Large-Scale Multiobjective Federated Neuroevolution for Privacy and Security in the Internet of Things

Xin Liu, Jianwei Zhao, Jie Li, Dikai Xu, Shan Tian, and Bin Cao

Abstract

With the development of communication techonologies, Internet of Things (IoT) devices will be deployed in more and more places and generate large amounts of data. The corresponding analysis of these newly available data will greatly improve our daily lives. However, these IoT devices can be attacked. Traditional intrusion detection systems (IDSs) usually use a centralized approach to transmit data to the cloud or a central server for analysis. This method has a great risk of privacy leakage. Federated learning (FL) is an excellent distributed learning stategy, which will have outstanding performance in preventing privacy leakage for IDSs in IoT. However, the FL-driven IDS is still in the infancy stage and needs further exploration. Therefore, we propose a large-scale multiobjective federated neuroevolution framework based on a deep fuzzy rough convolution neural network for IoT privacy and security.

Introduction

The Internet of Things (IoT) can generate lots of data. Various IoT devices can help us provide intelligent services. For example, wearable sensors can perceive physiological signals in the body to monitor people's health [1]. Moreover, IoT devices also can monitor surgery in the hospital, detecting the life state of people in real time. IoT plays an important role in our work and lives. Correspondingly, security and privacy protection become essential in IoT systems. Privacy protection includes protecting information that has significant commercial value related to personal identity. In the IoT system, every connected device is a potential entry point. However, the complexity and security vulnerabilities of the IoT system are caused by factors such as interoperability and mixing, which makes the issues of security and privacy extremely important.

Cheap hardware costs will drive the spread of IoT devices at an alarming rate. However, IoT devices are vulnerable to cyber attacks while generating large amounts of data. IoT architecture mainly includes the sensing layer, network layer, and application layer. Some information can be shared in IoT, which realizes cooperation between devices and performs specific intelligent tasks. However, the exchange of information among different layers will lead to potential security threats such as leakage of sensitive information. This requires ensuring secure access when designing and operating the IoT system, securing the privacy information in IoT systems. The security of IoT needs to be protected. Software-defined network and the blockchain have the characteristics of scalability and efficiency, and these techniques can be used to protect security and privacy in IoT. Especially, the intrusion detection system (IDS) has become an important tool for IoT security [2]. Sometimes intrusion detection is regarded as the second security gate behind the firewall, providing real-time protection against internal and external attacks. Traditional deep-learning-driven IDS is usually a centralized processing method that requires uploading data to the cloud or central servers, where great risks of privacy leakage may exist.

The authors are with Hebei University of Technology, China.

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant No. 61976242, in part by the Natural Science Fund of Hebei Province for Distinguished Young Scholars under Grant No. F2021202010, and in part by the Fundamental Scientific Research Funds for Interdisciplinary Team of Hebei University of Technology under Grant No. JBKYTD2002. This work is also supported by 2022 Interdisciplinary Postgraduate Training Program of Hebei University of Technology under Grant No. HEBUT-Y-XKJC-2022122.

Digital Object Identifier: 10.1109/IOTM.001.2100179

The emergence of federated learning (FL) provides the novel privacy protection methods for data in IoT [3]. On the Internet of Medical Things (IoMT), medical data are distributed on individuals, hospitals, and different mobile medical devices, and the data cannot be simply transmitted to the central processing equipment, because there are great risks of data leakage and network intrusion in the process of information transmission. FL is a kind of distributed machine learning method based on decentralized data. An effective mobile healthcare service system can be designed by considering privacy and security. While making full use of existing technologies and considering privacy and security, adequate models should be constructed for processing data generated by wearable healthcare devices. Wearable IoT can be used for continuous healthcare services, and the FL models can be used for helping diagnose diseases without leaking personal privacy [4]. Meanwhile, FL can be applied for intrusion detection by using an adversarial approach [5].

