Artificial Intelligence Enabled Internet of Things: Network Architecture and Spectrum Access

©ISTOCKPHOTO.COM/CHUNUMUNU

Hao Song
the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA

Jianan Bai
the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA

Yang Yi
the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA

Jinsong Wu
the School of Artificial Intelligence, Guilin University of Electronic Technology, Guilin, China and the Department of Electrical Engineering, Universidad de Chile, Santiago, CHILE

Lingjia Liu
the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, USA

Digital Object Identifier 10.1109/MCI.2019.2954643
Date of current version: 10 January 2020

Corresponding authors: Lingjia Liu (ljliu@ieee.org) and Jinsong Wu (wujs@ieee.org).

1556-603X/20©2020IEEE

***Abstract*—The explosive growth of wireless devices motivates the development of the internet-of-things (IoT), which is capable of interconnecting massive and diverse "things" via wireless communications. This is also called massive machine type communications (mMTC) as a part of the undergoing fifth generation (5G) mobile networks. It is envisioned that more sophisticated devices would be connected to form a hyperconnected world with the aids of the sixth generation (6G) mobile networks. To enable wireless accesses of such IoT networks, artificial intelligence (AI) can play an important role. In this article, the frameworks of centralized and distributed AI-enabled IoT networks are introduced. Key technical challenges, including random access and spectrum sharing (spectrum access and spectrum sensing), are analyzed for different network architectures. Deep reinforcement learning (DRL)-based strategies are introduced and neural networks-based approaches are utilized to efficiently realize the DRL strategies for system procedures such as spectrum access and spectrum sensing. Different types of neural networks that could be used in IoT networks to conduct DRL are also discussed.

In general, dense active users or machine devices will bring two major challenges: increased probability of access collisions and complicated resource management.

I. Introduction

The emerging waves of Internet-of-things (IoT) paradigm are attracting increasing attention from both industry and academia via its promising applications of intelligently connecting things or objects around us without human interventions [1]. With the automatic interactions among numerous devices, such as radio frequency identification (RFID), sensor networks, and mobile phones, IoT can assist our daily life in various ways including ubiquitous healthcare, control of home equipment, environmental monitoring, smart grid, and so on [2]–[4]. Nowadays, the evolution of the fifth generation (5G) wireless networks becomes the main driver for world-wide IoT development [5], [6]. Even though the surge of 5G networks has not fully arrived yet, it is time to envision what will appear in the sixth generation (6G) wireless networks [7]. Towards this end, our paper will not only provide solutions to technical challenges in 5G mobile networks but also provide visions on how these solutions may resolve issues in future 6G networks.

According to Gartner, there will be more than 30 billion IoT devices by the year 2025 [8]. Accordingly, the 5G network and future 6G networks are expected to support a massive number of smartly connected IoT devices [9], [10]. Our existing wireless technologies may break down when such a tremendous number of devices (things) attempt to access the network. To achieve the massive access of IoT devices, it is important to redesign and improve our existing networks [11].

Compared with conventional wireless communication networks targeting mainly at human communications, IoT networks, which also allow machine-to-machine communications, have unique characteristics and capability requirements [12]. First, IoT networks should be able to provide wireless access services to a large amount of dense wireless users or machine devices. In general, dense active users or machine devices will bring two major challenges: increased probability of access collisions and complicated resource management. When access collisions occur, users/devices will necessarily relaunch radio access procedures leading to increased transmission latency and degraded quality of service (QoS). For delay-sensitive data, latency is a very important factor causing the failure of the underlying transmissions. Dense active users or machine devices will bring additional difficulties in wireless resource management, including scheduling and power control due to the additional complications caused by the underlying wireless channel and inter-user interference. Furthermore, in order to effectively conduct resource management, channel measurements need to be conducted to obtain the underlying channel state information, the overhead of which could be substantial with a large number of active users and devices. Second, IoT networks should be able to handle heterogeneous wireless users or machine devices. Diverse wireless devices may co-exist in IoT networks with different QoS requirements and priorities. For example, by proper resource management, IoT networks should give priority to guarantee reliable transmissions of emergency information, such as health care and fire alarms.

The existing methods to tackle the aforementioned issues mainly rely on complicated algorithms, mechanisms and schemes [13], [14] where specific models are used. Due to the heterogeneous nature of IoT networks, such model-dependent solutions can not effectively adapt to real environment. Furthermore, algorithm-based approaches may be prohibitively complicated preventing them from being adopted in practice. On the other hand, artificial intelligence (AI)-based approaches can play an important role to handle resource management among a massive number of devices. Accordingly, deep neural networks and big data analytics are naturally suitable for information extraction from high-dimensional data and complicated decision makings [15]. We do believe that the AI-supported hyper-connected world would be an integral core part of future 6G wireless networks. In this article, more efficient and overhead-friendly approaches using AI will be explored and introduced.

