EURASIP Journal on Wireless Communications and Networking

EDITORIAL Open Access

Machine learning for trust, security, and privacy in computing and communications

Chin-Ling Chen[1*], Haishuai Wang[2], Abel C. H. Chen[3*], Chunjia Han[4], Yu-Chih Wei[5] and Xiaoyan Li[6]

*Correspondence: clc@mail.cyut.edu.tw; chchen.scholar@gmail.com

[1] Chaoyang University of Technology, Taichung, Taiwan
[2] Zhejiang University, Hangzhou, China
[3] Taoyuan, Taiwan
[4] University of London, London, UK
[5] National Taipei University of Technology, Taipei, Taiwan
[6] Fuzhou University, Fuzhou, China

In recent years, various machine learning methods such as supervised methods (e.g. *k* nearest neighbors (kNN), Bayes' classifier, decision tree (DT), support vector machine (SVM), random forest (RF), neural network (NN), convolutional neural network (CNN), recurrent neural network (RNN), long short-term memory (LSTM) network, gated recurrent unit (GRU) network) [1–3], unsupervised methods (e.g. association rules, *k*-means, density-based spatial clustering of applications with noise (DBSCAN), hierarchical clustering, deep belief networks (DBN), deep Boltzmann machine (DBM), auto-encoder (AE), de-noising auto-encoder, etc.) [4, 5], reinforcement learning methods (e.g. generative adversarial network (GAN), deep Q-network (DQN), trust region policy optimization, etc.) [6], and federated learning methods have been applied to trust, security, and privacy in computing and communications. These methods have been utilized to analyze data streams in networks and detect patterns of malicious activity for intrusion detection systems, as well as to propose time-series methods for preventing cyber-attacks and malfunctions.

Despite the rapid expansion of the field of machine learning methods for trust, security, and privacy in computing and communications, there are still several open research questions that need to be addressed. For instance, improving machine learning methods for detecting malicious activity, attack detection, mobile endpoint analysis, repetitive security task automation, and zero-day vulnerability prevention are critical issues in the field. Therefore, the special issue entitled "Machine Learning for Trust, Security and Privacy in Computing and Communications" in the EURASIP Journal on Wireless Communications and Networking aims to solicit papers on these and related topics across various disciplines of trust, security, and privacy in computing and communications.

Topics covered in this issue are categorized into the following five themes: (1) network and security, (2) machine learning and artificial intelligence, (3) communication and routing strategies, (4) optimization and algorithms, and (5) data analysis. This special issue has received a substantial number of submissions, resulting in a collection of 21 papers from several countries/regions including China, USA, UK, Finland, Saudi Arabia, and Japan. The careful selection process ensures that only high-quality papers with significant results are chosen for publication.

1 Network and security

Four papers on network and security are listed as follows: (1) "A blockchain-based secure storage scheme for medical information," by Sun et al. [7]; (2) "Network abnormal traffic detection method based on fusion of chord similarity and multiple loss encoder," by Lv et al. [8]; (3) "A security method of hardware Trojan detection using path tracking algorithm," by Huang et al. [9]; (4) "Early warning system for drivers' phone usage with deep learning network," by Hou et al. [10]. Detailed information of each article could be found in [7–10].

2 Machine learning and artificial intelligence

Six papers on machine learning and artificial intelligence are listed as follows: (1) "A framework for self-supervised federated domain adaptation," by Wang et al. [11]; (2) "Mixed-type data generation method based on generative adversarial networks," by Wei et al. [12]; (3) "The analysis of financial market risk based on machine learning and particle swarm optimization algorithm," by Liu and Yu [13]; (4) "Application of machine learning in intelligent encryption for digital information of real-time image text under big data," by Liu et al. [14]; (5) "Effects of psychological fatigue on college athletes' error-related negativity based on artificial intelligence computing method," by Li et al. [15]; (6) "ABOS: an attention-based one-stage framework for person search," by Chen et al. [16]. Detailed information of each article could be found in [11–16].

