Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8374473, 8 pages
https://doi.org/10.1155/2022/8374473

Research Article

Security-Aware Routing Protocol Based on Artificial Neural Network Algorithm and 6LoWPAN in the Internet of Things

Jiangdong Lu, Dongfang Li, Penglong Wang, Fen Zheng, and Meng Wang

Department of Computer and Simulation Technology, Naval Medical University, Shanghai 200433, China

Correspondence should be addressed to Fen Zheng; c12169@yahoo.com

Received 22 November 2021; Revised 13 December 2021; Accepted 16 December 2021; Published 12 January 2022

Academic Editor: Nima Jafari Navimipour

Today, with increasing information technology such as the Internet of Things (IoT) in human life, interconnection and routing protocols need to find optimal solution for safe data transformation with various smart devices. Therefore, it is necessary to provide an enhanced solution to address routing issues with respect to new interconnection methodologies such as the 6LoWPAN protocol. The artificial neural network (ANN) is based on the structure of intelligent systems as a branch of machine interference, has shown magnificent results in previous studies to optimize security-aware routing protocols. In addition, IoT devices generate large amounts of data with variety and accuracy. Therefore, higher performance and better data handling can be achieved when this technology incorporates data for sending and receiving nodes in the environment. Therefore, this study presents a security-aware routing mechanism for IoT technologies. In addition, a comparative analysis of the relationship between previous approaches discusses with quality of service (QoS) factors such as throughput and accuracy for improving routing mechanism. Experimental results show that the use of time-division multiple access (TDMA) method to schedule the sending and receiving of data and the use of the 6LoWPAN protocol when routing the sending and receiving of data can carry out attacks with high accuracy.

1. Introduction

The world of information technology and computers is expanding daily. This development has led to the creation of new systems with a specific type of communication [1, 2]. One of these connections is machine to machine. This type of communication is a solution to move, from single-purpose devices that data in the form of commands obtained from an application in the network to the Internet of Things (IoT) that allows the device to be multipurpose and applications to collaborate. Machine-to-machine communication with network structures can benefit from global standardization efforts [3–5]. Admittedly, the network-to-machine communication facilitation network has changed dramatically and its capabilities have greatly expanded, but machine-to-machine architectural solutions have remained relatively stable [6].

One of the most important parts of the Internet is bandwidth, which needs to be used to access objects connected to the Internet easily and quickly [7, 8]. When a packet is sent by a sender, some quality of service (QoS) factors such as response time, throughput, security, energy consumption, latency, and accuracy will be evaluated to show efficiency of the optimized routing protocol. Of course, considering the position and distance of objects is also very important. Today, by increasing intelligent attacks and anomaly behaviors, routing protocols should be aware on security and privacy conditions by using intrusion detection mechanisms. To improve security and throughput, it is necessary to have precise timing in the routing to avoid congestion. For this purpose, in the proposed method of this research, the TDMA protocol is used [9, 10], which can schedule. In this protocol, in the decision management section, the route operations are performed well and with high speed. After that, the bandwidth must be improved to ensure the security of the IoT environment. For this purpose, a protocol called 6LoWPAN will be used, which can improve bandwidth along with ensuring security [11]. But because its execution speed is slow and can affect security and even bandwidth access, it creates an optimization domain that is considered

a search environment [12]. Therefore, the artificial neural network (ANN) algorithm will be used chaotically to optimize bandwidth and increase security in intrusion detection method and solve connection problems between objects in the IoT environment, which will be promoted as a new idea in this research. One of the attacks that can be imagined in this research, and its main purpose is to identify it, is a flood attack on the IoT [13].

The main contribution of this study is organized as follows:

(i) Proposing a scheduling protocol TDMA in the routing process with the lowest energy consumption

(ii) Using the 6LoWPAN protocol and optimizing it to increase bandwidth and improve packet lost ratio in the IoT environment

(iii) Applying ANN-based machine learning method to enhance the data transmission routing

(iv) Evaluating performance of the proposed method and it is compared with recent developed methods

The rest of this paper is organized as follows: Section 2 present a literature review on recent routing mechanisms in IoT environments. Section 3 proposed a security-aware routing protocol with respect to an enhanced ANN method. Section 4 shows experimental results based on simulation results. Finally, Section 5 shows conclusion and future work.

