VHetNets for AI and AI for VHetNets: An Anomaly Detection Case Study for Ubiquitous IoT

Weili Wang (✉), Omid Abbasi (✉), Halim Yanikomeroglu (✉), Chengchao Liang (✉), Lun Tang (✉), and Qianbin Chen (✉)

Abstract
Vertical heterogeneous networks (VHetNets) and artificial intelligence (AI) play critical roles in 6G and beyond networks. This article presents an AI-native VHetNets architecture to enable the synergy of VHetNets and AI, thereby supporting varieties of AI services while facilitating the intelligent network management. Anomaly detection stands as an essential AI service across various applications in Internet of Things (IoT), including intrusion detection, state monitoring, analysis of device activities, and security supervision. In this article, we first discuss the possibilities of VHetNets used for distributed AI model training to provide the anomaly detection service for ubiquitous IoT, i.e., VHetNets for AI. After that, we study the application of AI approaches in helping implement the intelligent network management functionalities for VHetNets, i.e., AI for VHetNets, whose aim is to facilitate the efficient implementation of the anomaly detection service. Finally, a case study is presented to demonstrate the efficiency and effectiveness of the proposed AI-native VHetNets-enabled anomaly detection framework.

Introduction
6G and beyond networks are expected to exhibit some unique characteristics. First, satellites in space networks, high altitude platform stations (HAPs), unmanned aerial vehicles (UAVs) in air networks, and terrestrial base stations are integrated into vertical heterogeneous networks (VHetNets) to provide global coverage [1]. Second, ubiquitous Internet of Things (IoT), which is playing an important role in varieties of verticals including smart homes, healthcare wearables, environmental monitoring, industrial control, agriculture and transportation, supports seamless connectivity for anyone and anything [2], [3]. Third, intelligence exists in every corner of networks, ranging from end devices to the core. Numerous network nodes are endowed with built-in artificial intelligence (AI), thereby supporting varieties of AI services while facilitating the intelligent network management [4].

Anomaly detection is defined as a process of automatically detecting whether devices, components or systems are in their normal running states or not [5], which stands as an essential AI service across various applications in IoT for the uninterrupted operation and early warnings of abnormal behaviors. The foundation of anomaly detection lies in data, with machine learning emerging as the predominant technique to establish the anomaly detection model [6]. Conventional anomaly detection approaches in IoT typically employ static sensors for data sensing, and IoT gateways to relay sensing data to a central server for storage and analysis. However, the data explosion in ubiquitous IoT poses a major impediment to any centralized learning framework in view of the privacy concern and limited communication resources for data transmission. In addition, in situations where sensing targets are continually moving or located in hard-to-reach areas, traditional sensing solutions will endure great challenges.

Taking advantage of the broad field of view and the exceptional 3D mobility, a wireless sensing scheme assisted by UAVs was introduced in [7] for smart sensing and data collection from diverse IoT devices. However, in [7], sensing data were transmitted to a central server for centralized processing, which compromised the data privacy and communication efficiency. To protect the data privacy in ubiquitous IoT systems, [2] presented a novel federated imitation learning framework with a knowledge-sharing module by keeping the training dataset locally. Nevertheless, the paper lacked a discussion of effective learning architectures that support multi-dimensional input data. In [3], a data-driven VHetNet framework empowered with AI was designed to implement the intelligent network management, but how to utilize VHetNets to provide AI services required by IoT devices was not discussed.

Recently, AI for VHetNets has attracted many research efforts. In [8], the unique role of AI in design, topology management, handoff, and resource allocation for VHetNets was reviewed and concluded comprehensively. By contrast,
VHetNets for AI has gained less attention. In future networks, because HAPS and UAVs with integrated sensing and communication capability can execute edge computing functionality, they are great enablers for AI service provision in aerial networks [9]. Moreover, the two components of AI-native VHetNets, namely VHetNets for AI and AI for VHetNets, are not independent but complementary to each other. The former requires the latter to provide network planning and resource scheduling functionalities for the efficient implementation of AI services, while the latter relies on the former to further improve the network management efficiency.

