Ad Hoc Networks 119 (2021) 102541

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Privacy reinforcement learning for faults detection in the smart grid

Asma Belhadi [a], Youcef Djenouri [b], Gautam Srivastava [c,d], Alireza Jolfaei [e], Jerry Chun-Wei Lin [f,*]

[a] Kristiania University College, Norway
[b] Mathematics and Cybernetics, SINTEF Digital, Oslo, Norway
[c] Department of Math and Computer Science, Brandon University, Brandon, Canada
[d] Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan
[e] Department of Computing, Macquarie University, Sydney, Australia
[f] Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway

ARTICLE INFO

Keywords:
Energy systems
Privacy learning
Reinforcement learning
Anomaly detection
Smart grid

ABSTRACT

Recent anticipated advancements in ad hoc Wireless Mesh Networks (WMN) have made them strong natural candidates for Smart Grid's Neighborhood Area Network (NAN) and the ongoing work on Advanced Metering Infrastructure (AMI). Fault detection in these types of energy systems has recently shown lots of interest in the data science community, where anomalous behavior from energy platforms is identified. This paper develops a new framework based on privacy reinforcement learning to accurately identify anomalous patterns in a distributed and heterogeneous energy environment. The local outlier factor is first performed to derive the local simple anomalous patterns in each site of the distributed energy platform. A reinforcement privacy learning is then established using blockchain technology to merge the local anomalous patterns into global complex anomalous patterns. Besides, different optimization strategies are suggested to improve the whole outlier detection process. To demonstrate the applicability of the proposed framework, intensive experiments have been carried out on well-known CASAS (Center of Advanced Studies in Adaptive Systems) platform. Our results show that our proposed framework outperforms the baseline fault detection solutions.

1. Introduction

Automated energy management is an interesting area of research, particularly for distributed environments, where security and efficiency are crucial factors in the smart grid. The Internet of Things (IoT) plays an important role in addressing the challenges of different smart grid applications. IoT fosters new smart devices and applications as never seen before. Industry 4.0, medical monitorization, intelligent transport systems, smart agriculture, and Neighborhood Area Network (NAN) are just a few examples of the huge potential number of IoT smart grid applications will offer.

Smart Grid will be able to extend both monitoring as well as control within any electrical grid through the control of the bi-directional flow of data as well as electricity throughout an electrical grid network. Although there may exist many available technologies for communication, the ad hoc Wireless Mesh Network (WMN) has been well studied as a potential communication technology that is very well suited for the known requirements of the Smart grid's Neighborhood Area Networks (NAN) [1,2]. This has been due to the extended coverage (achieve through multi hopping), high throughput, low latency, and Quality of Service (QoS) abilities. All of these positive characteristics may enable data transportation using a hop by hop method from sources (for example, a Smart meter on every house) directly to backhaul distribution.

IoT technologies allow smart sensors to capture a large amount of data for further analysis [3], and most common research focuses on analyzing varied energy data in time and space through the smart grid. The most important representations in different industrial domains regarding energy perspectives including smart building [4], power systems [5], and renewable energy [6] in time series. You can analyze time series by processing long sequences of data through data mining, deep learning, or neural network technologies [7,8]. Time series research is one of the hot topics in the field of time series anomaly identification. The purpose of this analysis is to detect trends that are not "normal" (abnormal) from a collection of time series. Local Outlier Factor (LOF) is one of the most well-known anomaly detection techniques focused on using density computation. LoF has successfully made it possible to work with numerous industrial IoT technologies such as engineering [9], intelligent transportation [10], and many others; there is the unlimited capacity of LoF. However, methods [11–13] to detect basic outliers are only able to distinguish simple outliers, but cannot detect

* Corresponding author.
E-mail address: jerrylin@ieee.org (J.C.-W. Lin).

https://doi.org/10.1016/j.adhoc.2021.102541
Received 1 February 2021; Received in revised form 12 April 2021; Accepted 11 May 2021
Available online 28 May 2021

complex outliers. For instance, Javaid et al. [11] identify outliers in smart grid environments by developing an adaptive synthesis system to deal with imbalanced smart grid data. Nesa et al. [12] proposed an outlier detection solution for IoT environments while considering the errors caused by a malfunctioning sensor and the unusual phenomenon. Feremans et al. [13] suggested an anomaly detection strategy to deal with the mixed-type time series by exploring frequent pattern mining processes in the training of the isolation forest structure.

In comparison, the numerous implementations that do not have a stable platform for distributed data processing; privacy and security issues have become the problems. Blockchain technology has recently seen exciting opportunities and plenty of interest in the business and academia [14,15]. The implementation of effective cryptographic tools helps solve distributed problems.

Deep learning, blockchain technologies, and the collaborative design of artificial intelligence (AI) merged to become the special and most powerful method in heterogeneous and distributed computing [16–18] applied in many domains and applications. In recent years, as you might know, AI has gained considerable interest and has been used in many areas, such as reinforcement learning with Blockchain [16, 19]. Many studies had built their reinforcement learning models on a blockchain that is used for safely protecting the next-generation wireless networks. Also, other works followed a reinforcement learning approach to provide a framework for assessing the industrial Internet of things networks regarding several aspects, e.g., security, latency, decentralization, and scalability [20,21]. This paper covers the state-of-the-art blockchain learning frameworks and also introduces a new paradigm focused on blockchain learning to automatically detect time series of anomalous patterns in a distributed and heterogeneous setting. This article reflects on the most significant contributions in this paper as follows.