2. Related Works

This section illustrates a brief literature review on recent routing mechanisms using metahueristic algorithms. For example, authors in [14] offered a blockchain-SDN-based assigned design for intelligent cities with network function virtualization. Furthermore, the authors introduced an energy-optimized group leader determination algorithm that introduces to choose a group leader in an effective method. Besides, the SDN controller controls and supervises the actions of the IoT devices. In this paper, blockchain is applied to identify and overcome the cyberattacks in the IoT systems. The test outcome revealed that the proposed design works better rather than the current structure in terms of throughput, time, gas consumption, and communication overhead.

Authors in [15] reviewed energy control progresses in IoT based on an SLR style. 30 research studies were determined as the principal field of technical study. For analyzing existing issues on the energy control resolutions in IoT, a taxonomy was introduced to explain the technical features of each section of energy control. It is mentioned that a class of published research articles with 7 studies in the intelligent home have the largest percentage. Furthermore, energy control on intelligent collection, intelligent cities, and the intelligent building has been studied with 15 papers individually. Finally, smart grid and industry circumstances have 8 research studies in IoT networks.

Authors in [16] suggested a unique method for RPL protocol trying to develop the IoT network lifetime. The suggested method combined the consumed and recharged energy to choose the most suitable route to send data information. Simulation results showed that the proposed method efficiently reduced the energy loss and the network lifetime by choosing the best routes via the sink.

Authors in [17] introduced an innovative routing protocol that is suitable for mobile ad hoc networks, in particular, to be aware of node movement and link resistance. To this goal, a different movement discovery design was offered to provide any node to set a new metric based on the renewed movement factor. Therefore, each node in the networks can change its routing function based on the network requirements around it; consequently, the applied routing protocol can improve the packet delivery ratio compared to existing routing methods.

Authors in [18] proposed a framework based on machine learning techniques and artificial neural networks for identifying the RPL attacks in some case studies. The efficiency of the proposed framework is improved to the highest potential amount. The implementation outcomes revealed that the malicious node for the attack provides the highest amount of packets between all the nodes in the network. Consequently, it increases the energy usage of neighbors.

Authors in [19] suggested a method for determining congestion problems in IoT networks by offering the use of fuzzy logic. The difficulty of parent choice is formed and then solved applying the fuzzy weighted sum procedure. The suggested algorithm is dynamic and recognized the congestion and then chose the noncongested path by choosing the most suitable path in the network topology. The achieved outcomes from the Cooja simulator proved that the proposed algorithm has decreased delay and improved performance and more efficient use of network resources.

Authors in [20] presented a new method based on priority and energy usage to manage routing procedures within contents for low-power and lossy networks. All network slots apply timing models when transferring data to the target while analyzing network transfer, audio, and image information. This technique improved the robustness of the routing protocol and was eventually avoided from occurring congestion, too. Test results confirmed that the proposed method decreased overhead on the mesh, delay, and energy waste.

Authors in other recent works [21, 22] have applied heuristic algorithms to solve routing problem in IoT environments. Some of them check packet duration time and energy efficiency as well.

3. Proposed Security-Aware Routing Method

This section illustrates a new security-aware routing mechanism based on ANN prediction approach in IoT. One of the most important problems in establishing the IoT [23] with an energy-aware recognition approach is that nodes have no information about each other's performance [24]. The only information they receive from a primary source is authentic packets that are all broadcasted by the device or object itself and are not trusted under internal attacks. For this purpose, the packet find index (PFI) is expressed as [25]

$$PFI_{IJ} = \frac{1}{P_f^{ij}}. \quad (1)$$

The value P_f^{ij} is obtained from [26]

$$P_f^{ij} = \frac{N_s^{ij}}{N_t^{ij}}. \quad (2)$$

The PFI factor is calculated in the TDMA method with respect to applying the QoS factors. According to Equation (2), N_s^{ij} is the number of packets properly routed by node next step j in the IoT environment and N_t^{ij} is the total number of packets routed from node i to the next step j in the IoT environment. Using this relation, each node can obtain the packet find index for its next step nodes and calculates the packet find index of the path according to [27]

$$\begin{aligned} \mathrm{PFI}_{\mathrm{path}} = {} & \left(10 \times \mathrm{PFI}_{i,j+1}\right) + \log\left(10 \times \mathrm{PFI}_{i+1,i+2}\right) \\ & + \log\left(10 \times \mathrm{PFI}_{i+2,i+3}\right). \end{aligned} \quad (3)$$

