Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9865549, 8 pages
https://doi.org/10.1155/2022/9865549

Research Article

Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods

Lu Lihua

School of Computer Science, Northwest Polytechnic University, Xi'an, 710129 Shaanxi, China

Correspondence should be addressed to Lu Lihua; lihua1812@yahoo.com

Received 30 March 2022; Accepted 12 May 2022; Published 26 May 2022

Academic Editor: Nima Jafari Navimipour

With increasing development of Internet of Things (IoT) technology, wireless communications, big data, and smart applications, vehicular communications have become ubiquitous in smart cities, smart transportation systems, and Internet of Vehicles (IoV) environments. In this paper, a new Energy-aware Intrusion Detection System (EIDS) based on intelligent two-phase contract management model is presented for vehicle-to-vehicle (V2V) strategy in the IoV environments. In this strategy, the proposed EIDS predicts safe and energy-efficient end-to-end points for communication between existing vehicles in the IoV. The contract management process shows how the vehicles are connected together with a safe condition to transfer information. For prediction phase, a regression algorithm is applied to evaluate the proposed EIDS according to NSLKDD data set in the IoV environments. Simulation experiments show that the proposed regression-based EIDS strategy can effectively improve the accuracy and precision factors with 90% and 84%, respectively, and greatly minimize execution time by 4 seconds with respect to other machine learning algorithms.

1. Introduction

Today, vehicular communications have developed emerging topics on intelligent transportation systems with respect to wireless distribution and smart devices in the Internet of Things (IoT) environments [1, 2]. In the IoT, smart devices perform communication at different locations by providing a level of transparency among users and maintained an interconnected smart network. According to the main concept of the IoT [3], vehicular communications have wide collaboration between smart devices and big data on new intelligent concept of Internet of Vehicles (IoV) [4–6]. In the IoV environments, the communication model is divided into three statuses including vehicle to vehicle (V2V) [7, 8], vehicle to infrastructure (V2I) [9], and vehicle to people (V2P) [8, 10]. In these models, data transmission as an important problem statement has usually applied smart sensors and intelligent applications with minimum energy consumption to exchange and transfer the information between safety of vehicles [11], applications, devices, sensors, and peoples [12]. In this problem statement, Intrusion Detection Systems (IDS) have critical and emerging issues for supporting safety [13, 14], security [15], and privacy of data transmission [16] and information retrieval of intelligent transportation systems in the IoV [17]. The data transmission accumulated by V2V, V2I, and V2P case studies [8, 18, 19] can be managed securely to provide various cloud-edge services such as road safety, smart parking reservations, traffic management, vehicular routing management, and emergency issues [20].

According to the above critical problem statements on the IoV environments, this paper presents a new Energy-aware Intrusion Detection System (EIDS) to provide safety conditions for data transmission between vehicles as a V2V case study to avoid the existing attacks and critical points. In this paper, a machine learning method is presented to predict optimal energy consumption between vehicles to transfer data with safe and secured infrastructure in the IoV environments. The main contributions of this research are shown as follows:

(i) Proposing an energy-aware intrusion detection model for managing a safe data transmission method for V2V scenarios in IoV

(ii) Applying regression algorithm as the machine learning method to predict optimal secured infrastructure in the IoV environments

(iii) Increasing accuracy and precision factors for predicting existing attacks and critical points in the EIDS

The organization of the paper is presented as follows: Section 2 illustrates a comprehensive literature review for security-aware and energy consumption models in the IoT and intelligent transportation systems. Section 3 shows a conceptual model of the proposed energy-aware intrusion detection model based on regression algorithm. Section 4 presents simulation parameters and experimental results based on comparison of existing machine learning algorithms and discussion on evaluation factors, respectively. Finally, Section 5 provides a brief discussion on the experimental results, conclusion, and future works.

2. Related Work

In this section, some new relevant case studies are discussed and analyzed as a literature review for intrusion detection strategies using machine learning and evolutionary algorithms in the IoV, IoT, and vehicular ad hoc network (VANET). Many research studies have evaluated security-based cloud-edge service scheduling and allocation for energy-aware IoV systems [21–24].