1. We design a new method to help us identifying the complex anomalous patterns in distributed and heterogeneous time series.
2. The LOF algorithm is considered in the designed model to verify local anomalous patterns on each side of the distributed network.
3. We present a new approach that incorporates blockchain and reinforcement learning to discover global complex anomalous patterns from local simple anomalous patterns. Here, the blockchain is used to secure and protect the meting process while reinforcement learning is used to verify the complex anomalous patterns accurately.
4. Different optimization strategies have been suggested to improve the whole detection process. These strategies are based on both constraint satisfaction solvers and metaheuristic-based search.
5. We analyze the proposed framework on energy system use case. The findings indicated that the developed system is much greater and effective than the generic fault detection solutions.

The rest of this paper is organized as follows: Related work is summarized in Section 2. The problem of this paper and the proposed framework are respectively discussed in Section 3 and Section 4. We report our experimental results in Section 5. Section 6 gives the conclusion of this work.

2. Related work

A quick summary of the two major topics in this paper, e.g., the studies of time series anomaly identification in the smart grid and other applicable domains as well as a subsection on blockchain learning.

2.1. Anomaly detection

Singh et al. [22] explored different outlier detection techniques, in different data representations including time-series data. It also defines multiple kinds of outliers such as simple outliers, contextual outliers, collective outliers. Tao et al. [23] developed a spark-based parallel approach for network traffic anomaly detection to detect intrusion in the network. Their approach benefits from the merits of the gated recurrent unit self-learning and long-term dependency processing to accurately identify anomalous patterns. The genetic algorithm is also explored to simulate the intelligent process in the training phase. Yu et al. [24] presented a new approach that firstly considers a forecasting model of the time series data regarding the training model for further finding the predictive values. Anomalies can be expected to take place if the observed values fall below the specified prediction confidence interval, which is calculated by considering the predictive value and confidence coefficient. Yamanishi et al. [25] developed an incremental-based probabilistic model to learn outliers from time-series data, where the score for each data value is computed to determine its deviation from the learned model. The same authors [26] proposed the use of an online discounting learning algorithm to learn the probabilistic model developed in [25]. It detected anomalies in an online process using a finite mixture model of the time series data source, where a high score of time series data indicating a high possibility of being a statistical outlier. Xie et al. [27] adopted the phase space reconstruction approach to convert time series data into multi-dimension space based on chaos theory. Different kinds of anomalous are then derived based on a decision tree algorithm. Nesa et al. [12] involved anomaly detection process in different layers of IoT architecture. It proposed a non-parametric-based learning algorithm considering malfunctioning sensors, unusual phenomenon, and a varied probability distribution of time series data. Na et al. [28] adopted a local outlier factor algorithm by developing a new density-based sampling strategy to summarize the time series data in a compact and efficient structure. This approach allows to avoid a large amount of memory space required by local outlier factor, and identify long time series outliers, not detected by the existing time series outlier detection techniques. Kieu et al. [29] proposed two recurrent-based approaches for time series-based anomaly detection. Both approaches exploited autoencoders with the sparsely-connected recurrent neural networks to generate multiple models with different neural network connection structures. Zhang et al. [30] considered the multi-scale convolutional recurrent encoder–decoder that is used to verify the abnormal behaviors from multivariate time series data. It first built the multi-resolution matrices to feature the multiple levels of different time steps. It then used a convolutional encoder to encode each time series data and capture the temporal patterns. A convolutional decoder is finally used to rebuilt to detect and diagnose anomalies. Feremans et al. [13] developed an anomaly detection approach for mixed-type time series data. It studied the different correlations among the time series data, and extract the frequent patterns to build and train the isolation forest structure.

2.2. Blockchain technology

Dai et al. [19] built a reinforcement learning model by considering the blockchain framework to protect the next generation of wireless networks. It was able to optimize the utility of the system and the reliability of the caching data shared across the network. Weng et al. [17] then considered a DeepChain model that is utilized in a distributed deep learning environment for handling federated learning in which the learners may have the wrong uprating progress of the parameters. It is designed by the use of a value-driven incentive system using blockchain to behave correctly of all participants. Liu et al. [16] then considered the blockchain-based Industrial IoTs, and analyzed the reinforcement learning models to detect the scalability, decentralization, latency, and fraud (security) that are necessary to

build for the industrial Internet of things systems. Qui et al. [31] then take the Q-learning and optimization issue into account to state and provide the solutions regarding the view change, access selection, and computational resource that were allocated in the blockchain model. Liu et al. [32] presented reinforcement learning by adopting blockchain models to develop a secure platform that can maximize the collected data in industrial IoT. Dai et al. [33] then investigated the offloading issue in the online system as the progress of the Markov decision model, which is merged by reinforcement learning, optimization (GA-based model), and blockchain mining to find the maximal results in terms of long-term offloading. Kadadha et al. [34] developed a game-based approach using blockchain technology to ensure the quality of services in an urban VANET network environment. It designed on-chain smart contracts, composed of two processes: The node reputation manager, and the relay selection game manager. Chai et al. [35] considered the federated learning in the hierarchical structure that can be used for sharing the knowledge in vehicle-based environments. Lu et al. [36] also considered the blockchain-empowered model used in the federated learning asynchronously for finding the solution to secure and protect the shared data in IoVs (Internet of vehicles). Besides, Qu et al. [37] developed a new blockchain-based strategy involving federated learning to allow the updating process executed at the local end devices then exchange the data with the globally blockchain-empowered federated learning approach. The system that is created by autonomous machine learning allowed the model to be maintained globally without any centralized authority. Luo et al. [38] made use of a collaborative Internet of things technology that included software-defined networking controllers, which would exchange information via the blockchain to synchronize and achieve a global view. The method exploits both the hidden features of the controllers and the resource limitations of the environment, thus minimizing computational requirements.