In this article, by using IoT devices to provide data support, UAVs to perform data sensing from IoT devices and the local model training, and HAPS to execute the control agent and global aggregation, we design an AI-native VHetNets architecture through the hierarchical collaboration among three layers, namely HAPS, UAVs and ground IoT devices. In the proposed AI-native VHetNets architecture, on one hand, HAPS and UAVs in VHetNets can provide data, communication, computing, and storage resources required by AI services from varieties of IoT devices, namely VHetNets for AI. On the other hand, AI techniques can be applied to provide the intelligent network management functionalities (such as network planning, device association, and resource scheduling) for VHetNets, namely AI for VHetNets. The contributions of this article are summarized as follows:

- Design an AI-native VHetNets architecture to enable the synergy of VHetNets and AI, thereby supporting varieties of AI services from IoT devices while facilitating the intelligent network management for VHetNets.
- Establish an AI-native asynchronous federated learning (AFL)-based anomaly detection scheme with the assistance of VHetNets, where AFL framework aims to improve the learning efficiency and accuracy. In the proposed scheme, UAVs are responsible for performing the data sensing from IoT devices and the local model training, and HAPS is responsible for selecting the best UAV subset participating in the global aggregation.
- Introduce a new deep reinforcement learning (DRL) method called compound-action actor-critic (CA2C) to implement the intelligent network management, which combines the advantages of the deep deterministic policy gradient (DDPG) for handling continuous action spaces, and the deep Q-network (DQN) for handling discrete action spaces. The CA2C-based intelligent network management scheme will assist the implementation of the AI-native AFL-based anomaly detection model.

In this article, we first develop an AI-native VHetNets architecture to enable the synergy of VHetNets and AI. Then, we present the techniques of VHetNets for AI to implement an anomaly detection service, and AI for VHetNets to provide the intelligent network management functionalities. After that, we validate the efficiency and effectiveness of the proposed framework through a case study. Finally, the article is concluded, and the future research is presented.

**AI-Native VHetNets Architecture**

As shown in Fig. 1, the proposed AI-native VHetNets architecture is established through the hierarchical collaboration among three layers, including the ground plane, the sensing and data plane, and the control and aggregation plane, whose main roles are elaborated as follows:

**Ground Plane.** Ground IoT devices are kinds of applications in a variety of verticals, from industry to environments, from transportation to healthcare, from home area to public venues, and so on. Different IoT devices will produce large amounts of heterogeneous data, which can provide data support for AI service requests. For example, by collecting and analyzing the sensing data indicating running states of different systems, the anomaly detection model can be constructed to detect abnormal behaviors of monitored systems and provide early warnings before the occurrence of failure.

**Sensing and Data Plane.** Each UAV with integrated sensing and communication capacity plays the role of a sensor, computing node, and storage node. It is responsible for sensing ground IoT devices within its coverage, and training the local AI model based on its sensing data. Using UAVs as aerial nodes to provide wireless sensing support from the sky is a promising paradigm for its advantages of the broad field of view, the exceptional 3D mobility, and the capability of sensing performance optimization through dynamic UAV trajectory planning.

**Control and Aggregation Plane.** HAPS works as the control agent and global aggregation node. HAPS is a quasistationary network node that operates at an altitude of around 20 km [9]. HAPS, which can provide line-of-sight communication and wide coverage, has been regarded as an indispensable component for 6G networks. By AI techniques, HAPS can control and manage the whole network in an intelligent way through intermittent interactions with the network environment. Due to its quasi-stationary and wide coverage features, it can also work as the central node for the global aggregation of local models from UAVs.

In the proposed AI-native VHetNets architecture, AI for VHetNets means that the control agent in HAPS will implement the intelligent network management functionalities with the assistance of AI, including device association, UAV selection, and UAV trajectory planning. With respect to VHetNets for AI, UAVs and HAPSs can provide the data, communication, computing, and storage resources required by AI service requests from IoT devices.

**VHetNets for AI: An Anomaly Detection Service for Ubiquitous IoT**

As one of the indispensable AI services, an efficient anomaly detection model is vital to detect or even predict abnormal behaviors or attacks that exist in ubiquitous IoT systems.

