted for a swarm of UAVs. In federated learning, each UAV receives the common task that needs to be accomplished by the UAV swarm from the BS and improves its learning model for completing the required tasks based on its collected data only. Then each UAV summarizes the changes in its learning model and shares this summary with other UAVs in the swarm. This, indeed, will solve the vulnerability of raw data transmission between the UAVs, mitigating the risk of the adversarial machine learning.

Table 1 provides a summary of the wireless and security challenges of cellular-connected UAVs in UAV-DS, UAV-RMS, and UAV-ITS while suggesting ANN-based solution schemes.

Conclusion

In this article, we have summarized the main use cases of cellular-connected UAVs in UAV-DS, UAV-RMS, and UAV-ITS applications. We have highlighted the main wireless and security challenges that arise in such scenarios while introducing various AI-based solutions for addressing such challenges. Preliminary simulation results have shown the benefits of the introduced solutions for each cellular-connected UAV application use case.

Acknowledgment

This work was supported by the Army Research Office (ARO) under Grant W911NF-17-1-0593 and in part by the U.S. National Science Foundation under Grants OAC-1541105 and IIS-1633363. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of ARO or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for government purposes notwithstanding any copyright notation herein.

References

[1] M. Chen *et al.*, "Machine Learning for Wireless Networks with Artificial Intelligence: A Tutorial on Neural Networks," arXiv:1710.02913, Oct. 2017.
[2] S. Euler *et al.*, "Mobility Support for Cellular Connected Unmanned Aerial Vehicles: Performance and Analysis," arXiv:1804.04523, Apr. 2018.
[3] M. Mozaffari *et al.*, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," arXiv:1803.00680, Mar. 2018.
[4] E. Bulut and I. Güvenc, "Trajectory Optimization for Cellular-Connected UAVs with Disconnectivity Constraint," *Proc. IEEE ICC — Integrating UAVs into 5G*, Kansas City, MO, May 2018.
[5] G. Zhang *et al.*, "Securing UAV Communications via Joint Trajectory and Power Control," arXiv:1801.06682, Jan. 2018.
[6] P. Grippa *et al.*, "Job Selection in a Network of Autonomous UAVs for Delivery of Goods," *Proc. Robotics: Science and Systems*, Cambridge, MA, July 2014.
[7] J. Nielsen, R. Liu, and P. Popovski, "Ultra-Reliable Low Latency Communication Using Interface Diversity," *IEEE Trans. Commun.*, vol. 66, no. 3, Nov. 2017, pp. 1322–34.
[8] U. Challita, L. Dong, and W. Saad, "Proactive Resource Management for LTE in Unlicensed Spectrum: A Deep Learning Perspective," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, July 2018, pp. 4674–89.
[9] J. Konecny *et al.*, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," arXiv:1610.02527, Oct. 2016.
[10] A. Zeyer *et al.*, "A Comprehensive Study of Deep Bidirectionaltional LSTM RNNs for Acoustic Modeling in Speech Recognition," arXiv:1606.06871, Mar. 2017.
[11] U. Challita, W. Saad, and C. Bettstetter, "Cellular-Connected UAVs over 5G: Deep Reinforcement Learning for Interference Management," arXiv:1801.05500, Jan. 2018.

[12] A. Sanjab, W. Saad, and T. Basar, "Prospect Theory for Enhanced Cyberphysical Security of Drone Delivery Systems: A Network Interdiction Game," *Proc. IEEE ICC*, Paris, France, 2017.
[13] M. Chen *et al.*, "Caching in the Sky: Proactive Deployment of Cache-Enabled Unmanned Aerial Vehicles for Optimized Quality-of-Experience," *IEEE JSAC*, vol. 35, no. 5, May 2017, pp. 1046–61.
[14] A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet of Things Systems," arXiv:1803.00916, 2018.
[15] N. Srivastava and R. Salakhutdinov, "Multimodal Learning with Deep Boltzmann Machines," *Proc. Advances in Neural Information Processing Systems*, Lake Tahoe, CA, Dec. 2012.

Biographies

Ursula Challita received her Ph.D. degree from the University of Edinburgh in 2018. From 2016 to 2018, she was a visiting research scholar at Virginia Tech. Currently, she is an experienced researcher at Ericsson Research, Stockholm, Sweden, working on artificial intelligence for next-generation cellular networks. Her research interests include wireless networks, unmanned aerial vehicles, spectrum management, machine learning, and optimization theory.

Aidin Ferdowsi received his B.S. in electrical engineering from the University of Tehran, Iran, in 2016. He is currently a Ph.D. student at the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He is also a Wireless@VT Fellow. His research interests include cyber-physical systems, machine learning, security, and game theory.

Mingzhe Chen (S'15) received his B.S. degree from Huazhong University of Science and Technology, Wuhan, China. He is currently pursuing a Ph.D. degree at the Information and Communication Engineering Department of Beijing University of Posts and Telecommunications, China. He is also a visiting researcher in the Department of Electrical and Computer Engineering at Virginia Tech. His research interests include machine learning, virtual reality, content caching, and unmanned aerial vehicles.

Walid Saad [S'07, M'10, SM'15, F'19] received his Ph.D. degree from the University of Oslo in 2010. Currently, he is an associate professor in the Department of Electrical and Computer Engineering at Virginia Tech. His research interests include wireless networks, machine learning, game theory, cybersecurity, unmanned aerial vehicles, and cyber-physical systems. He was an author/co-author of seven conference best paper awards and received the 2015 IEEE ComSoc Fred W. Ellersick Prize.