After calculating the packet find index, each node calculates the path find index and then selects the path that has the best index to guide the data packets from the paths provided by the next step nodes. In this way, it removes malicious nodes from the closed path [28].

Figure 1 illustrates a brief procedure of the ANN strategy for a routing protocol using TDMA with respect to supporting QoS factors. In first step, each nominated IoT node should be checked as a cluster node. If the respected IoT node is cluster node, then the ANN method is applied to train and test procedure. The ANN method sets initial parameters for training layers and divides the dataset into two, train and test datasets. For each classification procedure, the TDMA factors are applied to check with classification method. Finally, the existing TDMA schedule is applied to the train test case [29]. On the other hand, if the IoT node is not a cluster node, system updates cluster list and the ANN method is applied to continue train procedure. For finalizing the proposed algorithm, each train set should archived convergence factor. If the algorithm has a convergence value, then the classification procedure will be finished. Otherwise, the system sends a message to check cluster node selection.

To calculate the PFI [30], after calculating the PFI of each parent [31], each node adds it to the value received from the parent and distributes it to all other nodes to determine the closed conduction index of each path. Node S then selects the path with the least possible value from the provided paths, and in this way, the malicious node G, which is a gray holes node that bypasses 50% of the packets, causing routing loss and loss. Energy will be removed from the data transmission path. It is important to note that these values are moved by the control packets, and all nodes are aware of them [32]. The goal of the PFI is to obtain routes with higher delivery rates so that malicious nodes can be removed from the packet routing path to provide the correct routing in the IoT environment. PFI is expressed as the number of transfers required to reach a destination pack. This index can be used as a metric (unit of measurement) in the initial deployment of the Internet of Things and to identify paths that have malicious black holes or gray holes nodes [33]. But this metric also has its limitations and problems. This index is introduced on the path, and the nodes should calculate the value of the path packet guidance index after calculating their parent packet guidance index and inform these nodes about these values, which is done with the help of control packets. For this purpose, to compare the metric of the closed conduction index with the expected number of transfers, with the help of simulation in MATLAB environment, these two metrics have been implemented on the processing environment. Because the IoT does not have proper routing and delivery operations and its problems were mentioned in previous sections, especially in the issue of security in intrusion detection method, this secure establishment of the IoT due to the presence of appendages such as black holes and gray holes and in general security issues remain almost unresolved. Bandwidth and security are also important during deployment in the intrusion detection method [34].

It is assumed that the target monitoring area in the IoT called A is a two-dimensional environment, and n moving nodes are randomly placed in the environment as $S = (S1, S2 \cdots)$. The ith position of the node is determined as a set $si = (xi\, xi, yi)$ $(i = 1, 2 \cdots n)$, and the Euclidean distance between the ith node and the point $p = (x, y)$ is determined according to [35]

$$d_{ip} = \sqrt{(x - x_i)^2 + (y - y_2)^2}. \quad (4)$$

The node detection model is divided into two methods of binary-based detection and probabilistic detection. This research is based on the binary mode, which is simpler to use and less computationally complex. The reason for using binary node detection, in addition to simplicity in application and less computational complexity, is the simplicity of its modeling, and also each time execution will not be a possible answer and the answer is guaranteed. Node detection is used probabilistically in other networks such as automotive wireless networks and underwater wireless sensor networks. The node detection model is calculated binary-based as [36]

$$p = \left(\text{if } d_{ip} \le r0 \cdot k = 1 \text{ else } k = 0\right). \quad (5)$$

In this research, several evaluation methods have been used which include throughput and the accuracy criteria. At the beginning, each study is completed, and finally, the results obtained from the research performed by each evaluation method are mentioned.

