AI-based Intrusion Detection for Intelligence Internet of Vehicles

Dapeng Man, Fanyi Zeng, Jiguang Lv, Shichang Xuan, and Wu Yang
Harbin Engineering University

Mohsen Guizani
Mohamed Bin Zayed University of Artificial Intelligence

***Abstract*—With the development of intelligent technologies, Internet of Things (IoT) opens up a new era in the field of automotive networks, namely, Internet of Vehicles (IoV). The main goal of IoV is to provide a secure and reliable network to vehicles so that users can enjoy various services. However, vulnerabilities and incomplete protection mechanisms have led to a proliferation of security threats against IoV networks. Intrusion detection technology is an effective protection solution for IoV security, especially when artificial intelligence (AI) technology has been introduced into intrusion detection study. This article first briefly introduces the concept and features of IoV, and then reviews the related research on AI-based IoV intrusion detection systems. Finally, we discuss the open challenges and future research directions.**

WHAT IS INTERNET OF VEHICLES

The Internet of Vehicles (IoV) is an integration of traditional vehicular ad-hoc networks (VANETs) and Internet of Things (IoT). It is an extended application of the IoT in intelligent transportation. The IoV takes mobile vehicles as the carrier of information perception. It utilizes next-generation information and communication technologies, such as sensor network technology, radio frequency identification technology, wireless communication technology, and big data analysis technology to achieve all-around network interconnection.

The IoV will enable vehicles to utilize resources such as cloud storage and computing. In addition to safe driving of vehicles and convenience for urban traffic management, IoV will also provide auto insurance, road infrastructure

Digital Object Identifier 10.1109/MCE.2021.3137790
Date of publication 23 December 2021; date of current version 6 December 2022.

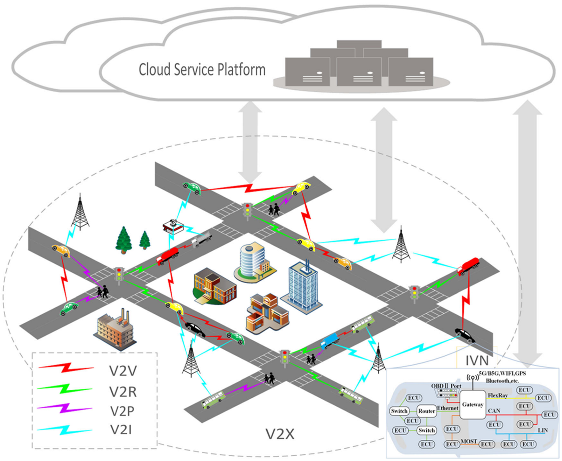

Figure 1. Architecture of the IoV.

construction and maintenance, logistics, and transportation. In a nutshell, the IoV aims to improve intelligence levels, automobilism capacity, and build fresh formats of transportation services. It will enhance transportation efficiency and driving experience, and provide users with comfortable, safe, intelligent, and efficient services.

Networking and intelligence are the future trends of IoV.[1] Single-vehicle intelligence has gradually changed to multivehicle intelligent collaboration. With the collaborative evolution of "smart vehicles" and "smart roads," the "terminal-management-cloud" vehicle networking ecosystem has become a typical solution for IoV.[1] From the perspective of network architecture, the "terminal" corresponds to the in-vehicle network (IVN) communication, and the "management" corresponds to the vehicle to everything (V2X) wireless communication. The first two parts together with the cloud service platform form the three-tier architecture of the IoV. Figure 1 depicts the three-tier architecture of the IoV.[2]

In the IVN communication, several buses (such as CAN, local interconnect network, FlexRay, media-oriented system transport, and Ethernet) not only connect various electronic control units (ECUs) in vehicles, but also connect various intelligent vehicle sensors and intelligent terminals to provide various services. For traditional fuel-based automobiles, the CAN is currently the most mature IVN communication protocol. V2X is mainly composed of vehicle-to-vehicle, vehicle-to-roadside, vehicle-to-pedestrian, and vehicle-to-infrastructure.[3] In V2X communication, dedicated short-range communications (DSRC) and long-term evolution-based vehicle to everything (LTE-V2X) are two mainstream V2X communication technologies. The IVN and V2X communication networks connect with the back-end cloud server through the backbone network behind, forming an organic combination of "people–vehicle–road–cloud.'' The cloud platform can provide unified data acquisition and intelligent decision-making services, and connect the whole vehicle network.