Subba et al. [25] provided a theory and algorithm using the IDS framework for VANET security. VANETs have sensors and On-Board Units (OBUs). OBUs use Road Side Units (RSUs) and IEEE 802.11p for connecting vehicles. VANETs are susceptible to diverse kinds of network attacks so they used Intrusion Detection Systems (IDSs) to solve them. Some IDS properties are not suitable for VANET such as IDS traffic volume, bandwidth limitation, dynamic network topology, communication overhead, and scalability which need to be fixed. They presented a new clustering algorithm that produced constant vehicular clusters using vehicular data. The proposed Cluster Head (CH) selection algorithm is based on the Vickrey-Clarke-Groves method. They suggested a game theory-based multilayered intrusion detection framework for VANET to detect different kinds of attacks in VANET. They used NS3 and Simulation of Urban Mobility (SUMO) for simulation. Simulation of the interaction between the IDS and the malicious vehicle reduces the size of IDS traffic by embracing a probabilistic IDS showing strategy based on the Nash equilibrium of the game. The problem is that the proposed algorithm is for vehicles that stop or move slowly. Their future work is to present a dynamic clustering algorithm and also improve components and develop the project.

Kang et al. [26] and his team have proposed an extremely impressive accidental confirmation protocol that contains homomorphic encryption to permit any personal vehicle to self-produce every number of confirmed personalities to get complete obscurity in VANETs. The suggested protocol barricades vehicles by detecting every prohibited person and increasing traceability. The purpose of this paper has been to propose an extremely effective accidental confirmation order in VANETs, the name of RAU+. The results of this paper show that their suggested RAU+ protocol is rather effective than another protocol and can efficiently decrease the network overhead. The disadvantage of this paper is that it requires more testing in the future to improve their protocol which can be spread to IoT schedules.

In [27], an authentication scheme has been proposed that has led to a complete summary of VANET, and it has been seen that this scheme meets VANET security requirements via security analysis. The signal phase is divided into two stages, and the previous calculation method is used to reduce the calculation cost in the signal stage. Road Side Unit (RSU) has been able to collect multiple signatures in a single unit, and the total length of the signature is a fixed size, which significantly reduces the transmission between the RSU and the application server and improves the verification efficiency for the application. In the next work, to reduce the cost of calculations and communications, the use of a lighter signature plan is considered.

Chen et al. [28] and his colleagues presented a new model based on barriers, and link performance on the highway is presented using the obstacle-based channel model. In this research, the authors have used Markov chain realistic channel model and dual-slop path loss model to evaluate this. Assessment measures can be referred to reliability and time. Evaluation and model of empirical results indicate that this system has effectiveness through security analysis and is also used to evaluate the end-end performance. The advantages of this project are using the real channel simulator, and its drawbacks can be pointed to the long-term connection time.

Zhang et al. [29] suggested a new design for the dissemination of safety messages for quality-based urban IoV provided for accurate estimation of connection probability among vehicles. In this model, the CFs algorithm is used. Simulation results represent a good approximation of the model and the superiority of this protocol. To evaluate the research, time and probability factors have been used. The advantages of this paper are the superiority of it is performing compared to similar studies, and its disadvantages can be referred to as delay.

In [30], the Media Access Control (MAC) program is deliberately based on multilateral cooperation to eliminate delays and data interference in the automotive network. The protocol transmits security data with the corresponding sensors installed along the road and sends the DA search packet in the SCHI gap to obtain RSU-covered car data. When transferring this data, the vehicle node, which has a security message for sending or receiving CCH gap subscribers and transferring nonaccident data, is obtained using the multifaceted reservation mechanism in the SCHI gap. With RSU coordination, security information is tracked by each node in order. To achieve the VANET terminal, RSU has played the role of wireless energy absorption, which has led to uninterrupted channel transmissions, reduced channel delays, and improved channel efficiency.

Yaqub et al. [31] provided a method named cooperative video retrieval scheme (CoRe). Streaming media has become a significant factor to satisfy VANET users, while downloading videos with proper qualities causes bandwidth consumption and may leave insufficient bandwidth for quality of service. To avoid such issues, the authors suggested a communicative system in which vehicles can request more bandwidth in case of sharing. They can ask another vehicle for bandwidth sharing, downloading a part of media, or forwarding the demanded video via a link. The system actually chooses a nearby neighbor vehicle to request, in order to preserve the V2V connection, and it must have sufficient bandwidth to share. Based on the results, CoRe helped users to obtain a better quality of the video. They decided to involve 5G and ICN technologies with a CoRe system in the future.