The remainder of this article is organized as follows. In Section II, we introduce the frameworks of both centralized and distributed IoT networks. Then, in Section III, potential technical challenges of centralized IoT networks are analyzed, and the corresponding solutions based on AI technologies are introduced to address these challenges. In Section IV, we introduce multiple AI-based schemes to tackle technical challenges

In the future, IoT networks may be configured with a control center to provide centralized control to be compatible with existing cellular mobile networks, or may be designed in a distributed fashion for better flexibility and scalability.

that may be encountered in distributed IoT networks. Finally, we conclude the article in Section V.

II. Network Architecture

To be compatible with existing cellular mobile networks such as the third Generation Partnership Project (3GPP) Long-Term Evolution (LTE)/LTE-Advanced, IoT networks may be configured with a control center to provide centralized control. On the other hand, for better flexibility and scalability, IoT networks may be also designed in a distributed fashion. Therefore, in this section, the frameworks of both centralized and distributed IoT networks will be discussed.

A. Centralized IoT Networks

Currently, centralized IoT networks based on cloud computing technologies or fog computing technologies are widely studied due to their remarkable advantages [16]–[18]. As shown in Fig. 1, cloud computing technologies based IoT networks consist of three main components: remote radio head (RRH) networks, fronthaul networks, and baseband cloud units. In such networks, all the functions originally implemented in base stations (BSs) and core networks, including storage, signal processing, scheduling, power control, computations, access control, and mobility management, and so on, are migrated to the cloud [19], [20]. With powerful cloud technologies, these functions could be executed efficiently and robustly. Furthermore, since only radio frequency (RF) units are remained in front ends, the complexity and operational cost of RRH networks will be greatly reduced. Fronthaul networks are used to establish connections and manage information exchanges between RRH networks and the cloud, which normally adopt wired physical mediums, such as cable and fiber, to enable high data rate and low latency data delivery. Based on the control information and signaling from the cloud, IoT users will conduct data transmissions and send feedback information to the cloud, such as channel state information (CSI), measurements report, and ACK/NACK signaling. Based on the feedback information, the cloud will reconfigure transmission parameters for all IoT users to maintain communication quality. All the transmissions between IoT users and the cloud will be forwarded by RRH networks and fronthaul networks.

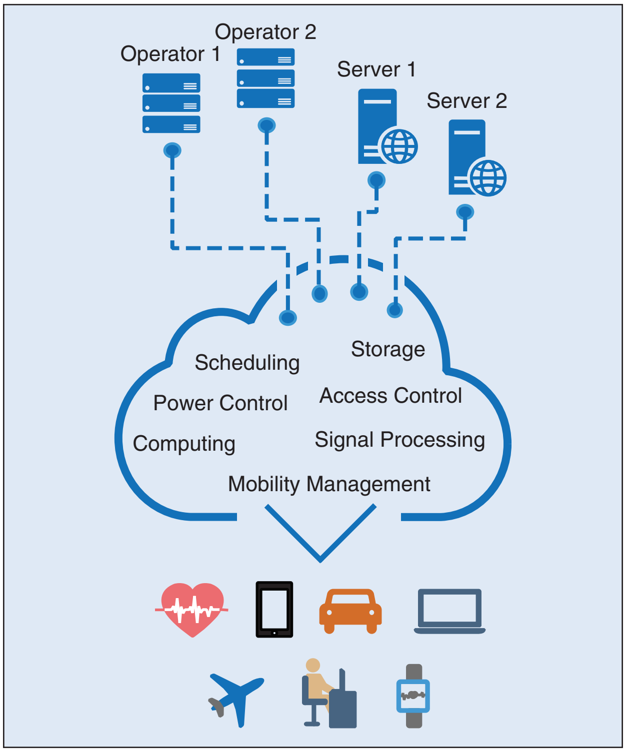

FIGURE 1 The architecture of centralized IoT networks.

Obviously, centralized control could achieve good performance for IoT networks, since complicated algorithms and mechanisms could be employed to globally optimize network performance [21], [22]. However, the overhead of computations and signal processing would exponentially increase with the growing number of IoT users. Therefore, centralized IoT networks will introduce substantial control overhead due to a large number of IoT users. Furthermore, centralized control will restrict the flexibility and scalability of the underlying IoT network, since IoT users may be required to follow the same protocol. For example, to conduct channel measurements, the control center in Fig. 1 may need to conduct measurement configurations for all IoT users within the network, based on which IoT users insert user-specific pilots, also referred as to reference signals (RSs), in their physical (PHY) radio frames [23]. Additionally, effective measurements of user-specific pilots require the underlying pilots from different users to be synchronized and orthogonalized.