The secure deployment of the IoT was completely modeled on security issues in this section with a security-aware routing mechanism. Based on this mechanism, data

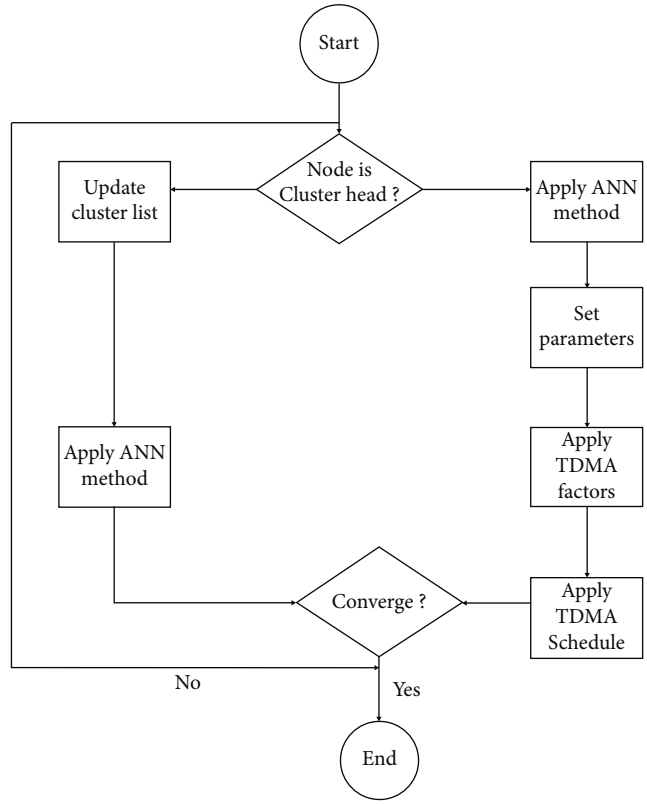

Figure 1: Procedure of the TDMA method using the ANN algorithm.

Table 1: Initial parameters of each tests case to detect attacks.

Test case	Number of IoT nodes	Number of features	Number of repetitions
Case 1	5, 10, 20	30	5000
Case 2	20, 30, 50	50	10000
Case 3	50, 80, 100	80	15000

transmission through the network, data confidentiality, accuracy, information integrity, accessibility, and attack detection were considered and a new and optimal model with knowledge of security issues was considered. In the next section, a simulation of the proposed approach will be performed and the results will be discussed [37].

4. Experimental Results and Discussion

In the previous section, new modeling was done to provide a way to ensure security of the intrusion detection method the IoT. Of course, any idea will need a simulation. In this section, the experimental results are performed in the MATLAB environment and fully mentioned and analyzed the results based on the intrusion detection method. A test case comparison is made between the available methods to ensure that the proposed approach is effective.

In this study, which is based on attacks that are supposed to improve the level of security to be able to measure the QoS, attacks on deprivation of services have been used. Hence, the DoS2017 dataset is used https://www.unb.ca/cic/datasets/dos-dataset.html, and the TDMA protocol should first be considered during routing after nodes are placed in the environment to schedule and reduce energy with the 6LoWPAN protocol [38]. In the following, the proposed approach detects attacks of deprivation of services in the context of the Internet of Things, and finally, the criteria of service quality and energy consumption are examined. Based on the analysis of the proposed approach in sending and receiving data and the proposed mechanism, it is important to examine the degree of accuracy criteria that detect attacks for security. The number of repetitions of the program is 5000, 10000, and 15000 rounds. Also, the number of features in each round is 30, 50, and 80 repetition and the number of IoT devices are including 20, 50, and 100. The storage of sent and received data in the IoT environment is placed in an intelligent and impenetrable database called a transmission rate. The initial parameters of each test case of security analysis results are presented in Table 1.

After examining all case studies with respect to detecting attacks, QoS factors are reviewed. Figures 2–4 show the throughput after applying the proposed mechanism for case study 1, 2, and 3 to the IoT environment.