3. Proposed Method

In this section, a new energy-based vehicle-to-vehicle collaboration is presented. Then, a new IDS approach is applied for the proposed V2V strategy to check and analyze performance of the IoV environments using machine learning methods. In the IoV environments, vehicles collaborate together in a secured end-to-end capacity using IoT application smart devices, sensors, and interconnection methods. On existing interconnection and intraconnection methods, the security is a significant challenge for a safe condition on data transmission between vehicles in the IoV environments. On the other hand, energy consumption of IoT nodes is a critical issue that represents the performance evaluation of vehicular communications in IoV applications. Certainly, in this section, we present a new energy-aware intrusion detection method with respect to minimizing energy consumption of vehicles as a fundamental parameter in the IoV environments.

In the IoV environment, some important factors such as traffic road scheduling, the moving speed of vehicles [32], the density of vehicles movements, and the infrastructure of the network change dynamically. Based on the abovementioned factors, each data transmission strategy between two or more than three vehicles should be examined with energy consumption, delay, and response time metrics. According to the V2V strategy, each vehicle has a communication range for collaboration with other vehicles in the IoV environment. For creating a data transmission connection, energy consumption between two vehicles should be examined before the intraconnection protocol [33]. According to Equation (1), the earned energy factor for transmitting information between two vehicles is evaluated as follows [34, 35]:

$$\mathrm{EV}_{ij} = (\mathrm{ET}_i \times N_{\mathrm{O}}) + \left(\mathrm{ET}_j \times N_{\mathrm{I}}\right), \tag{1}$$

where ET is the energy consumption for transmitting data in vehicles i and j, N_{O} is the number of transmission packets that is sent for each communication round, and N_{I} is the number of transmission packets that is received in each communication round [36, 37].

Also, the energy consumed in the data transmission between a vehicle and wireless server is calculated as follows according to the following equation [38]:

$$\mathrm{EW} = (\mathrm{ET}_i \times M) + \left(\mathrm{ES}_j \times K\right), \tag{2}$$

where M is the number of sent or received packets for each communication round to the wireless server, ES_j is the energy consumption for transmitting data to the vehicle j, and K is the number of sent packets for each communication round.

The total energy consumption metric for one communication round between existing vehicles and servers is computed according to the following equation [39]:

$$\mathrm{ET} = \left(\sum \mathrm{EV}_{ij} \times \mathrm{NV}\right) + \left(\sum \mathrm{EW} \times \mathrm{NS}\right), \tag{3}$$

where NV is the number of existing vehicles and NS is the number of existing wireless servers in a communication round.

To create a data transmission round, each vehicle as an active node in the IoV sends a request to the neighbors with a broadcast mode. Each other vehicle receives existing request and checks with information for all available candidates to transfer data between activated nodes. According to Figure 1, if a communication distance is higher than the communication range or there is no an activated vehicle in circle of requested vehicle, then targeted node sends request to the wireless server. After finding an appropriate and alive transmission link between existing vehicles and servers according to the V2V strategy [40], link establishment is considered to finalize data transmission link. Then, energy consumption of the established link is examined to check minimum energy consumption between all nodes including activated vehicles and wireless servers. According to Equation (1), the produced energy factor for transmitting information between two vehicles is evaluated. Also, based on Equation (2) [41], the energy consumed in the data transmission between the vehicle and wireless server is calculated. Finally, Equation (3) calculates the total energy consumption metric for one communication round between existing vehicles and the IoV servers. If there is an optimized energy-efficient established link for data transmission, then the intrusion detection method is applied. Otherwise, system reassigns finding transmission link between available vehicles and servers. When an optimized energy-efficient link is selected, the proposed intrusion detection method (EIDS) is activated [42, 43]. In this step, the regression algorithm as the proposed machine learning method selects applied data set for training process for detecting the malicious behaviors and attacks. The existing data set is divided into two sides; the first content is applied for train process as %70, and the other content %30 is evaluated for test process. In the train process, if intrusion detection has safe result for a transmitted link, then real data transmission and packets are transferred in this link. Otherwise, the selected link is unsafe for communication.