B. Distributed IoT Networks

Based on the above discussions, distributed IoT networks may be more appealing compared with the centralized ones due to low complexity, high flexibility, and high scalability [24]. The architecture of distributed IoT networks can be seen most clearly in Fig. 2. Fig. 2 shows a low-complexity architecture that a distributed IoT network can be configured to. In distributed IoT networks, only low-complexity access points (APs) are needed to be deployed with simplified protocol stacks. For example, for PHY and medium access control (MAC) layers, an AP only needs to fulfill some simple functions, such as modulation/demodulation, coding/decoding, and automatic repeat request, while IoT users are required to carry out other functions individually and distributively, including adaptive modulation and coding, multiple access, power control, and so on. The core network that connects with APs through cable or fiber consists of four main components, namely mobility management entity (MME), serving gateway (SGW), packet data network gateway (PDN-GW), home subscriber server (HSS), which are in charge of the system procedures related to mobility management, security, internet protocol (IP) data traffic delivery, access authorization, and subscriber-related information storage.

The probability that random access collisions occur will increase with the growth of the number of IoT users. As a result, in IoT networks with a large number of users, random access collisions may be a significant issue.

III. Artificial Intelligence-Based Approaches in Centralized IoT Networks

In this section, we analyze potential design challenges in centralized IoT networks and introduce corresponding AI technologies to address them.

A. Challenges of Contention-Based Random Access

Although powerful cloud computing technologies could enable centralized IoT Networks to possess low system complexity, efficient signal processing, and high-performance centralized resource management, many challenges still exist. For example, initial access can be extremely challenging considering the large number of underlying IoT users. Initial access is a procedure that users establish initial wireless connections with RRHs, which is realized by the contention-based random access (CRA) procedure [25]. Fig. 3 shows the detailed processes of the CRA procedure: First, when an IoT user attempts to start the procedure, it has to arbitrarily select a random access resource, including a preamble and a physical random access channel (PRACH), from a random access resource pool. At the stage of random access, all IoT users have to behave in a non-cooperative mode. Then, IoT users will send the randomly selected preamble on the randomly chosen PRACH. Since different preambles are orthogonal, random access collisions occur only if multiple users choose the same preamble and the same PRACH. Upon collisions, the control center may fail to recognize the transmitted preamble and the IoT users have to restart their random access processes. On the other hand, the control center may successfully receive the preamble, but it cannot figure out which users send the underlying preamble, as these IoT users have not been connected and registered in the underlying IoT network. In this case, the control center will schedule wireless resources for the IoT users that collide with each other to allow them to perform first transmissions. Then, these IoT users will use the same wireless resources to carry out their first transmissions, causing collisions again. Apparently, in this case, the signals of only one user can be successfully received by the network, while the signals of other users will be treated as noises or interferences. The user with its signals successfully received will survive in the random access contention, while other users have to restart their random access processes.

Random access collisions will result in serious transmission latency and even transmission outages. The probability that random access collisions occur will increase with the growth of the number of IoT users. As a result, in IoT networks with a large number of users, random access collisions may be a significant issue. One way to improve the probability of successful random

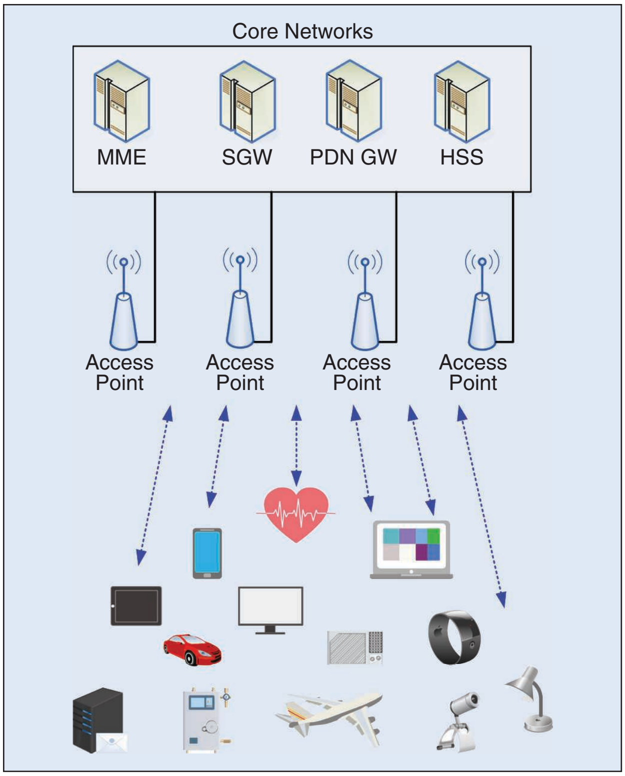

FIGURE 2 The architecture of distributed IoT networks.