SECURITY THREATS IN IOV

Since the IoV is designed for V2X networks, there is usually no reliable infrastructure to support.[3,4] The lack of centralized supervision and the essential characteristics of mobile *ad hoc* networks to disseminate and share information has resulted in a remarkable increase in security risks. Meanwhile, the complexity of intelligent connected vehicle systems and the increase in external interfaces[5] make the vehicle network more vulnerable to cyberattacks. At present, the security threats involved in IoV mainly include the following: 1) vehicle security threat, 2) security threat for the IoV communication, 3) security threat for the IoV cloud platform, and 4) security threat for the IoV mobile smart terminals.

Researchers have simulated many attack scenarios in the past to explore potential vulnerabilities in IoV. Summarizing previous studies,[3–5] this article mainly discusses potential network attacks derived from the above mentioned security threats. Table 1 shows the types of attacks and their descriptions.

INTRUSION DETECTION FOR IOV

In recent years, reactive systems such as intrusion detection systems (IDSs) have been widely studied and practiced as complementary solutions to active security countermeasures (such as access control and encryption algorithms).[6] Due to the complexity of the IoV network topology, constraints of computing and storage resources, time sensitivity, high connectivity, and other characteristics, the traditional IDSs are not applicable in the face of various network attacks in the IoV field. Thus, the current intrusion detection research for IoV is in full swing.

Table 1. Types of attacks and their descriptions.

Serial number	Attack type	Description
1	DoS, DDoS attack	Occupying and controlling nodes or network resources by sending a lot of requests or unrelated data
2	Sniffing attack	Such as port scanning attacks, the goal of which is to steal confidential data of the vehicle system
3	Brute force attack	Cracking information such as the password of the vehicle network or system
4	Integrity attack	Spoofing attack, replay attack, wormhole attack, Sybil attack, etc.
5	Web attack	To invade the web pages of vehicles or node servers, attackers implement web attacks through SQL injection or cross site scripting (XSS)
6	Malware attack	Attackers inject into the system through vulnerabilities in the communication interface to cause attacks by the forms of the worm, viruses, spyware, etc.
7	Fuzzy Attack	Attackers force the vehicle into an unexpected state or malfunction by injecting random information
8	Other types of attacks	

Previously, research on intrusion detection for IoV showed a fragmented state.[4] Some researchers focus on intrusion detection research for IVN,[2,7] the CAN protocol does not provide security mechanisms such as message authentication or data encryption at the design stage, so for IVN security researchers, the CAN bus is the main object of research for IVN intrusion detection. Others focus on out-of-vehicle networks.[8–11] In this article, we will not conduct a separateness study, but conduct a comprehensive discussion of intrusion detection research on internal and external networks.

Considering the current research directions, the IoV intrusion detection technologies are classified as follows: misuse-based intrusion detection, anomaly-based intrusion detection, and based on hybrid or other intrusion detection.[12] Compared with the misuse-based method or other methods, the anomaly-based method is the most promising in the IoV intrusion detection field.[13] Anomaly-based methods will be able to monitor known and unknown attacks effectively, and artificial intelligence (AI) technologies such as machine learning (ML) are generally applicable to the problem of abnormal intrusion detection in IoV.

AI-BASED IDS FOR IOV

At present, a considerable part of the existing IoV intrusion detection models are based on AI. Compared with IDS based on non-AI, the AI-based IDS (such as ML-based IDS) has the advantage that it can automatically mine the specific models in the data that cannot be mined manually, and provides more accurate detection results. Previous studies, however, have only included AI-based IDS as part of the various approaches they have reviewed. This article goes beyond these previous works, and focuses specifically on the intersection between AI technologies, IIoV security threats, and intrusion detection research. We cover a range of increasingly important AI technologies for IoV intrusion detection; these technologies have not been discussed independently in previous studies. Table 2 provides a comparative summary of contemporary typical AI-based IDSs for the IoV. We take the detection performance, low latency, lightweight, and generalization ability as the basic performance that the AI-based IDS for IoV needs to meet. The proposed solutions may be deployed in the ECUs of a vehicle, the RSUs of a VANET,[14] or other deployment points. There are different IDS deployment strategies for different detection tasks.