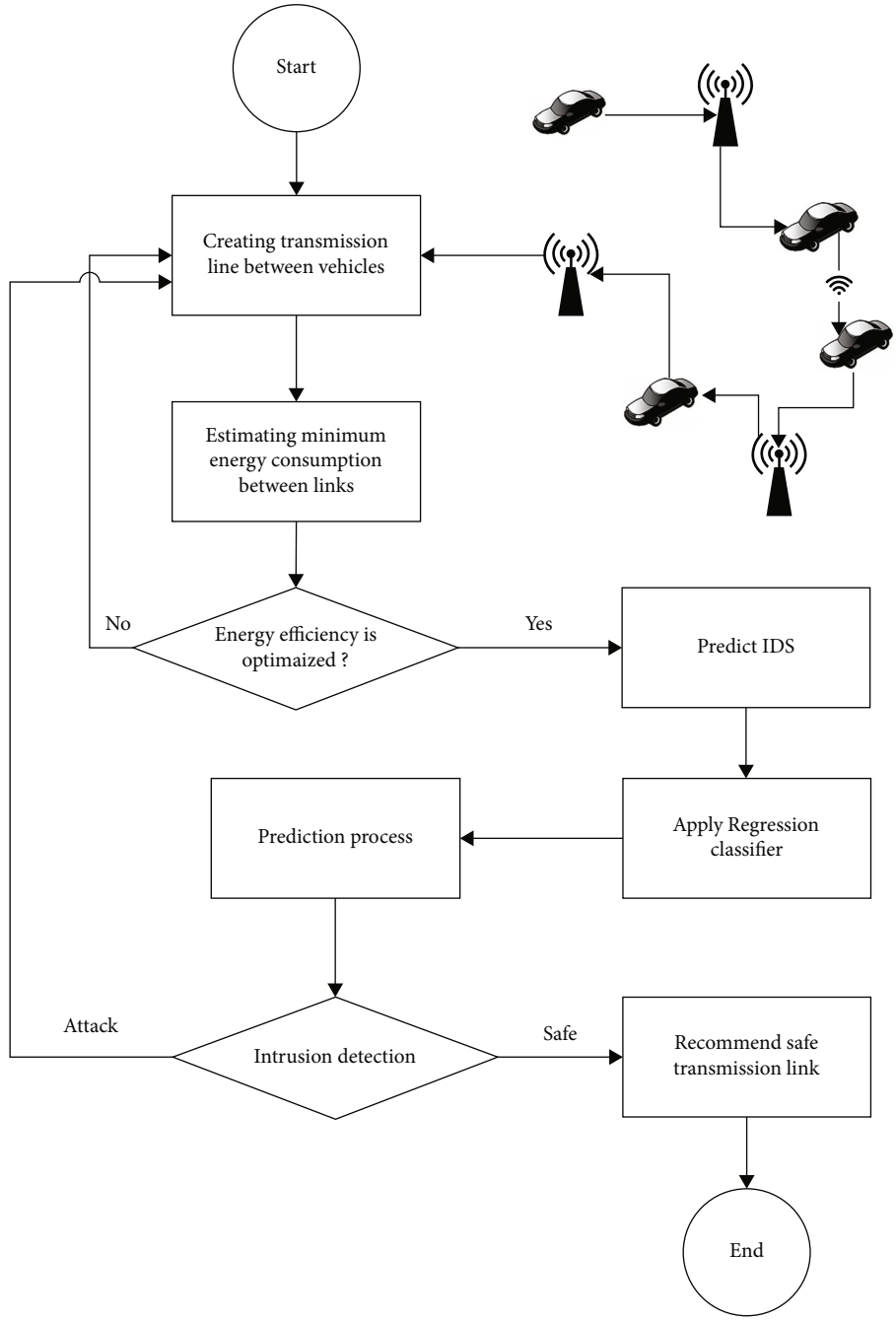

Figure 1: The EIDS flowchart based on regression prediction algorithm in IoV.

Table 1: Data set parameters.

Description	Train set	Test set
Attacks	3,925,650	250,436
Normal	972,781	60,591

According to the above mentioned framework, the proposed regression-based EIDS method checks minimum energy consumption for each selected transmission link and then proceeds intrusion detection process for existing data set.

4. Experimental and Simulation Results

This section proposes performance evaluation and comparison for the proposed EIDS with regression algorithm and other algorithms including the Support Vector Machine (SVM) [44], Random Forest (RF) algorithm [45], Multilayer Perceptron (MLP) algorithm [46], and Decision Tree (DT) algorithm [47]. We have applied the existing algorithms on the NSLKDD data set [48] as our case study (https://www.unb.ca/cic/datasets/nsl.html) with existing information. Also, WEKA toolkit [49] as simulation environment was used to evaluate the proposed EIDS case study using a

Table 2: Simulation parameters.