The throughput is achieved according to the transmitted packets. The throughput obtained by proposed method is compared with existing algorithms, and the comparison

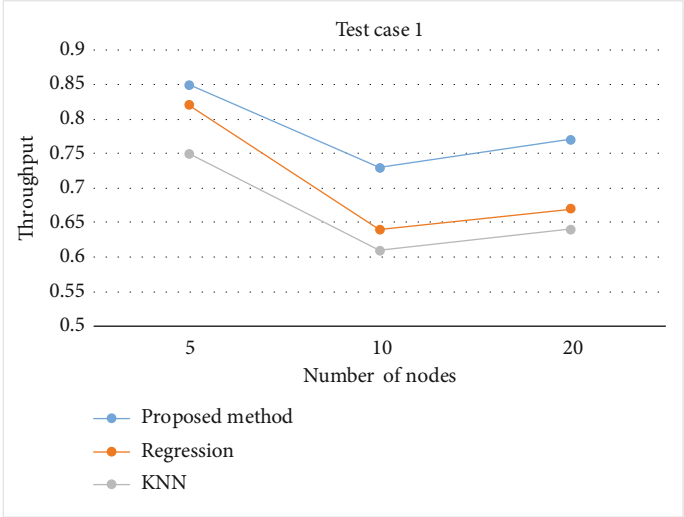

Figure 2: Throughput evaluation for existing algorithms in case study 1.

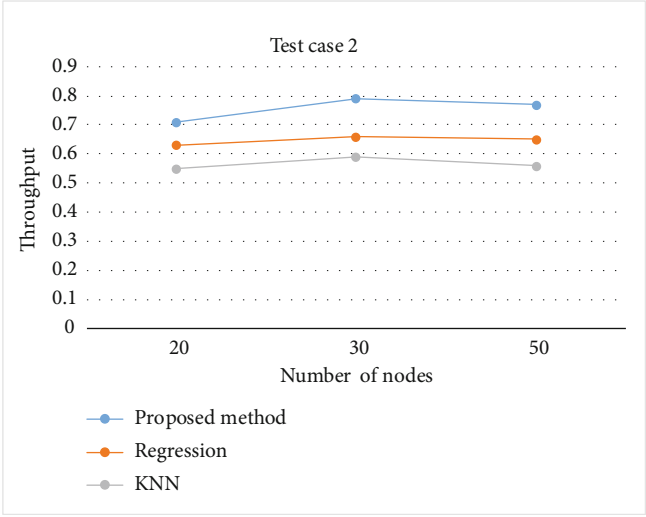

Figure 3: Throughput evaluation for existing algorithms in case study 2.

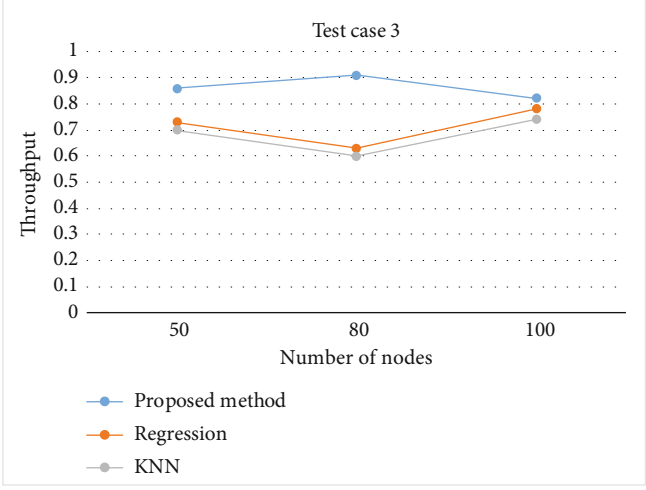

Figure 4: Throughput evaluation for existing algorithms in case study 3.