Neuroevolution strategies attempt to search efficient architectures for specific deep learning tasks with minimal human intervention. The IoT intrusion detection problem can be seen as a complex classification problem, which can be solved by deep learning methods such as a deep fuzzy rough convolution neural network (DFRCNN). The manual design of architecture is not only time-consuming but also may not have optimal performance. Therefore, we focus on using evolutionary computation to automate the architectural design of neural networks (NNs). Evolutionary computation is inspired by evolutionary phenomena in nature, which can obtain optimal or suboptimal solutions for complex problems. In traditional evolutionary NNs, the precision is treated as the only objective. However, by simultaneously considering multiple objectives, multiobjective evolutionary computation are capable of considering more properties of multiobjective optimization problems (MOPs), allowing these problems to be better understood and optimized. In this study, we construct a federated deep fuzzy rough convolution neural network model based on neuroevolution (F-DFRCNN-NE) for solving the IoT security and privacy problems. This model can not only prevent Internet intrusion but also protect privacy in IoT.

For IoT intrusion detection, the proposed multiobjective F-DFRCNN-NE model uses neuroevolution to optimize the network architecture. It can automatically search for the best NN architecture with minimal manual intervention. The DFRCNN mode is used. Training of the F-DFRCNN model is formulated as a multiobjective problem by simultaneously considering classification precision, recall, and network simplicity.

 2576-3180/22/$25.00 © 2022 IEEE

Related Work

IoT Security

IoT connects diverse devices through networks and generates vast amounts of data, which creates great value and economic benefits. It also improves our quality of daily life. Data theft has become a hazard in IoT systems, because hackers can get amounts of benefits from sensitive data [6]. Although IoT makes everything connected, these communication techniques can lead to data leakage. FL is appropriate for decentralized data. An asynchronous FL method has been proposed for intrusion detection [7]. It could improve communication efficiency and quality of service. Deep learning has been used in intrusion detection. Big data technologies have also been proved to be useful in IoT security [8].

IDS is usually used for identifying intruders targeting information systems. These intruders often access IoT systems without authorization. Intruders include the masquerader, misfeasor, clandestine user, and others. The IDS can collect data, analyze data, and carry out an emergency response if abnormal or hostile activities are found. Researchers often adopt a hybrid method for intrusion detection with deep learning [9]. These methods belong to centralized processing methods. Although they can prevent Internet intrusion, privacy is not guaranteed.

Federated Learning

FL is a distributed learning method in which multiple clients cooperate to solve problems under the premise of privacy protection. It is a privacy protection model trained in heterogeneous and distributed networks. FL can train a practical deep learning model by multiple nodes cooperatively, without directly accessing local data. so it is a distributed learning method that can protect privacy. Different participants own data that are usually not evenly distributed in heterogeneous IoT systems, which can be solved by a hierarchical FL framework [10]. FL can be used for anomaly detection [11]. In the complicated and heterogeneous IoT system, intelligent cyber attack detection is an arduous task. The FL model can effectively discriminate cyber attack as well as maintain better resource allocation [12]. FL is appropriate for the data generated by decentralized IoT systems. However, FL that can be used for intrusion detection is still in its infancy, and more efficient FL methods need to be designed for IoT.

Neuroevolution

Neuroevolution strategies can explore the optimal architecture in a given search space. Good search space should not be constrained and have some flexibility. The search space can be divided into cell-based search space for block searching and global search space for searching the whole NN. Search strategies determine the method of searching basic architecture units for specific search tasks.

In this article, we mainly focus on evolutionary search strategies, which do not rely on attribute information such as differentiability. Neuroevolution can be dated back to many years ago. The basic idea is to use evolutionary computation for the optimization of NN parameters and architecture. We can reconstruct the architecture by inheriting the current network knowledge. Evolutionary computation can be used to search for the best architecture. Deep neuroevolution utilizing multiobjective evolutionary computation can simultaneously optimize more than one objective via considering several aspects of the NN. In this study, we use deep neuroevolution to attain high accuracy as well as minimal network complexity.