In VHetNets, IoT devices provide the data support, and HAPS and UAVs provide the sensing, communication, computing, and storage capability for distributed AI model training to implement the anomaly detection service. Abnormal
behaviors occur infrequently in practice, leading to an imbalanced training dataset when collecting sensing data from IoT devices. Therefore, our approach to implement the anomaly detection involves creating a representation of normal behaviors and determining abnormal behaviors according to their degree of deviation from normal ones. The generative adversarial network (GAN) is adopted as the foundational model for anomaly detection in AI-native VHetNets, given its powerful capability to represent the distribution of high-dimensional complex data [10].

GAN consists of two models: the generator and discriminator, which are usually built with neural networks. The generator attempts to generate new (fake) samples from latent variables to fool the discriminator, and the discriminator attempts to distinguish fake samples from real ones. The generator and discriminator are updated alternately until the generator can generate fake samples sharing the same distribution with real ones, and the discriminator is unable to distinguish them.

Instead of uploading all sensing data from UAVs to HAPS and training the anomaly detection model at HAPS in a centralized manner, the distributed learning framework, like federated learning (FL), enables UAVs to execute local training on their own sensing data and avoid raw data transmission to HAPS for preserving privacy and improving communication.

In VHetNets, IoT devices provide the data support, and HAPS and UAVs provide the sensing, communication, computing, and storage capability for distributed AI model training to implement the anomaly detection service.
efficiency. However, traditional FL commonly adopts a synchronous aggregation mode to wait for all participating agents to finish their local training before the global aggregation, which will inevitably increase the global learning latency. In addition, unreliable data from IoT devices will cause low local model quality in UAVs, which will affect the global model’s learning efficiency and accuracy.

In this article, we propose an AI-native AFL-based anomaly detection scheme assisted by GAN, where HAPS uses AI techniques to select UAVs with high model quality and low energy consumption to join the global aggregation, and AFL is utilized as the learning framework for the GAN model training to improve the learning efficiency and accuracy. Fig. 2 illustrates the training processes of the AI-native AFL-based anomaly detection scheme assisted by GAN.

After the global generator and discriminator are well trained, an anomaly score, which is defined as the weighted combination of the generator loss and discriminator loss, can be constructed to determine the abnormal behaviors.

**AI for vHetNets: CA2C-based Intelligent Network Management**

Existing work mainly considers the anomaly detection as a standalone service that is independent of any other network management functionalities. In fact, the efficiency of the AI-native AFL-based anomaly detection scheme depends heavily on the network management functionalities of UAV selection, device association, and UAV trajectory planning [11], whose functions are presented as follows:

**Device Association.** The device association strategy is applied to decide which UAV a ground IoT device should associate with to maximize its successful sensing probability and the whole networks’ coverage, which is closely related to the data abundance to establish an accurate and robust anomaly detection model.

**UAV Selection.** The UAV selection strategy is used to select the best UAV subset participating in each global aggregation round, whose objective is to minimize the federated execution time and learning accuracy loss. The federated execution time mainly relies on UAVs’ locations, remaining...

---

**FIGURE 2. Training processes of the AI-native AFL-based anomaly detection scheme assisted by GAN.** The scheme’s workflow consists of nine steps as follows: (1) HAPS distributes initial global model parameters and UAV selection indicators to each UAV as local model parameters and update indicators, respectively; (2) Each UAV sets its local model parameters as global ones, then checks the selection indicator to determine whether to implement the local training step or not; (3) If a UAV is selected to participate in this global training round, then activate the training processes of local generator and discriminator; (4) Sample a mini-batch of fake data and real data to train the discriminator; (5) Based on the local discriminator model, sample a mini-batch of noise to train the generator every N discriminator training rounds; (6) Upload local parameters to HAPS for the global aggregation every K local training rounds; (7) HAPS obtains global generator and discriminator models by the model aggregation; (8) HAPS adopts AI techniques to determine the optimal UAV subset for the next global training round; (9) HAPS distributes model parameters and UAV selection indicators to all UAVs for their further updates. The above steps are implemented repeatedly until the global models converge.
energy and computing resources. The learning accuracy loss is related to the model quality of selected UAVs. **UAV Trajectory Planning.** Because some IoT devices randomly move with a rapid speed, UAVs also need to move correspondingly to complete the sensing process. However, the energy capacity of UAVs is limited, so the dynamic UAV trajectory planning strategy is vital to track moving IoT devices using minimum energy.