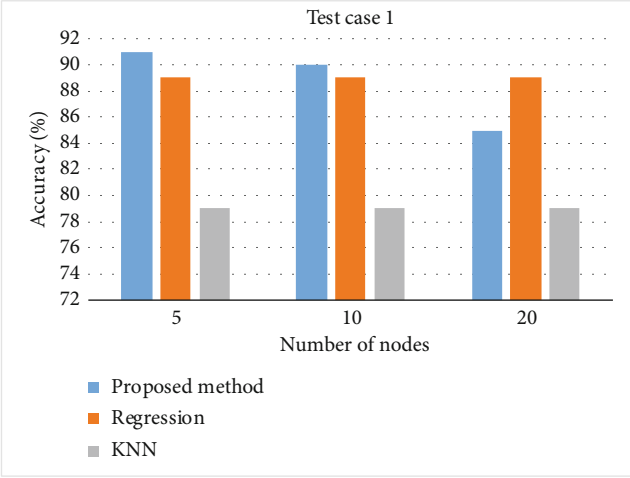

Figure 5: Accuracy evaluation factor for existing algorithms in case study 1.

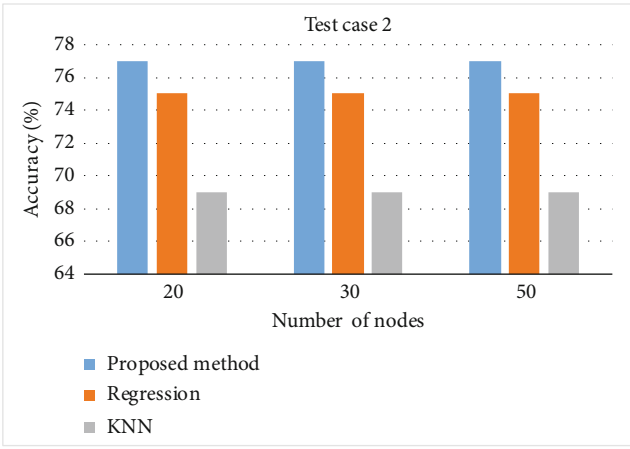

Figure 6: Accuracy evaluation factor for existing algorithms in case study 2.

results regression and KNN algorithms [39, 40]. The throughput of proposed method is found better than the other existing algorithms. Recently developed regression also obtained almost similar performance; however, it fails to attain an effective result on accuracy due to this and the throughput also gets reduced. It is observable that the ANN method with respect to the TDMA factors has optimized throughput value than other regression and the KNN algorithms in test cases 1, 2, and 3.

In the following, we examine the data accuracy in each case study. If the environment is secure, the data is encrypted in the transmitter and data can predicted with the proposed ANN approach with high accuracy. Figures 5–7 show the accuracy diagram of the proposed method in blue line with number of IoT devices in which it has higher accuracy than the previous two methods in case study 1, 2, and 3, respectively. Totally, we conclude that the proposed method has maximum accuracy factor for each

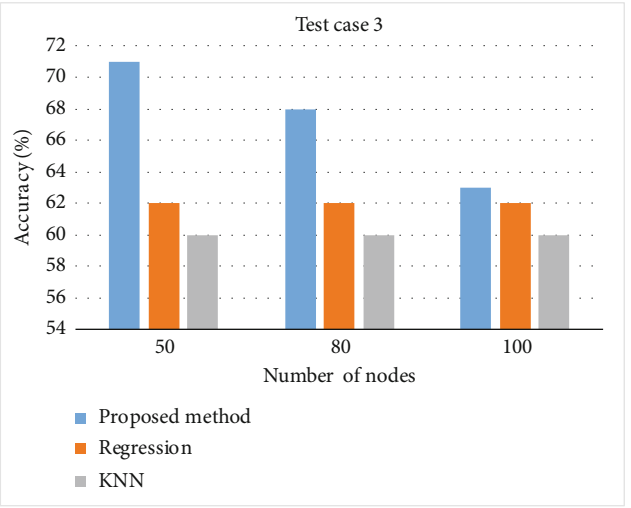

Figure 7: Accuracy evaluation factor for existing algorithms in case study 3.

test cases 1, 2, and 3 to compare other regression and KNN algorithms.

The proposed method has achieved better accuracy which is found higher than the other existing algorithms with respect to number of IoT nodes and number of features.