Description	Values (default)
Number of vehicles	10
Communication range between each vehicle	100, 200, 300, 400, 500
Environment dimension	50 ∗ 50 ∗ 50
Transmission rate (Mbps)	100

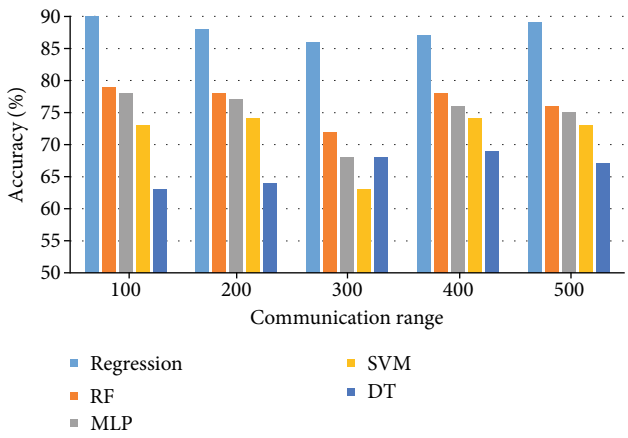

Figure 2: Evaluation of accuracy factor for energy-aware intrusion detection strategy in IoV.

Table 3: Prediction factors.

Prediction factor	Description
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Precision	$\frac{TP}{TP + FP}$

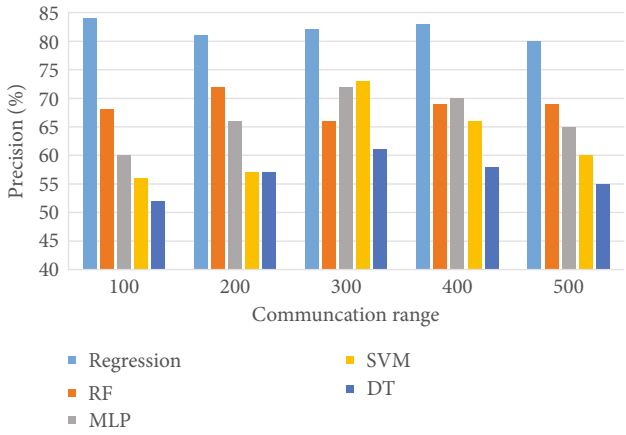

Figure 3: Evaluation of precision metric for energy-aware intrusion detection strategy in IoV.

system with Windows 10, Intel i5 3.10 GHz, 8 GB RAM. Also, a brief illustration about the applied NSLKDD data set is shown in Table 1 [50]. Then, the performance metrics used in the evaluation are introduced in Table 2.

According to the proposed Energy-aware IDS approach, we have presented a new regression-based prediction approach to detect minimum energy consumption for a data transmission procedure. For evaluating this procedure, some important prediction factors such as accuracy, precision, and execution time have been analyzed based on existing machine learning algorithms [51]. The experimental results evaluate important prediction factors including accuracy, precision, and execution time on the results of existing machine learning algorithms [52]. Table 3 shows prediction factors with respect to the following training parameters: True Positive (TP), True Negative (TN), False Positive (FP) [53], and False Negative (FN) metrics [54].

4.1. Simulation Results. We have simulated the proposed regression-based EIDS case study with respect to other algorithms in MATLAB environment that simulates the proposed prediction method for V2V strategy in the IoV environment. To evaluate the performance of the proposed algorithm, we considered five communication ranges between each vehicle for V2V strategy as 100, 200, 300, 400, and 500 in the IoV environment.

Figure 2 represents evaluation of accuracy factor with respect to each communication range step. According to the observed diagram, it can be achieved that the proposed regression-based EIDS has optimal score for the accuracy of prediction. The results obtained from the proposed regression-based EIDS method in the IoV were compared with other machine learning algorithms. This comparison on accuracy evaluation shows that the proposed regression-based EIDS has achieved a maximum accuracy factor of 90% for 10 vehicles. Moreover, another optimized machine leering algorithm is the RF algorithm that has approximately 78% accuracy higher than SVM, MLP, and DT prediction algorithms.

According to Figure 3, the proposed regression-based EIDS method has achieved higher precision metric for existing communication ranges between 80% and 85%. But the RF method has achieved only 74% just for communication range 200 with high precision, the SVM algorithm has shown 74% just for communication range 300, and the MLP algorithm has performed 71% of precision just for communication range 300 as best results for each prediction method. This evaluation illustrates that the DT algorithm has only a small amount of precision lower than 55% for detecting attacks in the IoV scenarios. With respect to this comparison, we conclude that the precision factor has different evaluation results with different communication ranges in other algorithms. However, the proposed regression-based EIDS method has attained maximum precision for the overall communication ranges.