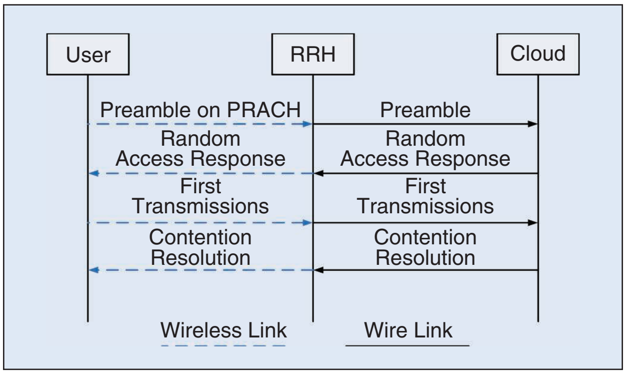

FIGURE 3 The processes of contention-based random access.

access is to adopt a greedy strategy under which the device sends multiple preambles on multiple PRACHs. By this way, the data link will be established as long as one of the preambles does not encounter collisions. In the sense of increasing the success probability of a single user, the greedy strategy seems to be a good choice. However, if a lot of users in IoT networks follow this strategy, collisions will dramatically increase and the network may break down. Therefore, the devices in an IoT network need to behave greedily at a proper level to maximize the overall random access performance. Conventional algorithm-based approaches may be difficult to resolve this problem since the number of users which try to access the IoT network is unknown as a priori. In this article, we resort to the more efficient and overhead-friendly approaches based on AI to intelligently adjust the greedy level of IoT users.

B. Contention-Based Random Access with Artificial Intelligence

Before establishing connections with the RRH networks and the cloud, IoT users need to carry out random access independently and competitively. As a result, labeled data related to random access parameters are infeasibly obtained. To improve the access probability, deep reinforcement learning (DRL) can be employed to facilitate IoT users to make proper decisions on the number of random access resource blocks used in one random access. A random access resource block can be denoted by a tuple (i, j) which refers to using i-th preamble and j-th PRACH. Each IoT user possesses independent neural networks to perform DRL individually. We assume that there are totally N random access resource blocks. Here, the action in reinforcement learning is defined as the number of random access resource blocks used in one random access. Accordingly, the output layer of a neural network consists of N neurons. Let the n-th neuron represent the action of using n random access resource blocks in one random access, $n = 1, 2, \ldots, N$. On the other hand, the state should provide the information on the action selected in the last random access and the corresponding reward. For example, if the last selected action is to use n random access resource blocks and the corresponding obtained reward is r, the current state could be represented by a vector, namely $[0, \ldots, 0, 1, 0, \ldots, 0, r]$, in which the n-th element and the $(N+1)$-th element are 1 and r, respectively, while the others are 0. Accordingly, the input layer consists of $N+1$ neurons, and the i-th element of the state vector will be input into the i-th neuron of the input layer, $i = 1, 2, \ldots, N+1$. Fig. 4 gives a simple example of the neural network based on the feed forward neural network (FFNN) [26] under the assumption that the total number of random access resource blocks is 4. The definition of the reward is of critical importance to the system performance: more reward should be given if an IoT user can conduct random access successfully. On the other hand, the reward should also take into account the impact of using multiple random access resource blocks instead of a single resource block, as using multiple random access resource blocks may potentially bring more collisions. Hence, the reward can be defined as follows.

$$r = A \cdot 1\{\text{The random access is successful}\} - \epsilon \cdot n, \tag{1}$$

where A and n denote the value of the reward brought by one successful random access and the number of random access resource blocks used in this random access, respectively. $1\{\cdot\}$ is the indicator function. It equals to 1 if the underlying random access is successful, otherwise, it is 0. ϵ stands for a weight to adjust the impact of n on the reward.

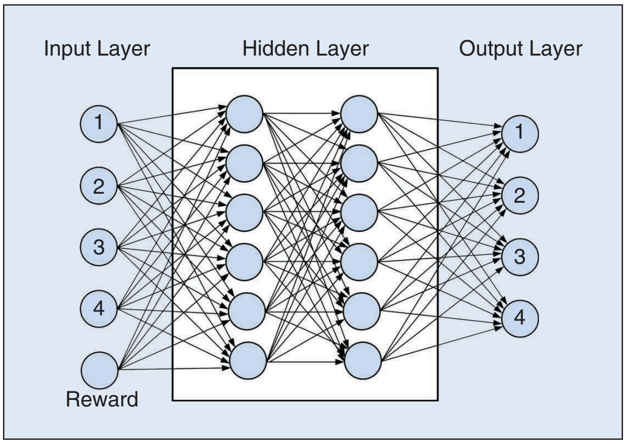

FIGURE 4 Neural network based on FFNN.