Large-Scale Multiobjective Federated Neuroevolution

Model Overview

In the FL system, to ensure privacy, participants often encode and encrypt the transmitted information during data communication. Meanwhile, the original user data are not transmitted to the central server. Therefore, training samples cannot be observed by the central server and model designer.

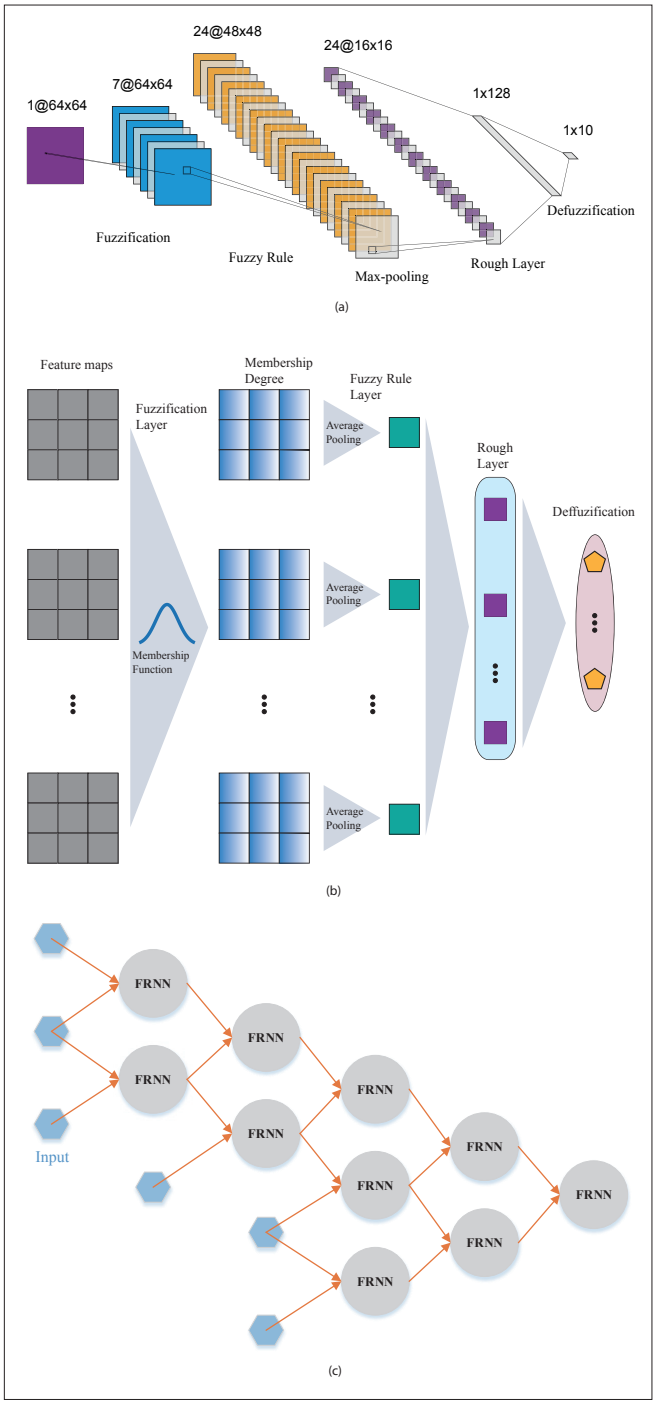

FIGURE 1. DFRCNN architectures: a) DFRCNN1; b) DFRCNN2; c) DFRCNN3.

The training process of a simple FL framework can be summarized as follows:

- The server establishes the basic model and informs each participant of the basic architecture and parameters of the model.
- Each participant uses local data for model training and uploads the model to the server.
- The server aggregates the models of all participants to build a global model to take all local information into account.