2.3. Motivation of the designed model

It is obvious that current solutions for time series data only have the potential to identify basic anomalous patterns, which is insufficient and not effective. The discovery of global anomalous patterns involves a highly safe distributed environment. As with current blockchain implementations, they are not ideal for dealing with time-series data. In comparison, we suggest a dedicated platform for identifying and learning deep anomalous patterns using blockchain technologies in heterogeneous distributed environments, which is suitable for security scenarios in industrial IoT using AI techniques, e.g., reinforcement learning in the designed model.

3. Problem statement

Definition 3.1 (*Time Series Database*)**.** Consider the set of m data $x = \{x_1, x_2, \ldots, x_m\}$, and each of the data is comprised of both spatial and time series parts. For x_l, it is considered as the lth data, and the concatenation progress of $x_l = [x_l(s)|x_l(t)]$ is then realized in which $x_l(s)$ shows the spatial information and $x_l(t)$ is the time series, respectively. While the r features is considered for the spatial information in which r is generally set as 2, and q features for the time series, we thus can obtain the following information for the lth data regarding $n = r + q$ dimensions as:

$$x_l = [x_{l1}(s), \ldots, x_{lr}(s)|x_{l1}(t), \ldots, x_{lq}(t)] \tag{1}$$

Definition 3.2 (*Similarity of time Series*)**.** Let x_1 and x_2 be the distances between two time series, respectively, we then can obtain that:

$$D(x_1, x_2) = SD(x_1, x_2) + TD(x_1, x_2), \tag{2}$$

in which (i) $SD(x_1, x_2)$ is the spatial distance that is measured by the similarity between two time series x_1 and x_2 and (ii) $TD(x_1, x_2)$ is the temporal distance that is used to measure the similarity of two time series x_1, and x_2. The spatial distance is obtained using Euclidean distance measure, and the temporal distance is determined using time-series measurements.

Definition 3.3 (*Candidates of Time Series*)**.** We define the set of the first p individual time series outliers found by a given time series outlier detection algorithm $\mathcal{A}$, denoted as $\mathcal{G}^+_{\mathcal{A}} = \{x_1^+, x_2^+ \ldots x_p^+\}$ by

$$\mathcal{G}^+_{\mathcal{A}} = \{x_i^+ | \forall j \in x \setminus \mathcal{G}^+_{\mathcal{A}}, SC(x_i, \mathcal{A}) \geq SC(x_j, \mathcal{A})\} \tag{3}$$

Note that SC(•, $\mathcal{A}$) is the ranking function used by $\mathcal{A}$.

Definition 3.4 (*Problem of Global Complex Anomalous Patterns Detection*)**.** Problem of global complex anomalous patterns detection considers to find the outliers of the set of all individual time series. In this paper, the set of all groups of time series outliers is then denoted as $\mathcal{G}^*$. We thus can obtain the following equation as:

$$\mathcal{G}^* = \{\mathcal{G}_i^* | Density(\mathcal{G}_i^*) \geq \gamma\} \tag{4}$$

Note that $Density(\mathcal{G})$ is the density of the group G, and γ is a varied density threshold in the range of $[0 \ldots m]$.

4. ITSA: Intelligent time series anomaly detection

In this section, we first give a brief overview of the main component of the developed ITSA (Intelligent Time Series Anomaly detection). The designed framework (as illustrated in Fig. 1) considers several perspectives together, e.g., blockchain, data mining, and reinforcement learning in deep learning. First, the data mining model is used to discover the local outlier factor that can be used to find the generic anomalous patterns locally from the time series. The reinforcement learning model of deep learning is then considered to merge the locally generic anomalous patterns discovered from each site forming the global complex anomalous patterns. The blockchain model is then utilized in the designed framework to secure the collected time series from them and the heterogeneous environment (each site in the designed system). Finally, the particle swarm optimization is used to efficiently find the hyper-parameters of the ITSA framework. We then can divide the designed ITSA framework into the following structures:

1. **Local Simple Anomalous Patterns Determination:** Typically, time series in most applications consist of temporal data points. The local simple anomalous patterns determination is performed using the local outlier factor, with the integration of DTW (Dynamic Time Warping) strategy to determine the similarity between time series data, having different time lengths.
2. **Global Complex Anomalous Patterns Determination:** After constructing the local simple anomalous patterns on each site, an intelligent merging strategy is used to derive the global complex anomalous patterns by employing reinforcement learning. We also integrate a blockchain mechanism to ensure data sharing across the different sites of the distributed system.

For the following sections, we illustrate the specifics behind ITSA components, respectively.