Traditional ML methods: Many traditional ML methods have their unique advantages in feature extraction and classification. Alshammari *et al.*[13] clustered and further classified intrusion events in VANET through K-nearest neighbor and support vector machine algorithms. Yang *et al.*[4]

Table 2. Summary of contemporary typical AI-based IDSs for the IoV.

Main AI Technology	Key Reference	Model	Deployment Point	Attack Types Detected	Datasets	Satisfiable Performance			
						Detection Performance	Low Latency	Lightweight	Generalization Ability
Traditional ML methods	Yang *et al*. [4]	Tree	Both IVN and external network	DoS, Port Scan, Botnet, Infiltration Attack, Brute Force, Web Attack	Car Hacking for IVN, CICIDS2017 for external network	High	Discussed	Not discussed	Discussed
	Gao *et al*. [25]	RF	VANETs	DDoS Attack	NSL-KDD, UNSW-NB15	High	Not discussed	Not discussed	Discussed
	Angelo *et al*. [14]	K-Means	CAN	DoS Attack, Fuzzy Attack, RPM Attack, GEAR Attack	Car Hacking datasets of HCRL	High	Discussed	Not discussed	Not discussed
Deep Learning	Anzer *et al*. [16]	MLP	OBUs	DoS Attack, U2R Attack, R2L Attack, Probe Attack	KDD Cup 1999	High	Discussed	Satisfiable	Not discussed
	Vitalkar *et al*. [8]	DBN	VANETs	Not explicitly stated	ISCX2012	Not discussed	Not discussed	Not discussed	Not discussed
	Peng *et al*. [3]	CNN	The vehicle terminals	Not explicitly stated	Acquired experimentally	High	Discussed	Satisfiable	Not discussed
	Nie *et al*. [12]	DCNN	RSUs	DDoS Attack	Acquired experimentally	High	Not discussed	Not discussed	Not discussed
	Song *et al*. [26]		CAN	Fuzzy Attack, RPM Attack, DoS Attack, GEAR Attack	Acquired experimentally	High	Discussed	Not discussed	Discussed
	Zeng *et al*. [11]	CNN, LSTM	RSUs	Wormhole Attack, Sybil Attack, DoS, Infiltrating Transfer Attack, DDoS, Black Hole Attack, Brute Force attack	ISCX 2012, Acquired experimentally	High	Discussed	Satisfiable	Discussed
	Ashraf *et al*. [5]	LSTM	Both IVN and external network	Fuzzy Attack, RPM Attack, DOS Attack, GEAR Attack	Car Hacking for IVN, the UNSW_NB for external network	High	Not discussed	Not discussed	Discussed
	Liang *et al*. [9]	GHSOM	VANETs	False Information Attack, Sybil Attack	Acquired experimentally	High	Not discussed	Not discussed	Not discussed
Reinforcement learning	Seo *et al*. [7]	GAN	CAN	DoS Attack, Fuzzy Attack, RPM Attack, GEAR Attack	Acquired experimentally	High	Not discussed	Not discussed	Discussed

CNN= Convolutional Neural Networks, DCNN= Deep Convolutional Neural Networks, LSTM= Long Short-Term Memory, DBN= Deep Belief Network, MLP=Multi-Layer Perceptron, GHSOM= Growing Hierarchical Self-Organizing Maps, ANN= Artificial Neural Network, DDoS= Distributed Denial of Service, RF= Random Forest, GAN= Generative Adversarial Networks, RSU= Road-Side Unit, OBU= On-Board Unit, DoS= Denial of Service, U2R= User to Root, R2L= Remote to Local, RNN=Recurrent Neural Networks

proposed an intelligent IDS based on the previous study, which was widely suitable for detecting CAN bus and external network attacks. The tree-based ML algorithms, including random forest (RF), decision tree, extra tree, and extreme gradient boost, were used in the design. The stacked detection model was with an accuracy of more than 99%, but with a longer execution time compared to any single model. After using the synthetic minority oversampling technique for reducing the category imbalance and computational cost, however, high detection performance and low delay cannot be satisfied simultaneously.