3 Communication and routing strategies

Two papers on communication and routing strategies are listed as follows: (1) "Asynchronous dissipative control for networked time-delay Markov jump systems with the event-triggered scheme and packet dropouts," by Chen et al. [17]; (2) "LEO laser microwave hybrid inter-satellite routing strategy based on modified Q-routing algorithm," by Zheng et al. [18]. Detailed information of each article could be found in [17, 18].

4 Optimization and algorithms

Four papers on optimization and algorithms are listed as follows: (1) "Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies," by Tariq [19]; (2) "DOA estimation algorithm based on spread spectrum sequence in low signal-to-noise ratio," by Zhou et al. [20]; (3) "A two-stage detection method of copy-move forgery based on parallel feature fusion," by Ye et al. [21]; (4) "Heuristic approaches for the car sequencing problems with block batches," by Yu et al. [22]. Detailed information of each article could be found in [19–22].

5 Data analysis

Five papers on data analysis are listed as follows: (1) "Coverless image steganography using morphed face recognition based on convolutional neural network," by Li et al. [23]; (2) "Robust watermarking algorithm for medical images based on log-polar transform," by Li et al. [24]; (3) "MFVT: an anomaly traffic detection method

merging feature fusion network and vision transformer architecture," by Li et al. [25]; (4) "SKDStream: a dynamic clustering algorithm on time-decaying data stream," by Liu et al. [26]; (5) "A novel high-dimensional trajectories construction network based on multi-clustering algorithm," by Ren et al. [27]. Detailed information of each article could be found in [23–27].

Authors' contributions
All authors hosted the special issue. Abel C. H. Chen and Chin-Ling Chen wrote the editorial. All authors read and approved the final manuscript.

Declarations

Competing interests
Guest Editors declare no conflict of interest.