4.1. Local simple anomalous patterns determination

The goal of this stage is to recognize anomalous patterns from the local-scale time series data. The LOF (Local Outlier Factor) is then utilized here to verify the required anomalies from time series. Also, the set of features of the training set of time series are then discovered and defined from the data. The used LOF applies the complex density estimation model that is used to compare the density estimation for each

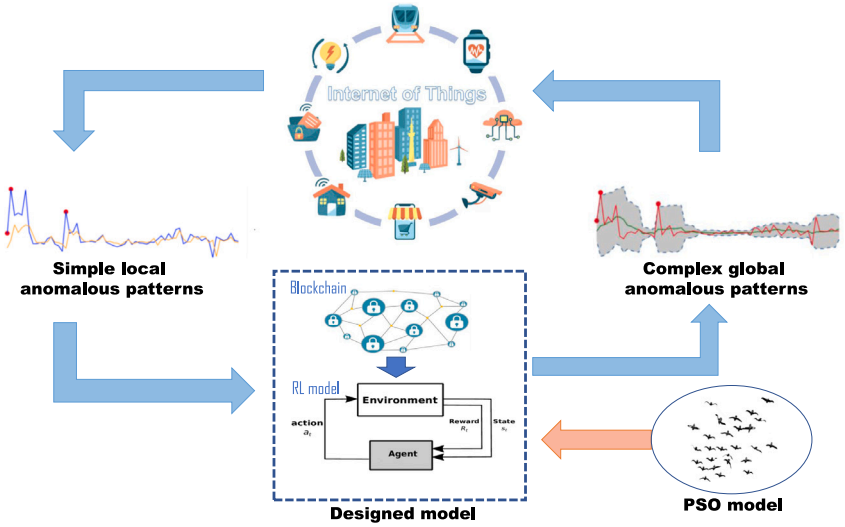

Fig. 1. The designed ITSA Framework.

extracted feature f with the consideration of the density estimation of the kNNs. The used density estimation in LOF can also be referred to as lrd (local reachability density), which can be calculated as:

$$\text{lrd}(f) = 1 \Big/ \frac{\sum_{p \in k\text{NN}(f)} \text{reach-dist}_k(f,p)}{|k\text{NN}(f)|} \tag{5}$$

in which the reach-dist (reachability-distance) with a k parameter is defined as:

$$\text{reach-dist}_k(f,p) = \max\{k\text{NN-}dist(p), dist(f,p)\} \tag{6}$$

Considering the distance measures of $dist$ and kNN-$dist(p)$, they are respectively the distance between the feature p and the k^{th} nearest neighbor of p. Through applying the DTW (Dynamic Time Warping) algorithm, we can calculate the distance between the features of time series. The DTW is capable to handle the transformation progress of local warping and shifting. Moreover, it can also be used to compare the time series regarding different lengths. Furthermore, the distance function of two time series features, e.g., f_i and f_j can be respectively defined as:

$$D(f_i, f_j) = \begin{cases} 0, \text{if } |f_i| - 1 = |f_j| - 1 = 0 \\ \infty, \text{if } |f_i| - 1 = 0, \text{or } |f_j| - 1 = 0 \\ f_{io} - f_{jo} + \sigma, \text{ otherwise} \end{cases} \tag{7}$$

in which, we can also obtain that:

$$\sigma = min \begin{cases} D(f_i / f_{io} f_j / f_{jo}) \\ D(f_i, f_j / f_{jo}) \\ D(f_i / f_{io}, f_j) \end{cases} \tag{8}$$

Note that f_{io}, f_{jo} are the current values of the time series f_i, and f_j. In general, this distance determines the best alignment between f_i, and f_j. Every element from f_i must be matched with the elements from f_j. The first element from f_i must be matched with the first element from f_j. The last element from f_i must be matched with the last element from f_j. The final score of the outlier can thus be defined and calculated as:

$$LOF(f) = \frac{1}{|k\text{NN}(f)|} \sum_{p \in k\text{NN}(f)} \frac{\text{lrd}(p)}{\text{lrd}(f)} \tag{9}$$

The local density estimation of lrd(p) is not considered to be compared with the other local density estimations except the density estimation of its k nearest neighbors. To obtain the global rankings of all points based on the outlierness, the relative (estimated) density is then compared to its k nearest neighbors by using Eq. (9). The relation to the local features of the dataset makes the process localization. Here, if the number of features is less than 1, it is defined as the outliers and will not be concerned for the further steps. A generic local anomalous pattern O_i of each site in the distributed environment is then discovered and output as the result of this progress.

4.2. Global complex anomalous patterns determination

Our aim in this phase is to learn the global complex anomalous patterns from the set of local generic anomalous patterns. Here, we will then use reinforcement learning by considering the approximate distribution over the reward function. The reward function is, of course, used as the evaluation criteria of the candidates of the complex anomalous patterns. A pattern is considered as an anomalous pattern if its density is no less than the minimum threshold value that is pre-defined by users' preference. We define a reward function with the given threshold value γ, which includes each candidate C_i in the set of the local anomalous patterns if its density is greater than γ. More formally, it is described in the following:

$$R(C_i|\Theta) = \begin{cases} C_i \subseteq O_i \\ Density(C_i|\Theta) \geq \gamma, \end{cases} \tag{10}$$

where the density $Density(C_i|\Theta)$ represent the density of the group candidate C_i, it is the product between the distances of the elements in C_i, and $\mathcal{L}(\Theta)$ is the function based on the parameter Θ. The purpose of $\mathcal{L}(\Theta)$ is to find the maximal likelihood of the complex candidates of the anomalous patterns, and it is defined as follows:

$$Density(C_i|\Theta) = \frac{\sum_{j=1}^{|C_i|} \sum_{l=1}^{|C_i|} D(f_j, f_l)}{|C_i| \times (|C_i| + 1)} \times \mathcal{L}(\Theta) \tag{11}$$

For each iteration of the training phase, a single reward function is then sampled from its approximate posterior. A generic policy of generation is then used in the iteration to produce the candidates of the complex patterns. After that, the policy is then gradually improved regarding the results of the sampled reward function. The candidates of the produced complex patterns from the target site are then used, and the reward function is then updated accordingly. This process is then executed repeatedly until the results are the converged.