Besides traditional ML algorithms, many advanced ML extension algorithms and models, for instance, deep learning (DL), have been applied to the study of IDS for IoV.[15] DL is a representation learning algorithm based on data, and it has many advantages that traditional ML methods do not have. It is able to use nonsupervised or semisupervised feature learning and hierarchical feature selection algorithms instead of manual characteristic acquisition. Many DL models have been applied to IoV intrusion detection, such as ANN, DNN, DBN, CNN, RNN, and GAN.

ANN/MLP: ANN has played a vital role in scientific research fields such as target classification and data fitting with its strong self-learning and self-adaptive capabilities. Since the model was proposed, various neural networks have appeared.[3,8] Researchers have applied various neural network models to the research of IoV intrusion detection.[9] MLP was the initial ANN design.[15] Anzer *et al.*[16] implemented a distributed intrusion detection system (DIDS) based on MLP to monitor malicious traffic in IoV. The researchers planned to install the DIDS in OBUs. Their IDS successfully detected different types of attacks, such as DoS, probe, R2L, and U2R. From the experiments, it can be understood that using a small number of selected features also has high detection accuracy, while reducing latency and complexity. However, there is still the limitation that the network must be deep enough to obtain better results.

DNN: DNN has more hidden layers than traditional ANN, the role of these hidden layers is very significant, and they give DNN superiority that can come from extracting high-level features from raw data. DNN has been extensively researched in the field of AI and is widely used in practical applications (e.g., image processing, speech recognition, and computer vision). The following types of models are extensions and improvements of the DNN model.

DBN: DBN is a DNN model superimposed by restricted Boltzmann machines; it is an effective means to deal with the problems of low speed and overfitting in the learning process of DNN. Vitalkar *et al.*[8] used DBN to realize intrusion detection on VANET. Their IDS output results can be binary classification and multiclass classification. Currently, there is not much research on applying DBN models alone as an algorithm for IoV intrusion detection, because DBN is more suitable as a means to understand the "philosophy" and "mindset" of DL.

CNN/DCNN: CNN is a DNN with a convolutional structure, and its application in the field of image processing is remarkable due to its characteristics of weight sharing and affine invariance.[15] Many researchers have applied CNNs to spatial mobile data analysis. Peng *et al.*[3] have designed a lightweight CNN-based IDS for vehicle terminals. By learning the data features in the network traffic graph, an image model of normal network traffic and abnormal network traffic was established, and the model was used to detect network data in real time. DCNN is structurally similar to CNN, but uses more convolutional layers and a larger parameter space to fit large-scale datasets. Nie *et al.*[12] designed a data-driven IDS based on DCNN. The author assumed that the coverage region of all RSUs was nonoverlapping, and that each RSU independently identified the invasion of the relevant OBU. By analyzing the link load behavior of RSU in IoV, various intrusion behaviors that caused irregular fluctuations in traffic flow were detected. The abovementioned method has better performance in terms of accuracy, but ignores the consideration of latency.

RNN: RNN is designed for modeling sequential data. However, the gradient disappearance and explosion problems make it difficult to train traditional RNN models. LSTM alleviates these problems by introducing a set of "gates," so it is very effective in classifying time series data.[17] Ashraf *et al.*[5] designed an LSTM autoencoding algorithm to identify multiple types of intrusion events from IoV networks. Zeng *et al.*[11] combined the LSTM model and the CNN model to design their IDS, which was used to automatically detect the traffic passing through the OBUs. The method could achieve higher detection performance with lower resource requirements. Mobile wireless networks generate large amounts of continuous data, and exploring RNN family-based intrusion detection techniques is promising for solving the problem of network attacks in IoV.