**INTELLIGENT NETWORK MANAGEMENT**

The intelligent network management functionalities consist of sequential decision-making processes with the time-varying network environment. Reinforcement learning (RL) is an effective solution to make sequential decisions through intermittent interactions with the network environment, which comprises a decision-making agent, network state, action, and reward [12]. Based on the network state, the agent takes an action and then obtains an instant reward. The network environment will enter into a new state after an action is taken on it. The state transition and instant reward will guide and reinforce the adaption of the agent’s policy, which determines the sequential actions with the evolution of the network environment. The learning process continues until the optimal policy that maximizes the accumulated reward is found.

For the efficient implementation of the AI-native AFL-based anomaly detection scheme, the decision-making processes for the intelligent network management are defined as follows:

**Decision-Making Agent:** HAPS works as the decision-making agent due to its quasi-stationary position, the line-of-sight communication, wide coverage, and multiple energy sources, including conventional energy (such as electrical batteries and fuel tanks), energy beams, and solar energy [8].

**State:** At each time slot \( t \), HAPS interacts with the network environment to observe its network state \( s(t) \), including the current location \( x_n(t) \) of each ground IoT device \( k \in K \), the previous location \( x_n(t-1) \) of each UAV \( n \in N \), and each UAV’s remaining energy \( E_n(t) \). Therefore, the network state \( s(t) \) is expressed as \( s(t) = \{ (x_n(t))_{k \in K}, (x_n(t-1))_{n \in N}, (E_n(t))_{n \in N} \} \). The network environment contains two key components: the current network state \( s(t) \), and each IoT device association indicator \( \lambda_{n,k} \) and each UAV selection indicator \( \gamma_{n,t} \), as well as the continuous variables of each UAV position \( x_n(t) \). The network environment will enter into a new state \( s(t+1) \) after an action \( a(t) \) is taken on the current network state \( s(t) \), and \( a(t) \) is expressed as \( a(t) = \{ (x_n(t))_{n \in N}, (\lambda_{n,k})_{k \in K, n \in N}, (\gamma_{n,t})_{n \in N} \} \). The reward \( r(t) \) is a numerical value obtained by the agent from the environment to quantify its satisfaction with adopted actions. The objective of the defined decision-making processes is to maximize the coverage capacity \( C(t) \) of UAVs, which is expressed as the total number of successfully sensed IoT devices, while minimizing the execution time \( E(t) \) and learning accuracy loss \( L(t) \) of the anomaly detection model. The execution time \( E(t) \) is the sum of the local model update and upload time, as well as the global model aggregation and distribution time. Therefore, the instant reward \( r(t) \) is defined as the weighted sum of coverage capacity, execution time, and learning accuracy loss at time slot \( t \), which is expressed as \( r(t) = \mu_1 C(t) - \mu_2 E(t) - \mu_3 L(t) \), where \( \mu_1, \mu_2, \) and \( \mu_3 \) are weight parameters and all greater than 0.

**CA2C APPROACH**

RL is hard to train to converge and obtain the optimal policy when facing large state and action spaces in large-scale networks. DRL overcomes this challenge by adopting deep neural networks (DNNs) as function approximators to predict Q-values. The success of DQN depends on two key techniques to stabilize the learning process with large state and action spaces, namely fixed target Q-network and experience replay. In each DQN training round, a random mini-batch of samples are extracted from the replay buffer to break the sample correlation and improve the learning efficiency [13]. However, DQN only handles the sequential decision-making processes with discrete action spaces.