To protect the shared data among the sites, Ethereum is then considered as the data storage service to establish a private blockchain that involves all sites in the developed model as the Ethereum nodes. All of the sites are used to verify data sharing transactions, and they are then compiled into blocks. As a prerequisite, all sites must be responsible for accepting and broadcasting data sharing transaction requests, in which

each site must apply to the certificate authority to receiving the public and private keys to become a legitimate terminal identity.

To guarantee the received data on the blockchain network is not forged and valid, it must first be encrypted with the private key, and then transfer to the certificate authority, which will validate that the data are from a legitimate source (or called site in the designed framework), and if it is true, the encrypted data, as well as the signature of certificate authority will be sent back to the given sites. Those messages will be also returned to the blockchain as storage requests by such sites.

4.3. Optimization

To ensure better privacy, we use an optimization solver based on the constraint satisfaction problem. The set of constraints of the whole data in the network are decomposed into several clusters. The clusters are explored to find the best configuration, which maximizes privacy. We propose two strategies for exploring the clusters of constraints:

• **Approximation-based strategy**. In this strategy, the clusters will be separately maintained without taking into account the shared data among sites. The local instantiation of the data is first carried out by utilizing the search procedure on each cluster. Here, the merging model (function) is then utilized to extract the global instantiation of the data. All local instantiation of data is then combined by the merging function. Such an approach returns a subset of all data from the whole set of constraints. This is because not all the shared data are considered in the search procedure of the designed model.

Proposition 4.1. *An upper (lower) bound of the number of the constraints satisfied by the approximation-based strategy, noted* $|\mathcal{A}|$, *is* $|C|$ $(|C| - (\sum_{i=1}^{k} S(G_i))$, *where* C *is the clusters of the constraints,* k *is the number of clusters,* $S(G_i)$ *is the number of conflicts constraints of the cluster* G_i*), and we note* $|C| - (\sum_{i=1}^{k} S(G_i)) \leq |\mathcal{A}| \leq |C|$.

Proof. In the worst case, the number of non-satisfied constraints of $\mathcal{A}$ is $|\{C_s, \exists(i,j) S(G_i) \cup S(G_j) \in C_s\}|$. This is maybe realized, where the shared variables appeared in the constraints of the clusters. In this case, $|\mathcal{A}| = |C|$ - $\sum_{i=1}^{k} S(G_i)$. In the case of the non-conflict, $S(G_i) \cup S(G_j) = \emptyset, \forall(i,j) \in k$, i.e $|\mathcal{A}| = |C|$.

From this proposition, one may argue that the quality of the approximation-based strategy highly depends on the number of shared data of all clusters. If the number of the shared data is minimized, the approximation-based strategy can satisfy all constraints. This will be fixed by choosing well the number of clusters.

• **Exact strategy**: This strategy takes the shared data and the clusters into consideration of the search procedure. This progress can be used to find the possible instantiation of data to satisfy all constraints. The search process is initially utilized on each cluster of constraints to derive the local instantiation of data. The local instantiation of data with the instantiation of shared data is then concatenated to derive the global instantiation of the whole constraints.

To better obtain the better performance regarding runtime, the PSO (particle swarm optimization) is then utilized in the designed model to find the optimal solution. The reason that we take the PSO in the optimization progress is that its capacities diversification and intensification; are two key points regarding the issue of constrain-satisfaction optimization.

PSO can perform global search over the entire search space with a higher convergence speed compared to the genetic algorithm, and the ant colony optimization. It enables automatic control of the search space and thereby improving the search effectiveness and efficiency at the same time. We then present the key elements of PSO for the constraint-satisfaction problem in the developed framework.

- Initialization of populations: First, the populations are randomly generated in the initial step. The populations are considered as the possible solutions among the sites.
- Updating procedure of particles: For each iteration, all particles are respectively updated based on their velocity and previous position.
- Fitness calculation: The evaluation procedure is then performed to verify the goodness of the solutions. Here, the evaluation function of the generated solutions is considered as the number of satisfied constraints. If a constraint does not violate the data transmitted among the sites, it then satisfies the constraint. The purpose of this step is to find the maximal value of the evaluation function.

To give more detailed of updating procedure in PSO, we first consider number of P particles in the developed framework, and a position vector is defined as $X_{ti}= (x_{i1}x_{i2}x_{i3} \dots x_{in})^T$, and the velocity vector is defined as $Vti = (v_{i1}v_{i2}v_{i3} \dots v_{in})^T$,. Note that the velocity of each i particle is at a t iteration. The updating procedure for a particle with its position and velocity is described as:

$$V_i^{t+1} = w \times V_i^t + c1 \times (p^t - X_i^t) + c2 \times (p^* - X_i^t) \tag{12}$$

and

$$X_i^{t+1} = X_i^t + V_i^{t+1}, \tag{13}$$

where $i = 1, 2, \dots, P$.

From Eq. (12), we can observe that two constant factors c_1 and c_2 are used for the next movement of a particle in an iteration. Note that p^t is the defined position for the best particle at iteration t, and p^* is defined as the position for the best particle since the first iteration. Besides, Eq. (13) is a formula to update the position of a particle, w is a parameter with a positive and constant value. Note that this parameter is a key value to balance the global and local search in which global search is defined as the exploration (while the value is set higher) and local search is considered as exploitation (while the value is set higher).