Finally, to assess execution time of this prediction, we can observe that the proposed regression-based EIDS has gained 4.5 s for communication range 100, 6.2 s for communication range 200, 14.8 s for communication range 300, 18.9 s for communication range 400, and 20.2 s of execution time for communication range 500 according to Figure 4. So, the proposed method significantly has minimum execution time for the overall communication ranges. On the other

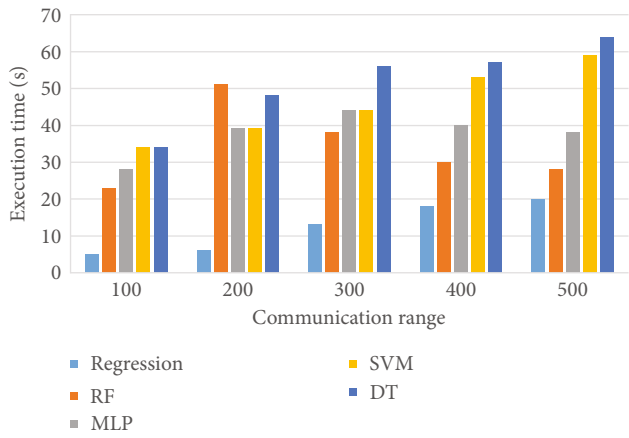

Figure 4: Execution time evaluation for the proposed EIDS strategy in the IoV environment.

hand, the execution time of DT algorithm is 69.8 s for communication ranges 300 and 500.

5. Conclusion

In this paper, a new Energy-aware Intrusion Detection System (EIDS) was presented for managing safe transitions and information in the IoV environments. Since the EIDS is based on prediction approach, machine learning techniques were applied to enhance quality of prediction for malicious and existing attacks according to train and test data sets with respect to low energy consumption for each vehicle. The experimental results have shown the efficiency performance of the proposed machine learning algorithms with minimum energy consumption, high accuracy, and maximum precision in the IoV environments. Also, the prediction time of the EIDS with the regression algorithm is lower than that of the other machine learning algorithms. Finally, the proposed algorithm guaranteed safe data transactions between the maximum numbers of vehicles in the IoV environments. In the future work, a new feature selection method for the effective predictable model in machine learning approach can be presented to optimize efficient accuracy and energy consumption with a high-quality priority in the vehicular communications.

Data Availability

The data that support the findings of this study are available from the NSLKDD data set as follows: https://www.unb.ca/cic/datasets/nsl.html [48].

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] S. Babu and A. P. Raj Kumar, "A comprehensive survey on simulators, emulators, and testbeds for VANETs," *International Journal of Communication Systems*, vol. 35, no. 8, article e5123, 2022.

[2] Z. Lv, L. Qiao, and I. You, "6G-enabled network in box for internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5275–5282, 2021.

[3] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *International Journal of Communication Systems*, vol. 35, no. 2, article e4198, 2022.

[4] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3832–3840, 2021.

[5] C. Zheng, Y. An, Z. Wang et al., "Knowledge-based engineering approach for defining robotic manufacturing system architectures," *International Journal of Production Research*, pp. 1–19, 2022.

[6] H. Kong, L. Lu, J. Yu, Y. Chen, and F. Tang, "Continuous authentication through finger gesture interaction for smart homes using WiFi," *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148–3162, 2021.

[7] M. Shurrab, S. Singh, H. Otrok, R. Mizouni, V. Khadkikar, and H. Zeineldin, "An efficient vehicle-to-vehicle (V2V) energy sharing framework," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5315–5328, 2022.

[8] A. R. Khan, M. F. Jamlos, N. Osman et al., "DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): a review," *Recent Trends in Mechatronics Towards Industry*, vol. 730, pp. 97–106, 2022.

[9] P. Liu and W. D. Fan, "Exploring the impact of connected and autonomous vehicles on mobility and environment at signalized intersections through vehicle-to-infrastructure (V2I) and infrastructure-to-vehicle (I2V) communications," *Transportation Planning and Technology*, vol. 44, no. 2, pp. 129–138, 2021.

[10] C. Zheng, Y. An, Z. Wang et al., "Hybrid offline programming method for robotic welding systems," *Robotics and Computer-Integrated Manufacturing*, vol. 73, article 102238, 2022.