GAN: In addition to the previous learning models, new DL techniques with better performance are being introduced. For instance, GAN has been actively applied to intrusion detection.[7] The advantage of GAN is that it can produce lifelike artifacts from target distributions,[15] and it can train any missing data through the reinforcement learning algorithm in the GAN model.[18] Considering that the emerging information physics system technology has the problems of unbalanced and incomplete sample data, which brings difficulties to the model training, Shahriar *et al.*[18] used GAN to generate synthetic samples, and IDS was trained based on the original samples and these generated samples, which also solved the problem of unbalanced or missing data. The traditional GAN training process is highly sensitive to model structure, learning rate, and other hyperparameters. Therefore, researchers need to use many "tricks" to ensure convergence and data fidelity.

Although anomaly-based IDSs detect the emerging attacks efficiently, it also inevitably has a high false alarm rate. AI technologies can greatly improve the detection accuracy of anomaly-based IDSs. However, it requires massive computing resources and storage resources.[2] In the current research, there are few intrusion detection schemes for IoV that can achieve high detection performance, low latency, lightweight, and strong generalization ability at the same time. Besides, how to obtain an effective dataset that can be used for training is also a challenge for relevant research. In addition, the security threats faced by AI technologies themselves have to be considered in the current research. For example, DL is vulnerable to adversarial examples (attackers deliberately design human inputs to trick the learning model into making mistakes).[15] Therefore, building DL-based intrusion detection models that are robust to adversarial cases is a must, but it is also very challenging.

OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Although a lot of research achievements have been achieved in the field of Intelligence IoV IDS, there are still many open issues worth discussing in the future.

Edge computing: The feature extraction and training process for AI-based intrusion detection need a large-scale quantity of computation. Due to the restrictions of resource, power, and communication latency, onboard devices and cloud platforms will not be able to store and process the massive data generated by such computing-intensive tasks.[19] To enhance the computing capacity and decrease the latency,[20] the intrusion detection tasks may be offloaded to the nearby mobile edge servers or devices.[21] Intelligent caching and computational offloading (such as power-efficient/energy-efficient data offloading) schemes to effectively decide where to perform intrusion detection tasks are also worth investigating. Furthermore, the design of multilayer IDS based on cloud-edge collaboration is also a topic worth exploring.

Federated learning (FL): AI-based IDSs for IoV inevitably need to dynamically update the detection model in the process of carrying out detection tasks. The current methods are to aggregate large amounts of data distributed in different mobile devices or nodes (such as vehicles, onboard devices) and upload the data directly to the central server of the cloud platform for training, which will result in serious communication overhead and delay. FL allows multiparticipant to collaboratively train and share the model without directly accessing the original data. Each participant uploads the model trained by the local dataset to the central server for global model aggregation. It can not only efficiently utilize bandwidth, but also reduce response latency.[22,23] Therefore, FL is very suitable for designing IoV IDS.

Transfer learning (TL): With the development of intelligent IoV, many new attack methods with different feature distributions will emerge. The detection accuracy of the original model will decrease significantly. Thus, collecting the labeled data from these new attacks to retrain the ML models is very necessary. However, this work will take a lot of labor and time. The model may fail to detect these attacks accurately because it cannot get enough labeled data within a short time. TL is an effective solution for little training data problems. By reusing the trained model for similar problems, the existing problems and the original problems will be mapped to the same feature space, so as to quickly train an effective detection model, and get better intrusion detection results.[24]

Active defense: There are a large number of IDSs for IoV. However, intrusion detection is only a means to discover the security threats in IoV. In order to ensure the IoV real security, it is necessary to develop defensive measures and respond immediately when an attack has been detected. The active defense system is able to make an automatic response by canceling users, terminating processes, closing systems, disconnecting connections, and other ways to prevent or reduce intrusion hazards. Therefore, the active defense for IoV is a meaningful future research direction. Although the automated response actions are effective in mitigating the damage caused by attacks, there may be some negative risks. For example, the isolation measures may result in partial interruption of communication links and even affect the normal operation of the network. Thus, how to use AI technology to make optimal active defense strategies will also be a considerable research subject.[2]

Privacy protection: For intrusion detection algorithms, especially AI schemes, such as ML, there are huge risks and vulnerabilities of privacy disclosure in the input data and model parameters. Therefore, intrusion detection for IoV also needs to meet the needs of privacy protection.[10] At present, privacy protection has three main research directions: differential privacy method based on noise disturbance, secure multiparty computation, and homomorphic encryption. The FL framework mentioned previously can also be applied in collaboration with these technologies. The privacy protection mechanism has a certain impact on efficiency, including the impact on computational overhead and communication costs. In practical application scenarios, especially in IoV intrusion detection tasks, how to balance detection performance and meet usability conditions (such as lightweight and low latency) while satisfying privacy, remains a great challenge.