5. Experimental evaluation

In the experimental section, we then evaluate the performance of the proposed ITSA framework and discuss the various components of the system. Specifically, the ability in identifying the local simple, and global complex anomalous patterns are analyzed using well-known datasets, including (i) CASAS (Center of Advanced Studied in Adaptive Systems) datasets,[1] and OPSD (Open Power System Data platform.[2] The scalability is then evaluated to see the performance of the designed ITSA framework compared to the state-of-the-art approaches in industrial IoT environments. Experiments are then executed on a personal computer (PC) with a 64-bit quad-core Intel Xeon E5520@2.27 GHz processor with 16 GB main memory, running on Microsoft Windows 10 OS platform. The Nvidia Tesla C2075 with 448 CUDA cores GPU (14 multiprocessors with 32 cores@1.15 GHz) is also used in the experiments. The GPU has 2.8 GB for global memory, 49.15 kB for the shared memory, and a warp size is 32. In the experiments, the GPU blocks are then used to simulate the distributed sites of the developed framework, and each site is then allocated to a GPU block. Note that the threads of a site shared the local memory, and the communication of sites is based on the global and constant memories of the GPU host.

In the designed model, the main issue for anomaly detection is the evaluation progress. This is essential for the new domains or applications focused on finding the local generic anomalous patterns and global complex anomalous patterns while the ground truth is generally uncertain or unknown. The model [39] is then utilized in the experiments to inject the synthetic complex anomalous patterns for time series data. The detailed information is then stated as follows:

[1] http://casas.wsu.edu/datasets/.
[2] https://data.open-power-system-data.org/.

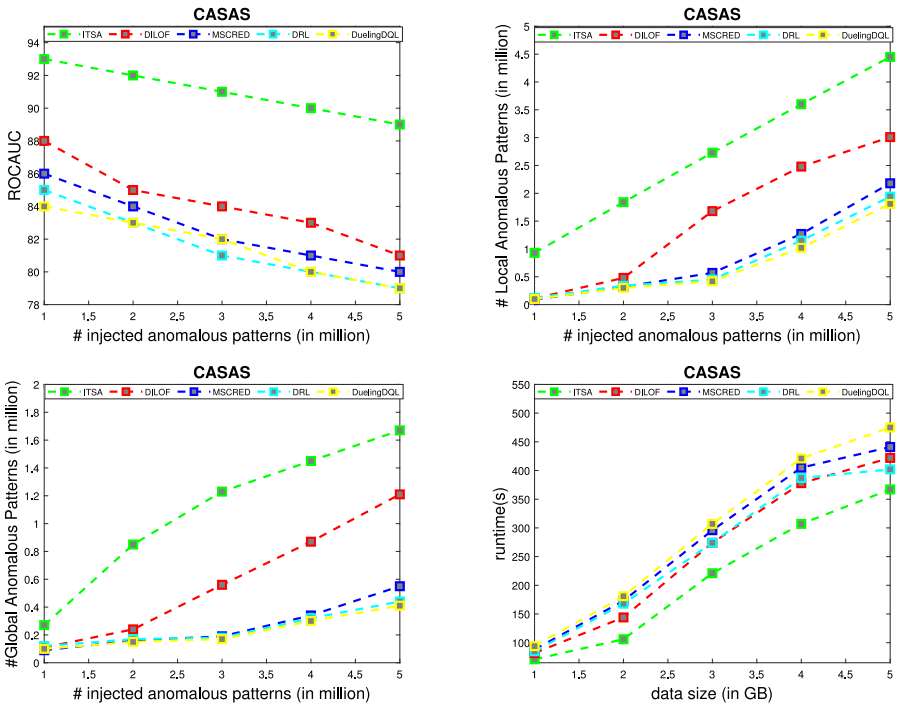

Fig. 2. ITSA vs. the state-of-the-art anomaly detection solutions using CASAS data.

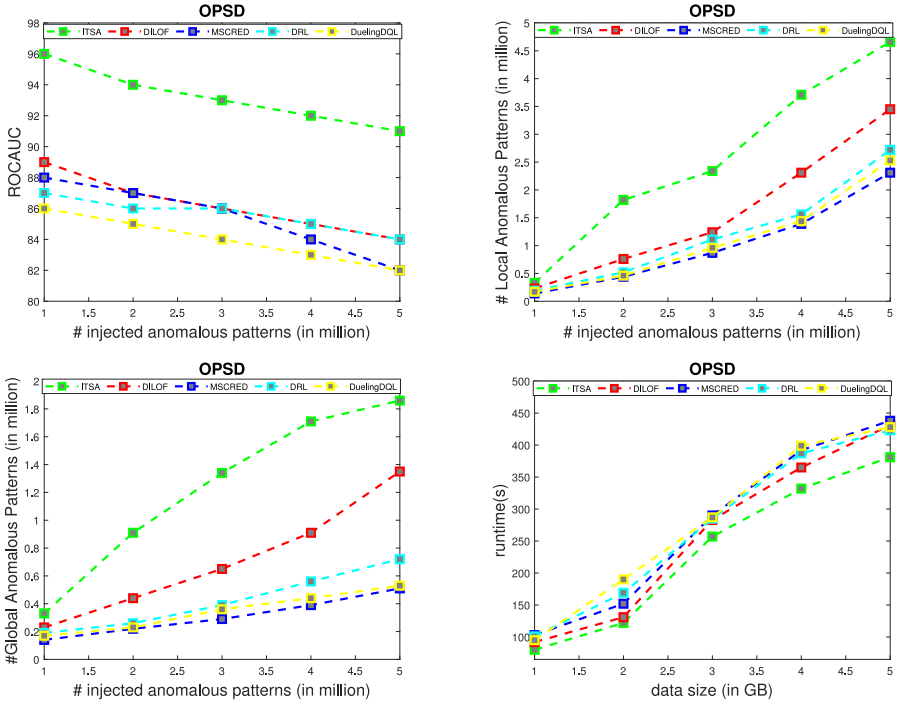

Fig. 3. ITSA vs. the state-of-the-art anomaly detection solutions using OPSD data.