5. Conclusion

In order to solve the problem of security-aware routing protocol in IoT environments, the ANN algorithm and TDMA protocol are given by studying the connectivity of network topologies. The method proposes an efficient routing protocol based on the 6LoWPAN strategy. First, we analyze the relationship between nodes and explain the scheduling packets and through modularization. Experimental results showed that the proposed method is compared with regression and KNN algorithms for simulation environments. The results show that the proposed method can effectively improve the accuracy ratio and enhance throughput factor. The research on the relevant theories and technologies of IoT has important value for the routing algorithms in the future 5G era as future work. Also, some evaluation metrics such as mean square error (MSE), time complexity, and packet loss with large amount of IoT nodes can be evaluated and analyzed in future research directions.

Data Availability

The CIC DoS dataset (2017) used to support the findings of this study are included at the following web page: https://www.unb.ca/cic/datasets/dos-dataset.html.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] R. Liu, X. Wang, H. Lu et al., "SCCGAN: style and characters inpainting based on CGAN," *Mobile Networks and Applications*, vol. 26, no. 1, pp. 3–12, 2021.

[2] M. Zhang, Y. Chen, and W. Susilo, "PPO-CPQ: a privacy-preserving optimization of clinical pathway query for e-healthcare systems," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10660–10672, 2020.

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

[4] J. Yan, Y. Meng, X. Yang, X. Luo, and X. Guan, "Privacy-preserving localization for underwater sensor networks via deep reinforcement learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1880–1895, 2021.

[5] T. Ni, D. Liu, Q. Xu, Z. Huang, H. Liang, and A. Yan, "Architecture of cobweb-based redundant TSV for clustered faults," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 7, pp. 1736–1739, 2020.

[6] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial security solution for virtual reality," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6273–6281, 2021.

[7] Y. Jiang and X. Li, "Broadband cancellation method in an adaptive co-site interference cancellation system," *International Journal of Electronics*, pp. 1–21, 2021.

[8] 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*, 2021.

[9] Z. Lv, L. Qiao, and I. You, "6G-enabled network in box for internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[10] A. Seyfollahi and A. Ghaffari, "A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8414503, 32 pages, 2021.

[11] M. Etemadi, M. Ghobaei-Arani, and A. Shahidinejad, "Resource provisioning for IoT services in the fog computing environment: an autonomic approach," *Computer Communications*, vol. 161, pp. 109–131, 2020.

[12] Z. Lv, D. Chen, and Q. Wang, "Diversified technologies in internet of vehicles under intelligent edge computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2048–2059, 2021.

[13] 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.

[14] M. J. Islam, A. Rahman, S. Kabir et al., "Blockchain-SDN based energy-aware and distributed secure architecture for IoTs in smart cities," *IEEE Internet of Things Journal*, 2021.

[15] D. Wang, D. Zhong, and A. Souri, "Energy management solutions in the Internet of Things applications: technical analysis and new research directions," *Cognitive Systems Research*, vol. 67, pp. 33–49, 2021.

[16] F. Chiti, R. Fantacci, and L. Pierucci, "A green routing protocol with wireless power transfer for internet of things," *Journal of Sensor and Actuator Networks*, vol. 10, no. 1, p. 6, 2021.

[17] A. Serhani, N. Naja, and A. Jamali, "AQ-routing: mobility-, stability-aware adaptive routing protocol for data routing in MANET–IoT systems," *Cluster Computing*, vol. 23, no. 1, pp. 13–27, 2020.

[18] S. Sharma and V. K. Verma, "AIEMLA: artificial intelligence enabled machine learning approach for routing attacks on internet of things," *The Journal of Supercomputing*, vol. 77, no. 12, pp. 13757–13787, 2021.

[19] J. Shreyas, H. Singh, S. Tiwari, N. N. Srinidhi, and S. M. Dilip Kumar, "CAFOR: congestion avoidance using fuzzy logic to find an optimal routing path in 6LoWPAN networks," *Journal of Reliable Intelligent Environments*, vol. 7, no. 4, pp. 325–340, 2021.