Received: 25 April 2023
Published online: 19 May 2023

References

1. C. Shi, L. Fang, Z. Lv, M. Zhao, Explainable scale distillation for hyperspectral image classification. Pattern Recognit. **122**, 108316 (2022). https://doi.org/10.1016/j.patcog.2021.108316
2. C.H. Chen, An arrival time prediction method for bus system. IEEE Internet Things J. **5**(5), 4231–4232 (2018). https://doi.org/10.1109/JIOT.2018.2863555
3. X. Xue, C. Jiang, J. Zhang, C. Hu, Biomedical ontology matching through attention-based bidirectional long short-term memory network. J. Database Manag. **32**(4), 14–27 (2021). https://doi.org/10.4018/JDM.2021100102
4. G. Liu, L. Xie, C.H. Chen, Unsupervised text feature learning via deep variational auto-encoder. Inf. Technol. Control. **49**(3), 421–437 (2020). https://doi.org/10.5755/j01.itc.49.3.25918
5. X. Xue, H. Wang, W. Liu, Matching sensor ontologies with unsupervised neural network with competitive learning. PeerJ Comput Sci. **7**, 763 (2021). https://doi.org/10.7717/peerj-cs.763
6. C. Shi, L. Fang, Z. Lv, H. Shen, Improved generative adversarial networks for VHR remote sensing image classification. IEEE Geosci. Remote. Sens. Lett. **19**, 1–5 (2022). https://doi.org/10.1109/LGRS.2020.3025099
7. Z. Sun, D. Han, D. Li et al., A blockchain-based secure storage scheme for medical information. J. Wirel. Commun. Netw. **2022**, 40 (2022). https://doi.org/10.1186/s13638-022-02122-6
8. X. Lv, D. Han, D. Li et al., Network abnormal traffic detection method based on fusion of chord similarity and multiple loss encoder. J. Wirel. Commun. Netw. **2022**, 105 (2022). https://doi.org/10.1186/s13638-022-02180-w
9. D.C. Huang, C.F. Hsiao, T.W. Chang et al., A security method of hardware Trojan detection using path tracking algorithm. J. Wirel. Commun. Netw. **2022**, 81 (2022). https://doi.org/10.1186/s13638-022-02165-9
10. J.H.J. Hou, X. Xie, Q. Cai et al., Early warning system for drivers' phone usage with deep learning network. J. Wirel. Commun. Netw. **2022**, 42 (2022). https://doi.org/10.1186/s13638-022-02121-7
11. B. Wang, G. Li, C. Wu et al., A framework for self-supervised federated domain adaptation. J. Wirel. Commun. Netw. **2022**, 37 (2022). https://doi.org/10.1186/s13638-022-02104-8
12. N. Wei, L. Wang, G. Chen et al., Mixed-type data generation method based on generative adversarial networks. J. Wirel. Commun. Netw. **2022**, 22 (2022). https://doi.org/10.1186/s13638-022-02105-7
13. T. Liu, Z. Yu, The analysis of financial market risk based on machine learning and particle swarm optimization algorithm. J. Wirel. Commun. Netw. **2022**, 31 (2022). https://doi.org/10.1186/s13638-022-02117-3
14. L. Liu, M. Gao, Y. Zhang et al., Application of machine learning in intelligent encryption for digital information of real-time image text under big data. J. Wirel. Commun. Netw. **2022**, 21 (2022). https://doi.org/10.1186/s13638-022-02111-9
15. J. Li, Y. Wang, S. Li, Effects of psychological fatigue on college athletes' error-related negativity based on artificial intelligence computing method. J. Wirel. Commun. Netw. **2022**, 76 (2022). https://doi.org/10.1186/s13638-022-02166-8
16. Y. Chen, D. Han, M. Cui et al., ABOS: an attention-based one-stage framework for person search. J. Wirel. Commun. Netw. **2022**, 75 (2022). https://doi.org/10.1186/s13638-022-02157-9
17. H. Chen, R. Liu, P. He et al., Asynchronous dissipative control for networked time-delay Markov jump systems with event-triggered scheme and packet dropouts. J. Wirel. Commun. Netw. **2022**, 82 (2022). https://doi.org/10.1186/s13638-022-02156-w
18. F. Zheng, C. Wang, Z. Zhou et al., LEO laser microwave hybrid inter-satellite routing strategy based on modified Q-routing algorithm. J. Wirel. Commun. Netw. **2022**, 36 (2022). https://doi.org/10.1186/s13638-022-02119-1
19. U. Tariq, Rampant Smoothing (RTS) Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies. J. Wirel. Commun. Netw. **2022**, 47 (2022). https://doi.org/10.1186/s13638-022-02123-5
20. F. Zhou, W. Zhang, B. Zhang et al., DOA estimation algorithm based on spread spectrum sequence in low signal-to-noise ratio. J. Wirel. Commun. Netw. **2022**, 60 (2022). https://doi.org/10.1186/s13638-022-02142-2
21. W. Ye, Q. Zeng, Y. Peng et al., A two-stage detection method of copy-move forgery based on parallel feature fusion. J. Wirel. Commun. Netw. **2022**, 30 (2022). https://doi.org/10.1186/s13638-022-02112-8

22. Y. Yu, X. Lu, T. Zhao et al., Heuristic approaches for the car sequencing problems with block batches. J. Wirel. Commun. Netw. **2022**, 26 (2022). https://doi.org/10.1186/s13638-022-02113-7
23. Y.H. Li, C.C. Chang, G.D. Su et al., Coverless image steganography using morphed face recognition based on convolutional neural network. J. Wirel. Commun. Netw. **2022**, 28 (2022). https://doi.org/10.1186/s13638-022-02107-5
24. T. Li, J. Li, J. Liu et al., Robust watermarking algorithm for medical images based on log-polar transform. J. Wirel. Commun. Netw. **2022**, 24 (2022). https://doi.org/10.1186/s13638-022-02106-6
25. M. Li, D. Han, D. Li et al., MFVT: an anomaly traffic detection method merging feature fusion network and vision transformer architecture. J. Wirel. Commun. Netw. **2022**, 39 (2022). https://doi.org/10.1186/s13638-022-02103-9
26. H. Liu, A. Wu, M. Wei et al., SKDStream: a dynamic clustering algorithm on time-decaying data stream. J. Wirel. Commun. Netw. **2022**, 102 (2022). https://doi.org/10.1186/s13638-022-02160-0
27. F. Ren, Y. Han, S. Wang et al., A novel high-dimensional trajectories construction network based on multi-clustering algorithm. J. Wirel. Commun. Netw. **2022**, 18 (2022). https://doi.org/10.1186/s13638-022-02108-4

Publisher's Note