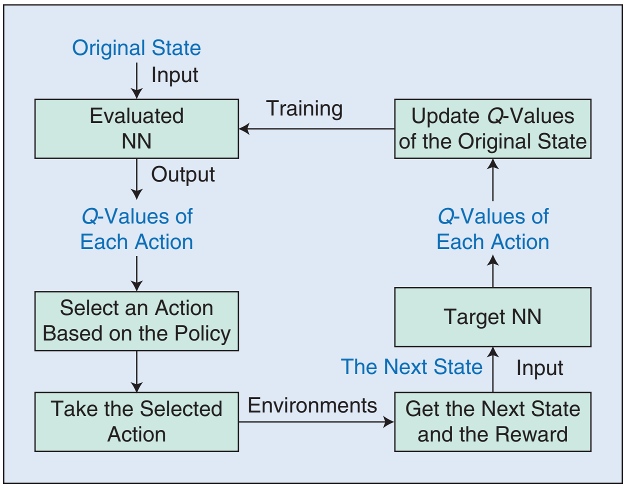

FIGURE 5 Online training of Deep Q-network.

C. Training Process of Deep Q-Network

Fig. 5 illustrates the online training process of the deep Q-network (DQN), in which two neural networks are used, namely an evaluated NN and a target NN [27], for DRL. After inputting an original state into the evaluated NN, Q-values of each action will be generated. Then, an action will be selected according to a predefined policy such as $\varepsilon-$greedy. After taking the selected action, the corresponding reward will be obtained and the state will be updated. The updated state will be input to the target NN to output

Q-values of each action. With Q-values generated by the target NN and the obtained reward, the Q-value of the original state and the selected action will be updated according to (2), which will be adopted as the target value to train the evaluated NN by the back-propagation algorithm. After several rounds, the target NN can be updated via replacing it with the evaluated NN, i.e.,

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \cdot \left[r_{t+1} + \gamma \cdot \max_{a_{t+1}} Q(s_{t+1}, a_{t+1}) - Q(s_t, a_t) \right], \tag{2}$$

where s_t, s_{t+1}, a_t, and a_{t+1} represent the original state, the updated state, the action selected based on Q-values of ENN, and the action selected based on Q-values of TNN, respectively. Besides, r_{t+1}, $\alpha \in (0,1)$, and $\gamma \in [0,1]$ denote the obtained reward, the learning rate, and the discounted rate, respectively.

IV. Artificial Intelligence-Based Approaches in Distributed IoT Networks

In distributed IoT networks, IoT users have to adjust transmission parameters individually without cooperations among IoT users and coordinations from the centralized control. AI-based techniques can support IoT users to adjust their transmission parameters intelligently for performance improvement.

A. Challenge of Spectrum Access

Due to the limited available spectrum, it is challenging for IoT network operators to acquire standalone licensed frequency bands. Alternatively, IoT networks may need to leverage available access opportunities in unlicensed frequency bands, such as industrial, scientific, and medical (ISM) bands, and unlicensed national information infrastructure (UNII) bands. Recently, the United States Federal Communication Commission (FFC) has opened up under-utilized licensed bands for unlicensed use. For example, the AWS-3 bands, including 1,695–1,710 MegaHertz (MHz), 1,755–1,780 MHz, and 2,155–2,180 MHz bands, and 3.5 GigaHertz (GHz) bands (3,550–3,700 MHz) have been opened up for dynamic spectrum access [28]. Despite these encouraging access opportunities, spectrum access on unlicensed bands will face many challenges. First, on some unlicensed bands especially for opened licensed bands, IoT users may share spectrum with primary users (PUs) with high priorities. These PUs should be protected from detrimental interference. For example, IoT network operators that attempt to access AWG-3 bands need to treat the federal meteorological-satellite systems as PUs [28]. Second, due to the lack of cooperations and coordinations, each IoT user has to conduct spectrum access individually with limited side information [29]. An IoT user may only be able to detect the channel gain of the links between its own transmitter and receiver, while the assumption of channel state information of different IoT users becomes unrealistic. Thus, conventional algorithm-based spectrum access methods cannot be directly applied.

Due to the difficulty of acquiring labeled data in distributed IoT networks, a DQN based spectrum access strategy is introduced for intelligent spectrum access.

B. Artificial Intelligence-Based Spectrum Access

Due to the difficulty of acquiring labeled data in distributed IoT networks, a DQN based spectrum access strategy is introduced for intelligent spectrum access. In the introduced strategy, spectrum sensing results will be adopted as the state in DRL. It is assumed that there are M channels available for IoT users. The state can be expressed as a spectrum sensing vector, $[s_1, s_2, \ldots, s_M]$. If the m-th channel is sensed to be idle, $s_m = 0$, otherwise $s_m = 1$, $m = 1, 2, \ldots, M$. Accordingly, a neural network is used to perform DRL where the input layer consists of M neurons. The m-th element in the spectrum sensing vector will be input into the m-th neuron in the input layer. Meanwhile, the output layer also consists of M neurons, where the m-th neuron represents the m-th channel. Fig. 6 shows an example of the neural network based on the recurrent neural network (RNN) with three available channels. The reward could be defined as

$$r = \sum_{j=1}^{M} \log_2(1 + SINR_j) - \varepsilon \cdot B \cdot 1_j\{\text{Collide with PUs}\}, \tag{3}$$

where $SINR_j$ represents the signal-to-interference plus noise ratio (SINR) of received signals on channel j. ε and B are the weight and the penalty caused by colliding with PUs on channel j, respectively. Online training will be applied to train the underlying DQN, enabling DQN to adapt to wireless environment variations, the processes of which have been presented in Fig. 5.