[20] F. Safara, A. Souri, T. Baker, I. al Ridhawi, and M. Aloqaily, "PriNergy: a priority-based energy-efficient routing method for IoT systems," *The Journal of Supercomputing*, vol. 76, no. 11, pp. 8609–8626, 2020.

[21] R. Yarinezhad and S. Azizi, "An energy-efficient routing protocol for the Internet of Things networks based on geographical location and link quality," *Computer Networks*, vol. 193, article 108116, 2021.

[22] R. Sahay, G. Geethakumari, and B. Mitra, "A novel network partitioning attack against routing protocol in internet of things," *Ad Hoc Networks*, vol. 121, article 102583, 2021.

[23] Z. Lv, R. Lou, and A. K. Singh, "AI empowered communication systems for intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4579–4587, 2021.

[24] H. Yi, "Secure social internet of things based on post-quantum blockchain," *IEEE transactions on Network Science and Engineering*, 2021.

[25] J. Dong, Y. Cong, G. Sun, Z. Fang, and Z. Ding, "Where and how to transfer: knowledge aggregation-induced transferability perception for unsupervised domain adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2021.

[26] H. Chen, Y. Miao, Y. Chen, L. Fang, L. Zeng, and J. Shi, "Intelligent model-based integrity assessment of nonstationary mechanical system," *Engineering*, 2021.

[27] F. Liu, G. Zhang, and J. Lu, "Multisource heterogeneous unsupervised domain adaptation via fuzzy relation neural networks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3308–3322, 2021.

[28] Z. Lv, Z. Wu, X. Wang, and M. Zhou, "3D facial similarity measurement and its application in facial organization," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 16, no. 3, pp. 1–20, 2020.

[29] M. K. Khan, M. Shiraz, K. Zrar Ghafoor, S. Khan, A. Safaa Sadiq, and G. Ahmed, "EE-MRP: energy-efficient multistage routing protocol for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6839671, 13 pages, 2018.

[30] C. Qin, Y. Jin, J. Tao et al., "DTCNNMI: a deep twin convolutional neural networks with multi-domain inputs for strongly noisy diesel engine misfire detection," *Measurement*, vol. 180, article 109548, 2021.

[31] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of using blockchain to protect the privacy of drone big data," *IEEE Network*, vol. 35, no. 1, pp. 44–49, 2021.

[32] H. Che and J. Wang, "A two-timescale duplex neurodynamic approach to mixed-integer optimization," *IEEE Transactions*

on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 36–48, 2021.

[33] W. Zhou, L. Yu, Y. Zhou, W. Qiu, M. W. Wu, and T. Luo, "Local and global feature learning for blind quality evaluation of screen content and natural scene images," *IEEE Transactions on Image Processing*, vol. 27, no. 5, pp. 2086–2095, 2018.

[34] M. Ghobaei-Arani, "A workload clustering based resource provisioning mechanism using biogeography based optimization technique in the cloud based systems," *Soft Computing*, vol. 25, no. 5, pp. 3813–3830, 2021.

[35] 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.

[36] S. Lv and F. Song, "Particle swarm intelligence and the evolution of cooperation in the spatial public goods game with punishment," *Applied Mathematics and Computation*, vol. 412, article 126586, 2022.

[37] T. Sui, D. Marelli, X. Sun, and M. Fu, "Multi-sensor state estimation over lossy channels using coded measurements," *Automatica*, vol. 111, article 108561, 2020.

[38] H. H. Jazi, H. Gonzalez, N. Stakhanova, and A. A. Ghorbani, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," *Computer Networks*, vol. 121, pp. 25–36, 2017.

[39] H. Liu, J. Liu, S. Hou, T. Tao, and J. Han, "Perception consistency ultrasound image super-resolution via self-supervised CycleGAN," *Neural Computing and Applications*, pp. 1–11, 2021.

[40] S. Tofighy, A. A. Rahmanian, and M. Ghobaei-Arani, "An ensemble CPU load prediction algorithm using a Bayesian information criterion and smooth filters in a cloud computing environment," *Software: Practice and Experience*, vol. 48, no. 12, pp. 2257–2277, 2018.