**DQN.** DQN is an extension of the traditional value-based Q-learning method, which utilizes DNNs as function approximators to predict Q-values. The success of DQN depends on two key techniques to stabilize the learning process with large state and action spaces, namely fixed target Q-network and experience replay. In each DQN training round, a random mini-batch of samples are extracted from the replay buffer to break the sample correlation and improve the learning efficiency [13]. However, DQN only handles the sequential decision-making processes with discrete action spaces.

**DDPG.** Policy gradient-based RL methods can be utilized to handle the sequential decision-making processes with continuous action spaces. To speed up the convergence of the policy gradient-based methods, DDPG is proposed to combine the policy-based approach with the value-based approach to estimate the policy gradient more efficiently [12]. In DDPG training, the critic network evaluates the policy quality by estimating the Q-value, and the actor function adopts the policy gradient method to update the policy. DNNs are used as the function approximators for the actor and critic networks. DDPG also uses two key techniques, namely target actor and critic networks, and experience replay to make the learning process more stable and efficient.

**CA2C APPROACH**

The intelligent network management functionalities defined in the above decision-making processes include UAV selection, device association, and UAV trajectory planning, which include both discrete indicators and continuous variables. In this article, the discrete indicators and continuous variables are not independent and can be solved through establishing standalone decision-making models, but highly correlated to reach a common objective, namely achieve an efficient anomaly detection model. Thus, the CA2C approach [13] is introduced in this article to realize the intelligent network management, which integrates the strengths of DDPG for handling continuous decision variables and DQN for handling discrete decision variables. In CA2C, the actor network is still used to generate continuous actions like in DDPG, i.e., UAV trajectory planning in this article. However, the critic network is built as the Q network, which can not only be used to determine discrete actions including device association and UAV selection, but also can provide the advantage of fast training and fast convergence.

---

1 Readers can find the detailed calculation methods for the coverage capacity, execution time, and learning accuracy loss in [11].
evaluate the quality of both continuous actions and discrete actions.

The learning processes of the CA2C-based intelligent network management are illustrated in Fig. 3 and explained as follows, which include three main sub-procedures.

1. **Environment Interactions:**
   1. Observe the network state;
   2. Execute both discrete and continuous actions determined by the actor and critic networks at each time slot;
   3. Calculate the reward as the feedback of selected actions;
   4. The environment enters into a new network state.

   The quadruple \(<\text{State}, \text{Action}, \text{Reward}, \text{Next state}>\) will be stored in the replay buffer as experience.

2. **Critic Network Training:** First, sample a mini-batch of experience as the training data.
   1. Based on the actor network, obtain UAV locations (continuous actions) for the observed state;
   2. Determine device association and UAV selection indicators (discrete actions) based on the Q-value estimated by the target critic network;
   3. The target actor network calculates UAV locations based on the observed state and discrete actions;
   4. Calculate the target value by adding instant reward and Q-value, which is estimated by the target critic network;
   5. Update critic parameters using Adam optimizer;
   6. Share critic parameters with the target critic network;
   7. Update parameters of the target critic network using the soft update method, namely the weighted sum of critic network's parameters and its own parameters, where the sum of weights is equal to 1.

3. **Actor Network Training:** First, sample a mini-batch of experience as the training data.
   1. Calculate the gradient of Q-value function with respect to UAV locations (continuous actions);
   2. Update actor parameters using Adam optimizer;
   3. Share actor parameters with the target actor network;
   4. Update parameters of the target actor network using the soft update method, which is the same as the update of the target critic network.

   The above three sub-procedures are executed alternately until all training episodes end. The integration between the AI-native AFL-based anomaly detection scheme and the CA2C-based intelligent network management method contributes to an efficient anomaly detection model.

**A Case Study**

In this section, a case study is presented to evaluate the performance of the proposed AI-native AFL-based anomaly detection scheme with the assistance of CA2C-based intelligent network management.