As shown in Fig. 1, we construct a DFRCNN in FL for IDS, then optimize this DFRCNN by neuroevolution. A DFRCNN model is constructed by introducing the fuzzy rough set theory into a deep convolutional NN (DCNN). Figure 1a shows a candidate DFRCNN

architecture. First of all, through the fuzzy layer, a series of fuzzy membership maps are generated. Then the fuzzy rule maps are generated by the convolutional fuzzy rule filter. Following is the pooling layer, which reduces the redundant information. Next, the fuzzy rules are transformed by the rough layer, and at the same time, each rough node corresponds to a consequence node. The final outputs are finally obtained by defuzzification. Figure 1b is an illustration of another architecture. As a feature extractor, the convolution layer can convert the original information into a series of feature maps. By removing the full connection layer, membership functions are utilized to generate the membership maps. The fuzzy rule layer is simulated by employing the average pooling layer, and the fuzzy rule strength is obtained by considering the membership degrees of input features. The fuzzy rough membership degree is obtained through the rough layer. Last, the final output is obtained by defuzzification. Figure 1c is also a DFRCNN architecture. The "FRNN" represents a fuzzy rough NN module; inputs are transformed features from the convolution layer. Each FRNN includes the fuzzification layer, the fuzzy rule layer, the rough layer, the consequence layer, and the defuzzification layer. The architecture is relatively simple, and has interpretability. Complex inputs are processed by deeply connecting multiple FRNN modules.

Encoding

For an NN, the network architecture can be represented by the number of network layers, node numbers, connection status, network module architecture, and others. Network parameters include connection weights, module parameters, and so on.

Activation Function: There are many activation functions, including Sign, Tanh, Softplus, Softsign, Sigmoid, ReLU, LeakyReLU, ELU, SELU, and so on. Model encoding takes into account the types of activation functions to dynamically select the appropriate type and improve network performance. Existing activation functions may have some limitations, and it is difficult to have excellent performance for all kinds of application problems, so the construction of novel activation functions can be explored.

Membership Function: For the fuzzy rough set, the number and formulation of membership functions are encoded. Candidate membership functions include Gaussian and Sigmoid, and so on. We can set the maximum number of membership functions for each input variable, and encode the type of each membership function and its parameters.

Encoding Scheme: We can encode all possible connections, including connections at the full connection layer, construction of fuzzy rules, and the connection between the fuzzy rule layer and the rough layer. Each variable represents the state of each connection. For connections with parameters, a variable can be used for encoding the weight of each connection. Network performance depends on multiple hyperparameters, including the number of layers, numbers of nodes, convolution kernel size, numbers of membership functions, and others. If the back propagation algorithm is used, the evolutionary algorithm is only responsible for the optimization of network architecture and hyperparameters, and does not encode parameters such as connection weights. If the evolutionary algorithm considers the optimization of network parameters, it will simultaneously encode the network architecture, hyperparameters, and parameters.

Evolutionary Operator

Different evolutionary operators have their own advantages. For specific neural evolution problems, it is necessary to test a variety of operators to find the dominant operator(s). At different stages of evolution, different operators (or operators with different parameters) also have different effects on the optimization performance. Different operators could be combined. Operators based on prior knowledge can be used. In the broad learning system, the weight parameters of the output layer can be obtained by the pseudo-inverse method. This strategy can be combined with the traditional evolutionary operator to ensure the fitting performance of the network while flexibly constructing the network architecture.

Large-Scale Evolution

Designing efficient grouping methods for large-scale problems is important for large-scale evolution. First, the variables of encoding architecture and encoding parameters are divided into different groups. Second, if there are still many variables in each group, it is planned to continue to divide. The partitioning strategies can be explored, including partition by network layer, partition by node, partition by module, matrix cutting, and so on.