[11] J. Chen, Q. Wang, and J. Huang, "Motorcycle ban and traffic safety: evidence from a quasi-experiment at Zhejiang, China," *Journal of Advanced Transportation*, vol. 2021, 13 pages, 2021.

[12] W. Zhou, J. Liu, J. Lei, L. Yu, and J. N. Hwang, "GMNet: graded-feature multilabel-learning network for RGB-thermal urban scene semantic segmentation," *IEEE Transactions on Image Processing*, vol. 30, pp. 7790–7802, 2021.

[13] S. Khan, K. Kifayat, A. Kashif Bashir, A. Gurtov, and M. Hassan, "Intelligent intrusion detection system in smart grid using computational intelligence and machine learning," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, article e4062, 2021.

[14] J. Yu, L. Lu, Y. Chen, Y. Zhu, and L. Kong, "An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 337–351, 2021.

[15] M. Zhang, Y. Chen, and J. Lin, "A privacy-preserving optimization of neighborhood-based recommendation for medical-aided diagnosis and treatment," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10830–10842, 2021.

[16] S. Zhao, F. Li, H. Li et al., "Smart and practical privacy-preserving data aggregation for fog-based smart grids," *IEEE*

Transactions on Information Forensics and Security, vol. 16, pp. 521–536, 2021.

[17] Z. Lv, Y. Li, H. Feng, and H. Lv, "Deep learning for security in digital twins of cooperative intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[18] J. Chen, Y. Liu, Y. Xiang, and K. Sood, "RPPTD: robust privacy-preserving truth discovery scheme," *IEEE Systems Journal*, pp. 1–8, 2021.

[19] Z. Li, L. Chen, L. Nie, and S. X. Yang, "A novel learning model of driver fatigue features representation for steering wheel angle," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 269–281, 2022.

[20] B. Cao, W. Zhang, X. Wang, J. Zhao, Y. Gu, and Y. Zhang, "A memetic algorithm based on two_Arch2 for multi-depot heterogeneous-vehicle capacitated arc routing problem," *Swarm and Evolutionary Computation*, vol. 63, article 100864, 2021.

[21] B. Cao, J. Zhang, X. Liu et al., "Edge-cloud resource scheduling in space–air–ground-integrated networks for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5765–5772, 2022.

[22] H. Cheng, M. Shojafar, M. Alazab, R. Tafazolli, and Y. Liu, "PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021.

[23] L. Zhang, H. Zheng, G. Cai, Z. Zhang, X. Wang, and L. H. Koh, "Power-frequency oscillation suppression algorithm for AC microgrid with multiple virtual synchronous generators based on fuzzy inference system," *IET Renewable Power Generation*, 2022.

[24] W. Yang, X. Chen, Z. Xiong, Z. Xu, G. Liu, and X. Zhang, "A privacy-preserving aggregation scheme based on negative survey for vehicle fuel consumption data," *Information Sciences*, vol. 570, pp. 526–544, 2021.

[25] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Future Generation Computer Systems*, vol. 82, pp. 12–28, 2018.

[26] J. Kang, D. Lin, W. Jiang, and E. Bertino, "Highly efficient randomized authentication in VANETs," *Pervasive and Mobile Computing*, vol. 44, pp. 31–44, 2018.

[27] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[28] R. Chen, Z. Zhong, V. C. M. Leung, and D. G. Michelson, "Link connectivity under more realistic channel model for vehicle-to-vehicle communications," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 22, no. 1, pp. 35–47, 2016.

[29] X. Zhang, Q. Miao, and Y. Li, "An adaptive link quality-based safety message dissemination scheme for urban VANETs," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2104–2107, 2018.

[30] H. Zhao, M. Zhang, K. Gao, T. Mao, and H. Zhu, "A multichannel cooperative demand-aware media access control scheme in vehicular ad-hoc network," *Wireless Personal Communications*, vol. 104, no. 1, pp. 325–337, 2019.

[31] M. A. Yaqub, S. H. Ahmed, and D. Kim, "Asking neighbors a favor: cooperative video retrieval using cellular networks in VANETs," *Vehicular Communications*, vol. 12, pp. 39–49, 2018.

[32] Z. Liu, L. Fang, D. Jiang, and R. Qu, "A machine-learning based fault diagnosis method with adaptive secondary sampling for multiphase drive systems," *IEEE Transactions on Power Electronics*, vol. 37, no. 8, pp. 8767–8772, 2022.