We consider a 1 km \(\times\) 1 km area with a HAPS, 5 UAVs and 30 ground IoT devices. The proposed UAVs’ propulsion energy model in [14] is used to evaluate the energy consumption of UAVs in moving and hovering patterns. In the moving pattern, the energy consumption of UAVs is relevant to their moving velocity, which is set as 30 m/s.
Its calculation method and corresponding parameters have been given in [14]. For UAVs’ energy consumption in hovering pattern, the hovering power of UAVs is set as 168 W, and the hovering energy is proportional to the communicating and computing time. Besides, the communicating power and computing power at UAVs are fixed as 5 W and 20 W, respectively. The considered scenario is simulated in Python language using Pytorch package. In the simulation, socket is used to realize the communication between emulated UAVs and HAPS.

We choose a well-known dataset published by Inter Berkeley Research Lab² as sensing data from ground IoT devices. The dataset includes temperature, humidity, light and voltage features collected from 54 distributed Mica2Dot sensors every 31 seconds. The dataset consists of normal data only and is unlabeled. Because the 54 distributed Mica2Dot sensors were deployed on different geolocations and collected the same data features, the distribution of data samples can be regarded as IID. We divide the dataset into three disjoint datasets: training dataset for model training, validation dataset for setting the discriminant criterion of anomalies, and test dataset for performance evaluation. The validation dataset and test dataset are manually-labeled by injecting random noise into them to simulate abnormal behaviors.

The proposed AI-native AFL-based anomaly detection scheme is established on the GAN model and assisted by the CA2C-based intelligent network management. In the simulation, an improved modification of GAN called WGAN-GP [15] is used as the basic anomaly detection model to avoid the mode collapse issue in GAN. The FL-based anomaly detection method and the standalone anomaly detection method are used as baseline schemes. In the FL-based scheme, each UAV participates in all global aggregation rounds, and the UAV selection process is not included. In the standalone scheme, each UAV independently learns its own anomaly detection model without engaging in any data or parameter exchange, and there are no intelligent network management functionalities assisting its training process. Fig. 4(a) shows the convergence performance of the WGAN-GP model in three different anomaly detection schemes. It can be seen that the proposed scheme has the best convergence performance among the three different schemes.

In Fig. 4(a) and (b), an episode includes 50 time slots, and the duration of each time slot is set as 1s, which is the length of a global iteration. To make the implementation details of CA2C and GAN training clearer, the relationship between the training processes of CA2C approach and the WGAN-GP model is illustrated in Fig. 4(c).
between an episode, a global iteration, and a local iteration is illustrated in Fig. 4(c).

We compare the detection performance, execution time and energy consumption of the proposed scheme with the FL-based and standalone schemes. Metrics used for evaluating the detection performance include precision, recall, accuracy and F1-score. The comparison results are presented in Fig. 5.

Fig. 5(a) shows the average execution time and maximum execution time of different schemes over total 50 time slots. From Fig. 5(a), we can see that the proposed AI-native AFL-based anomaly detection scheme consumes the least execution time, and the FL-based scheme causes the most execution time. This is because the FL-based scheme needs to wait for the completion of local model updates by all UAVs and then execute the global aggregation process. The execution time of the standalone scheme is averaged among all UAVs, and it also brings more execution time than the proposed scheme because UAVs with long execution time will affect the average values. Fig. 5(b) shows the average energy consumption in UAVs with different schemes. From Fig. 5(b), we can see that the proposed scheme consumes the least energy compared to the FL-based and standalone schemes. The reason is that the proposed scheme is assisted by the CA2C-based intelligent network management, where UAVs are not required to participate in every global aggregation, and the dynamic UAV trajectory planning is executed to reduce the energy consumption, so a lot of energy is saved. Fig. 5(c) shows the detection performance of different methods. The proposed scheme can achieve the best detection performance compared to the other two schemes because the UAV selection process in the proposed scheme can keep UAVs with less learning accuracy from affecting the global anomaly detection model. Therefore, the proposed scheme can achieve the best detection performance with the least execution time and energy consumption.