Designing efficient cooperative coevolutionary methods is also important for large-scale evolution, especially for distributed parallel large-scale evolution. All variable groups need to be combined to form a complete solution, which can be decoded into an NN model to obtain each optimization objective value. In order to reduce information exchange frequency and communication cost as well as facilitate parallel deployment, each subpopulation of a variable group temporarily stores the information of variables in other groups. In addition, based on the temporary information, new information is generated using evolutionary operations such as crossover.

Optimization Objectives

Precision: For each input sample, an output vector whose size is the same as the number of categories in the classification problem is generated. The label that corresponds to the node with the maximum value is the prediction. By comparing each sample label prediction to the corresponding ground truth label, the classification precision for each category can be calculated, and by optimizing the average precision, the classification performance of the F-DFRCNN-NE model can be improved.

Recall: Precision indicates the ratio of correct predictions for one category among all predicted samples. From another perspective, the recall indicator reflects the ratio of samples that are correctly recognized for a category. By simultaneously considering both precision and recall, a classification model can achieve better classification performance.

Network Simplicity: To improve the generalization and interpretability of the network, network simplicity is optimized to generate networks with sparse connections. The ratio of the connections that are activated throughout the F-DFRCNN-NE model is minimized to generate simple networks via simultaneously considering the fuzzy rule layer and fuzzy rough membership layer.

Constraints: For each output node in the full connection layer that is not associated with the membership function, a penalty constant with an extremely large value will be added to all the objective functions. This step forces the optimization algorithm to generate valid networks in which data flow from the inputs to all the output nodes.

Available Datasets

For IDSs in IoT, it is necessary to have data sets containing normal and abnormal behaviors to evaluate the effectiveness of recognizing attacks. So far, there are many public data sets available for testing and evaluation in the field of network security.

The IoT Devices Captures dataset[1] represents the traffic generated during the setting of 31 smart home IoT devices of 27 different types. Each directory in the dataset represents a device, including the traffic data transmitted by the device and MAC address. Devices connect to the user network through WiFi or Ethernet, and some devices use other IoT protocols, such as ZigBee or Z-Wave. The devices are among the most common equipment related to intelligent lighting, home automation, safety cameras, home appliances, and health monitoring equipment. It is tedious for so many devices in the IoT to use the traditional intrusion detection algorithm. Using our framework can not only ensure the accuracy of intrusion detection, but also minimize the overhead of intrusion detection model.

The Car Hacking: Attack & Defense Challenge 2020 Dataset[2] is used to test the attack and detection technology of a controller area network (CAN). It contains the CAN messages of a vehicle in dynamic and static states. CAN messages of different vehicle states

are in different files. Each CAN message file contains normal and attack messages. Attack messages can be divided into four types: flooding, spoofing, replay, and fuzzing. The vehicle cyber has very high requirements for the accuracy and real-time activity of the intrusion detection model, so it is necessary to use our optimized NN with high recognition accuracy but low complexity.

The UNSW-NB15 dataset[3] was created by the IXIA PerfectStorm tool at the University of New South Wales in Australia. It contains 2,540,044 data pieces, each containing 49 features. There are 9 attack types containing exploit, worms, and more.

N-BaIoT datasets[4] are also available. Due to the proliferation of IoT devices and the fact that IoT devices are more vulnerable than desktop computers, resulting in many botnet attacks against IoT, N-BaIoT provides a public botnet dataset collected from nine real IoT devices in the lab. The collected malicious data is classified into two botnet types: BASHLITE and Mirai. To launch an attack, BASHLITE forcibly opens the default credentials of Telnet ports to infect IoT devices. The BASHLITE attack types are combo, Scan, junk, TCP, and UDP. Mirai attacks include scan Ack UDP Plain UDP and Syn attacks.

Future Directions

Interpretability is a meaningful research direction. FL can combine the interval-2 FRNN, increasing the model interpretibility. Deep NNs can combine fuzzy set and rough set, adding a fuzzy rough layer, using the fuzzy rough theory to describe the fuzzy rough membership degree, which describes the relationship between the inputs and the rough nodes, representing the uncertainty of information. Thus, the federated model can improve interpretability under the condition of protecting privacy.