C. Challenge of Spectrum Sensing

Spectrum sensing is performed to harvest available channels or idle channels during spectrum access. As shown in Fig. 7, some

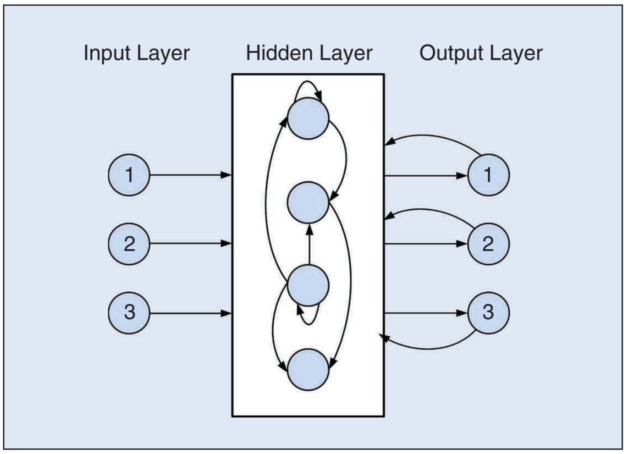

FIGURE 6 Neural network based on RNN.

In distributed IoT networks, accurate labeled data may be difficult to be obtained, therefore, a DRL-based spectrum sensing scheme is introduced to seek for the proper spectrum sensing frequency.

disjoint sensing slots are inserted into each radio frame to periodically check the availability of channels [30]. One of the most important parameters during this process is the sensing frequency which measures the density of sensing slots in a radio frame. High sensing frequency requires more wireless resources to conduct spectrum sensing and will result in low data transmission efficiency. On the other hand, it also provides accurate and timely sensing results. To improve the network performance, the spectrum sensing frequency should be adjusted based on the underlying wireless environments. For example, in fast time-varying environments, frequent spectrum sensing should be conducted to timely track the availability of channels. Therefore, it is important to have a robust design that is capable of intelligently adjusting the sensing frequency in response to the time-varying and dynamic environments.

D. Artificial Intelligence-Aided Spectrum Sensing

We assume that the maximum number of sensing slots to be inserted into a radio frame is K, and the length of a sensing slot is a fixed value τ. Sensing slots are uniformly distributed in a radio frame as shown in Fig. 7. In distributed IoT networks, accurate labeled data may be difficult to be obtained, therefore, a DRL-based spectrum sensing scheme is introduced to seek for the proper spectrum sensing frequency. The action of reinforcement learning is defined as the number of sensing slots that are inserted into a radio frame. Consequently, the output layer is composed of K neurons where the k-th one corresponds to the action of using k sensing slots in a radio frame, $k = 1, 2, \ldots, K$. The state is composed of two parts, including the actions chosen during the last attempt and the corresponding reward. As an instance, if the last selected action is using k sensing slots and the corresponding reward is r, the state can be given as a vector $[0, \ldots, 0, 1, 0, \ldots, 0, r]$ with the k-th element being 1, the $N+1$-th element being r, and 0 otherwise. Accordingly, $N+1$ input neurons should be included in the input layer, in which the i-th element in the state vector is adopted as the i-th input. Fig. 8 gives an example of the neural network based on reservoir computing (RC) under the maximum number of sensing slots of 3. The definition of the reward should consider the trade-off between spectrum sensing accuracy and transmission efficiency. Consequentially, the reward could be defined as

$$r = T_{\text{eff}} - \epsilon \cdot k \cdot \tau, \tag{4}$$

where T_{eff} represents the effective transmission time calculated by $T_{\text{eff}} = mT$. m and T are the number of collision-free data transmission phases and the length of each data transmission phase, respectively. k denotes the number of spectrum sensing slots to be inserted into a radio frame. ϵ is a predefined constant to adjust the weights between spectrum sensing accuracy and transmission efficiency. The online training processes have been described in Fig. 5, which could enable each IoT user to learn and attain an appropriate spectrum sensing frequency.