**Conclusion and Future Research**

In this article, we first propose an AI-native VHetNets architecture through the hierarchical collaboration among HAPS, UAVs and ground IoT devices. Then, to implement VHetNets for AI, we design an AI-native AFL-based anomaly detection scheme with the assistance of VHetNets. After that, we introduce a CA2C-based intelligent network management method to implement AI for VHetNets. The integration between the AI-native AFL-based anomaly detection scheme and CA2C-based intelligent network management method contributes to an efficient anomaly detection model. The anomaly detection case study demonstrates that the synergy of AI and VHetNets can achieve an accurate anomaly detection model with low execution time and energy consumption.

For future research, the proposed framework can be extended by involving the blockchain technology to improve privacy and security during distributed AI model training. On one hand, although AFL has distinct privacy advantages, it still faces two security threats: poisoning participants and inference attacks. These two threats may result in the convergence failure of global AI models or privacy leakage of sensitive information. On the other hand, UAVs and HAPS operate...

![Figure 5](image-url)
in the air networks and rely on wireless communication technologies to implement data exchange, so the AI-native VHetNets are more susceptible to endure these privacy and security issues. Therefore, the recognition of malicious participants and secure transmission during aggregation are major concerns in constructing secure AFL frameworks. With the advantages of decentralization, immutability, anonymity, and security, integrating blockchain with the AFL framework can defend against numerous threats and attacks. In addition, in the field of using AFL framework over wireless networks, considering different time granularity for determining different network management strategies is still an open issue, which requires extensive research efforts in the future.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62071078 and Grant 62001076, in part by the Sichuan Science and Technology Program under Grant 2021YFQ0053, and in part by the Postdoctoral Fellowship Program of CPSF under Grant GZC20233364.

References

[1] Z. Wang et al., “AI-based cloud-edge-device collaboration in 6G space-air-ground integrated power IoT,” IEEE Wireless Commun., vol. 29, no. 1, pp. 16–23, Feb. 2022.
[2] A. Yu et al., “Federated imitation learning: A cross-domain knowledge sharing framework for traffic scheduling in 6G ubiquitous IoT,” IEEE Netw., vol. 35, no. 5, pp. 136–142, Sep./Oct. 2021.
[3] T. Darwish et al., “A vision of self-evolving network management for future intelligent vertical HetNet,” IEEE Wireless Commun., vol. 28, no. 4, pp. 96–105, Aug. 2021.
[4] W. Wu et al., “AI-native network slicing for 6G networks,” IEEE Wireless Commun., vol. 29, no. 1, pp. 96–103, Feb. 2022.
[5] X.-X. Lin, P. Lin, and E.-H. Yeh, “Anomaly detection/prediction for the Internet of Things: State of the art and the future,” IEEE Netw., vol. 35, no. 1, pp. 212–218, Jan./Feb. 2021.
[6] J. Jiang et al., “Outlier detection approaches based on machine learning in the Internet-of-Things,” IEEE Wireless Commun., vol. 27, no. 3, pp. 53–59, Jun. 2020.
[7] D. Van Huynh et al., “Real-Time optimized path planning and energy consumption for data collection in unmanned aerial vehicles-aided intelligent wireless sensing,” IEEE Trans. Ind. Inform., vol. 18, no. 4, pp. 2753–2761, Apr. 2022.
[8] G. K. Kurt et al., “A vision and framework for the high-altitude platform station (HAPS) networks of the future,” IEEE Commun. Surveys Tuts., vol. 23, no. 2, pp. 729–779, 2nd Quart., 2021.
[9] G. K. Kurt and H. Yankomeroglu, “Communication, computing, caching, and sensing for next-generation aerial delivery networks: Using a high-altitude platform station as an enabling technology,” IEEE Veh. Technol. Mag., vol. 16, no. 3, pp. 108–117, Sep. 2021.
[10] A. Creswell et al., “Generative adversarial networks: An overview,” IEEE Signal Process. Mag., vol. 35, no. 1, pp. 53–65, Jan. 2018.
[11] W. Wang et al., “A vertical heterogeneous network (VHetNet)—Enabeled asynchronous federated learning-based anomaly detection of the Cloud,” IEEE Open J. Commun. Soc., early access, Dec. 12, 2023, doi: 10.1109/OJCOMS.2023.3342008.
[12] S. Gong et al., “Deep reinforcement learning for backscatter-aided data offloading in mobile edge computing,” IEEE Netw., vol. 34, no. 5, pp. 106–113, Sept./Oct. 2020.
[13] J. Hu et al., “Cooperative Internet of UAVs: Distributed trajectory design by multi-agent deep reinforcement learning,” IEEE Trans. Commun., vol. 68, no. 11, pp. 6807–6821, Nov. 2020.
[14] Y. Zeng, J. Xu, and R. Zhang, “Energy minimization for wireless communication with rotary-wing UAV,” IEEE Trans. Wireless Commun., vol. 18, no. 4, pp. 2329–2345, Apr. 2019.
[15] I. Gujrati et al., “Improved training of Wastewater GANs,” in Proc. Adv. Neural Inf. Process. Syst., May 2017, pp. 5769–5779.