[33] F. Meng, S. Yang, J. Wang, L. Xia, and H. Liu, "Creating knowledge graph of electric power equipment faults based on BERT–BiLSTM–CRF model," *Journal of Electrical Engineering & Technology*, pp. 1–10, 2022.

[34] J. Mou, P. Duan, L. Gao, X. Liu, and J. Li, "An effective hybrid collaborative algorithm for energy-efficient distributed permutation flow-shop inverse scheduling," *Future Generation Computer Systems*, vol. 128, pp. 521–537, 2022.

[35] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Information Sciences*, vol. 575, pp. 379–398, 2021.

[36] B. Cao, Y. Zhang, J. Zhao, X. Liu, L. Skonieczny, and Z. Lv, "Recommendation based on large-scale many-objective optimization for the intelligent internet of things system," *IEEE Internet of Things Journal*, 2021.

[37] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the Internet of Things," *ACM Transactions on Sensor Networks (TOSN)*, vol. 18, no. 3, pp. 1–21, 2022.

[38] L. Zhang, T. Gao, G. Cai, and K. L. Hai, "Research on electric vehicle charging safety warning model based on back propagation neural network optimized by improved gray wolf algorithm," *Journal of Energy Storage*, vol. 49, article 104092, 2022.

[39] K. Wang, H. Wang, and S. Li, "Renewable quantile regression for streaming datasets," *Knowledge-Based Systems*, vol. 235, article 107675, 2022.

[40] C. Zhao, F. Liao, X. Li, and Y. du, "Macroscopic modeling and dynamic control of on-street cruising-for-parking of autonomous vehicles in a multi-region urban road network," *Transportation Research Part C: Emerging Technologies*, vol. 128, article 103176, 2021.

[41] B. Li, J. Yang, Y. Yang, C. Li, and Y. Zhang, "Sign language/gesture recognition based on cumulative distribution density features using UWB radar," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–13, 2021.

[42] Z. Lv, D. Chen, and H. Lv, "Smart city construction and management by digital twins and BIM big data in COVID-19 scenario," *ACM Transactions on Multimidia Computing Communications and Applications*, 2022.

[43] Z. Wu, J. Cao, Y. Wang, Y. Wang, L. Zhang, and J. Wu, "hPSD: a hybrid PU-learning-based spammer detection model for product reviews," *IEEE transactions on cybernetics*, vol. 50, no. 4, pp. 1595–1606, 2020.

[44] Y. Zhang, F. Liu, Z. Fang, B. Yuan, G. Zhang, and J. Lu, "Learning from a complementary-label source domain: theory and algorithms," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–15, 2021.

[45] Z. Lv, D. Chen, H. Feng, W. Wei, and H. Lv, "Artificial intelligence in underwater digital twins sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 18, no. 3, pp. 1–27, 2022.

[46] Z. Wu, C. Li, J. Cao, and Y. Ge, "On scalability of association-rule-based recommendation," *ACM Transactions on the Web (TWEB)*, vol. 14, no. 3, pp. 1–21, 2020.

[47] L. Liao, L. Du, and Y. Guo, "Semi-supervised SAR target detection based on an improved faster R-CNN," *Remote Sensing*, vol. 14, no. 1, p. 143, 2022.

[48] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*, Ottawa, ON, Canada, 2009.

[49] C. Liu, D. Wu, Y. Li, and Y. du, "Large-scale pavement roughness measurements with vehicle crowdsourced data using semi-supervised learning," *Transportation Research Part C: Emerging Technologies*, vol. 125, article 103048, 2021.

[50] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, "Improving high-impact bug report prediction with combination of interactive machine learning and active learning," *Information and Software Technology*, vol. 133, article 106530, 2021.

[51] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, "A comparative study of class rebalancing methods for security bug report classification," *IEEE Transactions on Reliability*, vol. 70, no. 4, pp. 1658–1670, 2021.

[52] G. Sun, Y. Cong, J. Dong, Y. Liu, Z. Ding, and H. Yu, "What and how: generalized lifelong spectral clustering via dual memory," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PP, p. 1, 2021.

[53] W. Zheng, J. Y. Cheng, X. Wu, R. Sun, X. Wang, and X. Sun, "Domain knowledge-based security bug reports prediction," *Knowledge-Based Systems*, vol. 241, article 108293, 2022.

[54] L. Zhong, Z. Fang, F. Liu, B. Yuan, G. Zhang, and J. Lu, "Bridging the theoretical bound and deep algorithms for open set domain adaptation," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–15, 2021.