In addition, the intelligent service data privacy, location privacy of connected vehicles, user identity privacy, and other information in the IoV also need a very strong security guarantee. Therefore, privacy protection technologies such as the ones mentioned previously have gradually been applied in the IoV environment. Unfortunately, this gives attackers new opportunities to take advantage of, for example, attackers can use encrypted channels to hide their malicious attacks, which is a very big threat to IoV security, and an effective intrusion detection mechanism is urgently needed. At present, the research on malicious encrypted traffic detection for IoV is basically in a blank, the topics including feature extraction, identification, and classification for encrypted traffic based on AI technology are well worth exploring, and interested researchers can invest in them and contribute to the protection of IIoV security.

CONCLUSION

This article systematically introduces the related concepts of the IoV, and briefly describes the IoV network composition from the perspective of the system architecture. We also summarize the security threats and attacks faced by the IoV network. We focus on the current anomaly-based IDS for IoV, and detail the application of AI technology in IDS. Finally, we discuss the open issues of IoV intrusion detection research.

ACKNOWLEDGMENTS

This research is supported in part by the National Natural Science Foundation of China under Grant 61771153, Grant 61831007, and Grant 61971154, and in part by the Fundamental Research Funds for the Central Universities under Grant 3072020CF0601.

REFERENCES

1. B. Ji *et al.*, “Survey on the Internet of Vehicles: Network architectures and applications,” *IEEE Commun. Standards Mag.*, vol. 4, no. 1, pp. 34–41, Mar. 2020.
2. W. Wu *et al.*, “A survey of intrusion detection for in-vehicle networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.
3. R. Peng, W. Li, T. Yang, and K. Huafeng, “An Internet of Vehicles intrusion detection system based on a convolutional neural network,” in *Proc. IEEE Int. Conf. Parallel Distrib. Process. with Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw.*, 2019, pp. 1595–1599.
4. L. Yang, A. Moubayed, I. Hamieh, and A. Shami, “Tree-based intelligent intrusion detection system in Internet of Vehicles,” in *Proc. IEEE Global Commun. Conf.*, 2019, pp. 1–6.
5. J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4507–4518, Jul. 2021, doi: 10.1109/TITS.2020.3017882.
6. J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, “BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,” in *Proc. IEEE Global Commun. Conf.*, 2018, pp. 1–6.
7. E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based intrusion detection system for in-vehicle network,” in *Proc. 16th Annu. Conf. Privacy, Secur. Trust*, 2018, pp. 1–6.
8. Vitalkar and Rasika, “A review on intrusion detection system in vehicular ad-hoc network using deep learning method,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 2020, pp. 1591–1595, 2020.
9. J. Liang, J. Chen, Y. Zhu, and R. Yu, “A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position,” *Appl. Soft Comput.*, vol. 75, pp. 712–727, Feb. 2019.
10. X. Wu, X. Xu, and M. Bilal, “Towards privacy protection composition framework on Internet of Vehicles,” *IEEE Consum. Electron. Mag.*, early access, Jun. 28, 2021, doi: 10.1109/MCE.2021.3092303.
11. Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, “DeepVCM: A deep learning based intrusion detection method in VANET,” in *Proc. IEEE 5th Intl Conf. Big Data Secur. Cloud, IEEE Intl Conf. High Perform. Smart Comput., IEEE Intl Conf. Intell. Data Secur.*, 2019, pp. 288–293.
12. L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, “Data-Driven intrusion detection for intelligent Internet of Vehicles: A deep convolutional neural network-based method,” *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2219–2230, Oct.–Dec. 2020.
13. A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, “Classification approach for intrusion detection in vehicle systems,” *Wireless Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018.
14. G. D’Angelo, A. Castiglione, and F. Palmieri, “A cluster-based multidimensional approach for detecting attacks on connected vehicles,” *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12518–12527, Aug. 2021.