In a federated environment, data is often heterogeneous on different mobile devices, and the assumption is that the mobile terminals and the central server are trusted. Therefore, we need to design more practical algorithms based on non-IID data. Due to data heterogeneity, lack of computing resources, communication costs, external attacks, and other factors, we cannot guarantee the participation of all users. Therefore, high quality data, reduced communication costs, rich computing resources, and others can be used to stimulate users' interest in participation, improving user engagement. Performance and efficiency of the FL model are important. Federated learning needs to train a large amount of high-quality data on the mobile terminals, and needs stable network connection and powerful terminal data processing capability, which tend to increase the model size and the cost of communications. In the future, a multiobjective neural architecture search algorithm can be used to automatically optimize network architecture and reduce communication time. In addition, with the rapid development of FL combined with other technologies, its testing standards need to be further unified.

Conclusion

Although deep learning for IDS in IoT systems has achieved success, the data need to be transmitted to the central server, which increases the risk of privacy leakage. In this study, we use an FL-driven IDS to classify normal and abnormal behaviors to evaluate the effectiveness of recognizing attacks. We construct an F-DFRCNN-NE model for IoT privacy and security. The federated neural evolution framework explores neural architecture based on evolutionary computation. It encodes network modules and connections, sets optimization variables, constructs search space, searches with evolutionary strategies, and generates desired neural architecture. In the process of federated neural evolution, the federated environment ensures information security. With the help of differential privacy, training data can be effectively protected and misappropriation can be prevented. Optimization variables can encode convolution, pooling, and full connection modules, as well as their attributes and parameters, and flexibly construct neural architecture through evolution. This F-DFRCNN-NE model can protect participants' privacy while defending them from cyber intrusion.

References

[1] Y. S. Can and C. Ersoy, "Privacy-Preserving Federated Deep Learning for Wearable IoT-Based Biomedical Monitoring," *ACM Trans. Internet Technology*, vol. 21, no. 1, Feb. 2021, pp. 21:1–17.

[2] B. B. Zarpelo, R. S. Miani, and C. T. Kawakani, "A Survey of Intrusion Detection in Internet of Things," *J. Network and Computer Applications*, vol. 84, Apr. 2017, pp. 25–37.

[3] X. Liu *et al.*, "Federated Neural Architecture Search for Medical Data Security," *IEEE Trans. Industrial Informatics*, vol. 18, no. 8, Aug. 2022, pp. 5628–36.

[4] H. Elayan, M. Aloqaily, and M. Guizani, "Deep Federated Learning for IoT-Based Decentralized Healthcare Systems," *2021 Int'l. Wireless Commun. and Mobile Computing*, 2021, pp. 105–09.

[5] I. Siniosoglou *et al.*, "Federated Intrusion Detection in NG-IoT Healthcare Systems: An Adversarial Approach," *IEEE ICC 2021*, Dec. 2021.

[6] W. Alhakami *et al.*, "Healthcare Device Security: Insights and Implications," *Intelligent Automation and Soft Computing*, vol. 27, no. 2, Mar. 2021, pp. 409–24.

[7] S. Agrawal *et al.*, "Temporal Weighted Averaging for Asynchronous Federated Intrusion Detection Systems," vol. 2021, Dec. 2021, pp. 1–10.

[8] M. A. Amanullah, R. A. A. Habeeb, and F. H. Nasaruddin, "Deep Learning and Big Data Technologies for IoT Security," *Computer Commun.*, vol. 151, Feb. 2020, pp. 495–517.

[9] K. Narayana Rao, K. Venkata Rao, and P. R. P.V.G.D., "A Hybrid Intrusion Detection System Based on Sparse Autoencoder and Deep Neural Network," *Computer Commun.*, vol. 180, Dec. 2021, pp. 77–88.