Biographies

WENLI WANG (wangwl@cqupt.edu.cn) received the M.E. and Ph.D. degrees in information and communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2013 and 2016, respectively. She is currently a Post-Doctoral Researcher with Carleton University form December 2021 to January 2023. She is currently a Post-Doctoral Researcher with the Cyber Security and Information Law Research Center, Chongqing. Her current research interests include intelligent network management and self-healing techniques in 6G.

OMID ABBASI (Senior Member, IEEE) (omidabbasi@sce.carleton.ca) received the B.Sc. degree in electrical engineering from the University of Tabriz, Tabriz, Iran, in 2011, and the M.Sc. degree in electrical engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2015, and the Ph.D. degree in electrical engineering from the Sahand University of Technology, Tabriz, in 2020. Since February 2019 to September 2020, he was a Visiting Researcher with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada. He is currently a Post-Doctoral Fellow with Carleton University. His current research interests include high-altitude platform station (HAPS) for 6G. He has actively served as a reviewer for flagship IEEE journals and conferences.

HAIM YANKOMEROGULU (Fellow, IEEE) (haim@sce.carleton.ca) is currently with the Non-Terrestrial Networks (NTN) Laboratory, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada. His research group has made substantial contributions to generations of wireless technologies. His group’s current focus is the wireless access architecture of the future and non-terrestrial networks (NTNs). His extensive collaboration with industry resulted in 40 granted patents. He is a fellow of the Engineering Institute of Canada (EIC), the Canadian Academy of Engineering (CAE), and the Asia-Pacific Artificial Intelligence Association (AAIA). He is a Distinguished Speaker for both the IEEE Communications Society and the IEEE Vehicular Technology Society. He has received several awards for his research, teaching, and service.

CHENGCHAO LIANG (liangc@cu鄣pt.edu.cn) received the Ph.D. degree in electrical and computer engineering from Carleton University, Canada, in 2017. He was a cross-appointed Post-Doctoral Fellow with the Department of Systems and Computer Engineering, Carleton University, and the Huawei Ottawa Research and Development Centre from 2017 to 2019. He is currently a Full Professor with the School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications. He is on the editorial boards of EURASIP Journal on Wireless Communications and Networks and Transactions on Emerging Telecommunications Technologies. He has served as a reviewer and a TPC member for many IEEE journals and conferences. His research interests include wireless communications, satellite networks, internet protocol, and optimization theory. He was awarded the Senate Medal for the Ph.D. degree.

LUN TANG (tangl@cqupt.edu.cn) received the Ph.D. degree in communication and information system from Chongqing University, Chongqing, China. He is currently a Professor with the School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing. His current research interests include 5G/6G wireless networks, network slicing, UAV, and edge/cloud networks.

QIANGHAI CHEN (Senior Member, IEEE) (cqh@cu鄣pt.edu.cn) received the Ph.D. degree in communication and information systems from the University of Electronic Science and Technology of China, Chengdu, China, in 2002. He is currently a Professor with the School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China and the Director of the Chongqing Key Laboratory of Mobile Communication Technology, Chongqing. He has authored or coauthored more than 100 papers in journals and peer-reviewed conference proceedings, and has coauthored seven books. He holds 47 granted national patents.