- **Injecting local simple anomalous patterns**: local simple anomalous patterns are produced by inserting the noise information repeatedly by a probability $p \sim \mathcal{U}(0.8, 1.0)$. A parameter μ is defined as a threshold in the designed system.
- **Injecting global complex anomalous patterns**: For the global complex anomalous patterns, again, the noise information is then repeatably inserted by a probability $p \sim \mathcal{U}(0.0, 1.0)$. A parameter μ is defined as a threshold in the designed system.

For whether local simple/global complex anomalous patterns insertion, each point p_{il} in time series TS_i is the updated as:

$$p_{il} = \begin{cases} p_{il} + n \sim \mathcal{N}(0,1) & \text{if } p \geq \mu \\ p_{il} & \text{otherwise.} \end{cases} \tag{14}$$

ROCAUC is then considered as one of the evaluation criteria in the experiments, as well as the number of detected outliers since it is the common criteria to see the performance of the anomalous detection models. The state-of-the-art models DILOF (Density summarizing

Incremental Local Outlier Factor) [28], MSCRED (Multi-Scale Convolutional Recurrent Encoder-Decode) [30], DRL (Deep Reinforcement Learning) [19], and DuelingDQL (Dueling Deep Q-Learning) [31] are then compared with the developed ITSA framework, and the results are indicated in Figs. 2 and 3.

This part of the experiment consists of comparing the developed ITSA model to the state-of-the-art baseline anomaly detection solutions. As the results shown in Figs. 2 and 3, many various types of experiments have been conducted by varying the amount of injected anomalous patterns from 1 million to 5 million. The findings show that ITSA outperforms the other two baseline solutions in terms of ROCAUC, as well as the amount of local and global anomalous patterns for the CASAS and the OPSD dataset. Additionally, the distance between ITSA and other solutions is expanded with the number of anomalous patterns added during the injection. As a part of this, the developed ITSA has an opportunity to recognize anomalous patterns in heterogeneous sources as in the case of energy systems. This is due to the productive combination of the local outlier factor and the advantages of reinforcement learning in tackling more complex tasks rather than the state-of-the-art baseline approaches.

The second aspect of the experiments is to measure the runtime performance of the designed ITSA against the state-of-the-art baseline approaches. As the results shown in Figs. 2 and 3, many various types of experiments have been conducted by varying the size of the datasets from 1 GB to 5 GB. The findings have shown that the developed ITSA is better than the state-of-the-art baseline approaches for both CASAS and OPSD databases. For large-scale databases, the difference between the designed ITSA and the state-of-the-art baseline approaches is huge. In this situation, the ITSA can examine and spot anomalous patterns in heterogeneous sources regardless of their size especially in the case of the energy industry. Thanks to the advantages of learning progress in the designed hybrid ITAS model, the local generic anomalous patterns can be easily examined by the local outlier factor, and the global complex anomalous patterns can be easily discovered. The general approach is that we use this two-stage procedure to minimize the size of the search space for exploring the possible solutions. Then, we can only use the generic local anomalous patterns to efficiently discover the global complex anomalous patterns.

6. Conclusion

In this study, we develop a new ITSA framework based on reinforcement blockchain learning for identifying complex anomalous patterns from distributed and heterogeneous time series data. The local outlier factor is first adopted to detect the local simple anomalous patterns in each site. The discovered local generic anomalous patterns are then easily merged by the reinforcement blockchain learning to refer to the global complex anomalous patterns efficiently. Experiments have been performed on industrial IoT environments, particularly in energy applications. From the output results, we can observe that the designed ITAS outperforms the state-of-the-art baseline approaches in terms of outlier detection and runtime performance. Thus, the developed ITAS can secure the learning process for generating the global complex anomalous patterns.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J.P.A. Leon, T. Begin, A. Busson, J. Luis, A fair and distributed congestion control mechanism for smart grid neighborhood area networks, Ad Hoc Netw. 104 (2020) 102169.

[2] H.E. Erdem, V.C. Gungor, On the lifetime analysis of energy harvesting sensor nodes in smart grid environments, Ad Hoc Netw. 75 (2018) 98–105.

[3] J.C.W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, M. Aloqaily, Privacy preserving multi-objective sanitization model in 6g iot environments, IEEE Internet Things J. 8 (7) (2021) 5340–5349.

[4] D. Djenouri, R. Laidi, Y. Djenouri, I. Balasingham, Machine learning for smart building applications: review and taxonomy, ACM Comput. Surv. 52 (2) (2019) 1–36.

[5] L. Zhu, C. Lu, Y. Luo, Time series data-driven batch assessment of power system short-term voltage security, IEEE Trans. Ind. Inf. 16 (12) (2021) 7306–7317.