15. P. P. Zhang and H. Haddadi, “Deep learning in mobile and wireless networking: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2224–2287, Jul.–Sep. 2019.
16. A. Anzer and M. Elhadef, “A multilayer perceptron-based distributed intrusion detection system for Internet of Vehicles,” in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput.*, 2018, pp. 438–445.
17. T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, “Securing the Internet of Vehicles: A deep learning based classification framework,” *IEEE Netw. Lett.*, vol. 3, no. 2, pp. 94–97, Jun. 2021, doi: 10.1109/LNET.2021.3058292.
18. M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, “G-IDS: Generative adversarial networks assisted intrusion detection system,” in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf.*, 2020, pp. 376–385.
19. M. Adhikari, A. Munusamy, A. Hazra, V. G. Menon, V. Anavangot, and D. Puthal, “Security and privacy in edge-centric intelligent Internet of Vehicles: Issues and remedies,” *IEEE Consum. Electron. Mag.*, early access, Sep., 30, 2021, doi: 10.1109/MCE.2021.3116415.
20. N. Wang *et al.*, “When energy trading meets blockchain in electrical power system: The state of the art,” *Appl. Sci.*, vol. 9, no. 8, pp. 1–31, Apr. 2019.
21. A. Mourad, H. Tout, O. A. Wahab, H. Otrok, and T. Dbouk, “Ad hoc vehicular fog enabling cooperative low-latency intrusion detection,” *IEEE Internet Things J.*, vol. 8, no. 2, pp. 829–843, Jan. 2021.
22. W. Y. B. Lim *et al.*, “Federated learning in mobile edge networks: A comprehensive survey,” *IEEE Commun. Surveys. Tuts.*, vol. 22, no. 3, pp. 2031–2063, Jul.–Sep. 2020.
23. B. Ghimire and D. B. Rawat, “Secure, privacy preserving and verifiable federating learning using blockchain for Internet of Vehicles,” *IEEE Consum. Electron. Mag.*, early access, Jul. 29, 2021, doi: 10.1109/MCE.2021.3097705.
24. X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, “Transfer learning based intrusion detection scheme for Internet of Vehicles,” *Inf. Sci.*, vol. 547, pp. 119–135, 2021.
25. Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, “A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network,” *IEEE Access*, vol. 7, pp. 154560–154571, 2019.
26. H. M. Song, J. Woo, and H. K. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.

Dapeng Man is currently an associate professor with Harbin Engineering University, Harbin, China. His research interests include mobile computing security and IoT security. Man received the B.S., M.S., and Ph.D. degrees in computer science and technology from Harbin Engineering University in 2003, 2007, and 2009, respectively. He is a member of CCF. Contact him at mandapeng@hrbeu.edu.cn.

Fanyi Zeng is currently working toward the Ph.D. degree with the College of Computer Science and Technology, Harbin Engineering University, Harbin, China. Her research interests include mobile computing security and IoT security. Contact her at zengfanyi@hrbeu.edu.cn.

Jiguang Lv is currently an associate professor with Harbin Engineering University, Harbin, China. His main research interests include mobile computing security and IoT security. Lv received the M.S. and Ph.D. degrees in computer science and technology from Harbin Engineering University in 2014 and 2018, respectively. He is a Member of CCF. Contact him at lvjiguang@hrbeu.edu.cn.

Shichang Xuan is currently an associate professor with Harbin Engineering University, Harbin, China. His main research interests include information security and blockchain. Xuan received the B.S., M.S., and Ph.D. degrees in computer science and technology from Harbin Engineering University in 2007, 2010, and 2017, respectively. Contact him at xuanshichang@hrbeu.edu.cn.

Wu Yang is currently a professor and doctoral supervisor with Harbin Engineering University, Harbin, China. His main research interests include wireless sensor network, peer-to-peer network, and information security. Yang received the Ph.D. degree in computer system architecture from Computer Science and Technology School, Harbin Institute of Technology, Harbin, China. He is a member of ACM and senior member of CCF. Contact him at yangwu@hrbeu.edu.cn.

Mohsen Guizani is currently a professor with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. Guizani received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is a fellow of IEEE and a senior member of ACM. Contact him at mguizani@ieee.org.