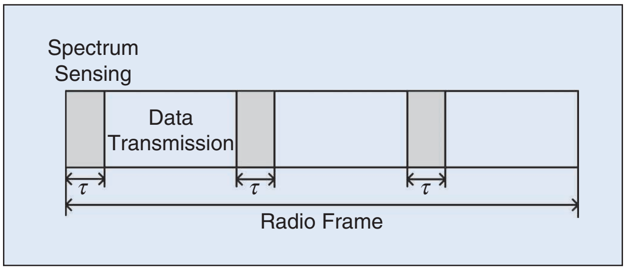

FIGURE 7 Spectrum sensing.

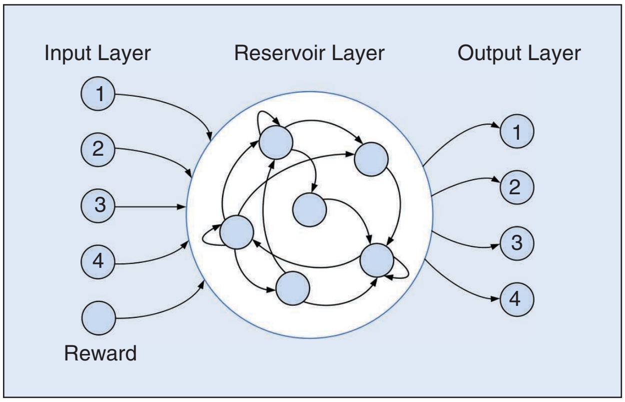

FIGURE 8 Neural network based on RC.

E. Selection of Underlying Neural Network Architectures

The types of neural networks should be selected carefully since they will directly impact the performance of the DQN. The FFNN is a basic neural network architecture, which has been widely applied in multiple applications in practices [31]. As shown in Fig. 4, the most significant feature of FFNN is its simple structure, in which signals only travel in the feed-forward direction. This feature makes FFNN easily trained, which is important for IoT networks [32]. However, the downside is that FFNN can not fully capture the underlying temporal correlation among the data which is critical for IoT networks due to the dynamic nature of the environment. On the other hand, the RNN is a powerful neural network that can explore the temporal correlation nature of the underlying data. In RNN, the activation updates of neurons in hidden layers, also referred to as recurrent neurons, need to take into account not only current input signals but also previous signals from recurrent neurons and output neurons, as shown in Fig. 6 [31]. In this way, RNN is able to create combinations of current and historic input signals and learn temporal correlations in dynamic systems. For example, RNN have been widely used in natural language processing, where sentences generally need to be understood based on both the current sentences and previous sentences [33]. Thus, RNN may be a better choice for IoT networks to learn the dynamics of the underlying wireless environments. However, the training process of RNN is complicated [34], [35] which is too difficult to be applied in IoT networks. To cope with that, the RC could be an alternative method to significantly reduce the underlying training. As shown in Fig. 8, RC is a special type of RNN, in which only the weights in output layer will be trained, while the other weights in the input layer and reservoir layers are fixed and generated randomly [36]. In this way, the difficulty of training RNN is significantly alleviated, while the feature of the temporal correlation still remains. It is shown that RC can be easily trained to conduct spectrum access for dynamic spectrum access networks [29] and high-rate symbol detection [37] for wireless networks. As a result, the RC can be an ideal neural network candidate for IoT networks.

V. Conclusion

IoT is a novel paradigm to interconnect massive wireless devices, which has the potentials to be applied in diverse applications and fields. However, due to a huge number of wireless devices in IoT networks, many technical challenges need to be addressed. In this article, we first have discussed potential architectures to construct IoT networks and design the frameworks for both centralized and distributed IoT networks. Furthermore, the possible technical challenges in our designed IoT networks have been analyzed. Then, AI-based solutions have been discussed to address these challenges related to random access, spectrum access, and spectrum sensing. To facilitate IoT users to choose transmission parameters individually and intelligently, reinforcement learning is employed, which is a model-free method to achieve good system performance without relying on accurate labeled data. Furthermore, for better efficiency, DQN has been used to conduct efficient online training for reinforcement learning. Finally, the advantages and disadvantages for different types of neural networks to be used in IoT networks have been discussed. We would like to envision that AI-enabled hyper-connected devices and world would become an important part in 5G networks and a core part of the future 6G networks. AI may greatly support Internet of things in different ways for PHY, MAC, network, transport, and application layers.