[10] A. A. Abdellatif *et al.*, "Communication-Efficient Hierarchical Federated Learning for IoT Heterogeneous Systems with Imbalanced Data," *Future Generation Comp. Sys. — Int'l. J. Escience*, vol. 128, Mar. 2022, pp. 406–19.

[11] D. Wu, Y. Deng, and M. Li, "FL-MGVN: Federated Learning for Anomaly Detection Using Mixed Gaussian Variational Self-Encoding Network," *Info. Processing & Management*, vol. 59, no. 2, Mar. 2022, p. 102,839.

[12] M. Abdel-Basset, H. Hawash, and K. Sallam, "Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System," *IEEE Trans. Industrial Informatics*, vol. 18, no. 3, Mar. 2022, pp. 1905–17.

Biographies

Xin Liu (202011701002@stu.hebut.edu.cn) eceived her Master's degree in economics from Jilin University, Changchun, China, in 2012. She is currently working toward a Ph.D. degree in management science and engineering with the School of Economics and Management, Hebei University of Technology, Tianjin, China. Her main research interests include intelligent computation with its applications to the Internet of Things and smart healthcare.

Jianwei Zhao (201422102003@stu.hebut.edu.cn) received his Master's degree in computer science and technology in 2018 from Hebei University of Technology, China, where he is currently working toward a Ph.D. degree in control theory and control engineering with the School of Artificial Intelligence. His main research interests include intelligent computation with its applications to the Internet of Things, big data, graphics and visual media, high-performance computing, and cloud computing.

Jie Li (lijie@hebut.edu.cn) received her Ph.D. degree in electrical engineering from Hebei University of Technology in 2002. She is currently a professor with the School of Economics and Management, Hebei University of Technology. Her research interests include big data analytics in smart healthcare, business, and finance.

Dikai Xu (202112801011@stu.hebut.edu.cn) received his Master's degree in computer technology from Changchun University of Technology, China, in 2021. He is currently pursuing a Ph.D. degree in control science and engineering with the School of Artificial Intelligence, Hebei University of Technology. His main research interests include multiobjective evolutionary learning with its applications to intrusion detection, neural architecture search, and lightweight neural networks.

Shan Tian (202022801024@stu.hebut.edu.cn) received his Bachelor's degree in vehicle engineering in 2018 from Shandong University of Science and Technology, China. He is currently working toward a Master's degree in control science and engineering with the School of Artificial Intelligence at Hebei University of Technology. His main research interests include intelligent computation with its applications to the Internet of Things, big data, graphics and visual media, high-performance computing, and cloud computing.

Bin Cao [SM] (caobin@scse.hebut.edu.cn) received his Ph.D. degree in computer application technology from Jilin University, Changchun, China, in 2012. From 2012 to 2014, he was a postdoctoral fellow with the Department of Computer Science and Technology, Tsinghua University, Beijing, China. He is currently a professor at Hebei University of Technology. His research interests include intelligent computation with its applications to the Internet of Things, big data, graphics and visual media, high-performance computing, and cloud computing.

Foonotes

[1] S. Marchal, Creator, 3 Apr 2017, IoT Devices Captures, Aalto Univ.; captures_IoT_Sentinel(.zip), doi: https://doi.org/10.24342/285a9b06-de31-4d8b-88e9-5bdba46cc161.

[2] H. Kang *et al.*, Feb. 3, 2021, "Car Hacking: Attack & Defense Challenge 2020 Dataset," *IEEE Dataport*. DOI: https://dx.doi.org/10.21227/qvr7-n418

[3] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," *Military Commun. and Info. Sys. Conf.*, 2015, IEEE, 2015. DOI: http://doi.org/10.1109/MilCIS.2015.7348942

[4] Y. Mirsky *et al.*, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," 2018; *Network and Distributed System Security Symp.*, San Diego, CA. DOI: http://dx.doi.org/10.14722/ndss.2018.23204