Acknowledgment

The work of H. Song, J. Bai, Y. Yi and L. Liu is supported in part by U.S. National Science Foundation (NSF) under grants ECCS-1802710, ECCS-1811497, and CNS-1811720.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[2] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," vol. 1, no. 1, pp. 22–32, Feb. 2014.
[4] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sept. 2012.
[5] J. An, K. Yang, J. Wu, N. Ye, S. Guo, and Z. Liao, "Achieving sustainable ultra-dense heterogeneous networks for 5G," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 84–90, Dec. 2017.
[6] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET CPS: Theory Appl.*, vol. 2, no. 1, pp. 49–54, Apr. 2017.
[7] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sept. 2018.
[8] "Gartner says the internet of things will transform the data center," Gartner Inc., 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2684616
[9] M. R. Palattella et al., "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
[10] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, June 2018.
[11] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of Things: Challenges and opportunities," in *Internet of Things*. Berlin: Springer-Verlag, Jan. 2014, pp. 1–17.
[12] H. Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, "Advertising in the IoT era: Vision and challenges," *IEEE Commun. Mag.*, Nov. 2018.
[13] S. Li, G. Oikonomou, T. Tryfonas, T. M. Chen, and L. D. Xu, "A distributed consensus algorithm for decision making in service-oriented internet of things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1461–1468, May 2014.
[14] V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," *Future Gen. Comput. Syst.*, vol. 83, pp. 619–628, June 2018.
[15] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digital Commun. Netw.*, vol. 4, no. 3, pp. 161–175, Aug. 2018.
[16] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero, and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog computing, cloud computing, and more fog computing," in *Proc. IEEE 19th Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Athens, Greece, Dec. 2014, pp. 325–329.
[17] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. 1st Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, Aug. 2012, pp. 13–16.
[18] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating Internet of Things and cloud computing and the issues involved," in *Proc. 11th Int. Bhurban Conf. Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, Jan. 2014, pp. 414–419.
[19] H. Song, X. Fang, and Y. Fang, "Millimeter-wave network architectures for future high-speed railway communications: Challenges and solutions," *IEEE Wireless Commun. Mag.*, vol. 23, no. 6, pp. 114–122, Dec. 2016.
[20] H. Song, X. Fang, and C.-X. Wang, "Cost-reliability tradeoff in licensed and unlicensed spectra interoperable networks with guaranteed user data rate requirements," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 1, pp. 200–214, Nov. 2017.
[21] M. Hassanalieragh et al., "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges," in *Proc. IEEE Int. Conf. Services Computing*, New York, NY, June 2015, pp. 285–292.
[22] T. Baker, M. Asim, H. Tawfik, B. Aldawsari, and R. Buyya, "An energy-aware service composition algorithm for multiple cloud-based IoT applications," *J. Netw. Comput. Appl*, vol. 89, pp. 96–108, July 2017.
[23] *Evolved Universal Terrestrial Radio Access (E-UTRA)*, 3GPP TS 36.214 V10.1.0.
[24] C. Sarkar, S. N. A. U. Nambi, R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini, "DIAT: A scalable distributed architecture for IoT," vol. 2, no. 3, pp. 230–239, June 2015.
[25] *Evolved Universal Terrestrial Radio Access: Medium Access Control Protocol Specification*, 3GPP TS 36.321 V12.7.0.
[26] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Netw*, vol. 61, pp. 85–117, Jan. 2015.
[27] H. Van Hasselt, A. Guez, and D. Silver, "Deep reinforcement learning with double Q-learning," in *Proc. AAAI*, 2016, pp. 2094–2100.
[28] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 2, pp. 110–128, July 2016.
[29] H. Chang, H. Song, Y. Yi, J. Zhang, H. He, and L. Liu, "Distributive dynamic spectrum access through deep reinforcement learning: A reservoir computing based approach," vol. 6, no. 2, pp. 1938–1948, Apr. 2019.
[30] S. Stotas and A. Nallanathan, "Optimal sensing time and power allocation in multiband cognitive radio networks," *IEEE Trans. Commun.*, vol. 59, no. 1, pp. 226–235, Jan. 2011.
[31] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, *Deep Learning*. Cambridge, MA: MIT Press, 2016.
[32] R. S. Scalero and N. Tepedelenlioglu, "A fast new algorithm for training feedforward neural networks," *IEEE Trans. Signal Process.*, vol. 40, no. 1, pp. 202–210, Jan. 1992.
[33] T. Mikolov, M. Karafiát, L. Burget, J. Černockỳ, and S. Khudanpur, "Recurrent neural network based language model," in *Proc. 11th Annu. Conf. Int. Speech Communication Association*, Makuhari, Chiba, Japan, Sept. 2010, pp. 1045–1048.
[34] R. Pascanu, T. Mikolov, and Y. Bengio, "On the difficulty of training recurrent neural networks," in *Proc. Int. Conf. Machine Learning*, Atlanta, GA, Feb. 2013, pp. 1310–1318.
[35] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult," *IEEE Trans. Neural Netw.*, vol. 5, no. 2, pp. 157–166, Mar. 1994.
[36] M. Lukoševičius, "A practical guide to applying echo state networks," in *Neural Networks: Tricks of the Trade*. Berlin: Springer-Verlag, 2012, pp. 659–686.
[37] S. Mosleh, L. Liu, C. Sahin, Y. R. Zheng, and Y. Yi, "Brain-inspired wireless communications: Where reservoir computing meets MIMO-OFDM," vol. 29, no. 10, pp. 4694–4708, Oct. 2018.