[6] H. Jahangir, H. Tayarani, S.S. Gougheri, M.A. Golkar, A. Ahmadian, A. Elkamel, Deep learning-based forecasting approach in smart grids with micro-clustering and bi-directional lstm network, IEEE Trans. Ind. Electron. early access (2020).

[7] O.B. Sezer, M.U. Gudelek, A.M. Ozbayoglu, Financial time series forecasting with deep learning: A systematic literature review: 2005–2019, Appl. Soft Comput. 90 (2020) 106181.

[8] F. Wang, M. Li, Y. Mei, W. Li, Time series data mining: A case study with big data analytics approach, IEEE Access 8 (2020) 14322–14328.

[9] Y. Djenouri, G. Srivastava, J.C.W. Lin, Fast and accurate convolution neural network for detecting manufacturing data, IEEE Trans. Ind. Inf. 17 (4) (2020) 2947–2955.

[10] Y. Djenouri, A. Zimek, M. Chiarandini, Outlier detection in urban traffic flow distributions, in: IEEE International Conference on Data Mining, 2018, pp. 935–940.

[11] N. Javaid, N. Jan, M.U. Javed, An adaptive synthesis to handle imbalanced big data with deep siamese network for electricity theft detection in smart grids, J. Parallel Distrib. Comput. 153 (2021) 44–52.

[12] N. Nesa, T. Ghosh, I. Banerjee, Non-parametric sequence-based learning approach for outlier detection in iot, Future Gener. Comput. Syst. 82 (2018) 412–421.

[13] L. Feremans, V. Vercruyssen, B. Cule, W. Meert, B. Goethals, Pattern-based anomaly detection in mixed-type time series, in: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, 2019, pp. 240–256.

[14] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. 107 (2020) 841–853.

[15] Y. Xiao, N. Zhang, W. Lou, Y.T. Hou, A survey of distributed consensus protocols for blockchain networks, IEEE Commun. Surv. Tutor. 22 (2020) 1432–1465.

[16] M. Liu, F.R. Yu, Y. Teng, V.C. Leung, M. Song, Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach, IEEE Trans. Ind. Inf. 15 (6) (2019) 3559–3570.

[17] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, W. Luo, Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive, IEEE Trans. Dependable Secure Comput. 14 (8) (2019) 1–18.

[18] J.C.W. Lin, Y. Shao, Y. Djenouri, U. Yun, Asrnn: a recurrent neural network with an attention model for sequence labeling, Knowl.-Based Syst. 212 (2021) 106548.

[19] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5g beyond, IEEE Netw. 33 (3) (2019) 10–17.

[20] M. Tariq, M. Adnan, G. Srivastava, H.V. Poor, Instability detection and prevention in smart grids under asymmetric faults, IEEE Trans. Ind. Appl. 56 (4) (2020) 4510–4520.

[21] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, S. Ricci, A privacy-enhancing framework for internet of things services, in: International Conference on Network and System Security, Springer, 2019, pp. 77–97.

[22] K. Singh, S. Upadhyaya, Outlier detection: applications and techniques, Int. J. Comput. Sci. Issues 9 (1) (2012) 307–323.

[23] X. Tao, Y. Peng, F. Zhao, C. Yang, B. Qiang, Y. Wang, Z. Xiong, Gated recurrent unit-based parallel network traffic anomaly detection using subagging ensembles, Ad Hoc Netw. 116 (2021) 102465.

[24] Y. Yu, Y. Zhu, S. Li, D. Wan, Time series outlier detection based on sliding window prediction, Math. Probl. Eng. 2014 (2014) 879736.

[25] K. Yamanishi, J.i. Takeuchi, A unifying framework for detecting outliers and change points from non-stationary time series data, in: ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002, pp. 676–681.

[26] K. Yamanishi, J.I. Takeuchi, G. Williams, P. Milne, On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms, Data Min. Knowl. Discov. 8 (3) (2004) 275–300.

[27] C. Xie, Z. Chen, X. Yu, Sequence outlier detection based on chaos theory and its application on stock market, in: International Conference on Fuzzy Systems and Knowledge Discovery, 2006, pp. 1221–1228.

[28] G.S. Na, D. Kim, H. Yu, Dilof: Effective and memory efficient local outlier detection in data streams, in: ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018, pp. 1993–2002.

[29] T. Kieu, B. Yang, C. Guo, C.S. Jensen, Outlier detection for time series with recurrent autoencoder ensembles, in: The International Joint Conference on Artificial Intelligence, 2019, pp. 2725–2732.
[30] C. Zhang, D. Song, Y. Chen, X. Feng, C. Lumezanu, W. Cheng, J. Ni, B. Zong, H. Chen, N.V. Chawla, A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data, in: AAAI Conference on Artificial Intelligence, 33, 2019, pp. 1409–1416.
[31] C. Qiu, F.R. Yu, H. Yao, C. Jiang, F. Xu, C. Zhao, Blockchain-based software-defined industrial internet of things: A dueling deep q-learning approach, IEEE Internet Things J. 6 (3) (2018) 4627–4639.
[32] C.H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning, IEEE Trans. Ind. Inf. 15 (6) (2018) 3516–3526.
[33] Y. Dai, D. Xu, K. Zhang, S. Maharjan, Y. Zhang, Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks, IEEE Trans. Veh. Technol. 69 (4) (2020) 4312–4324.
[34] M. Kadadha, H. Otrok, A blockchain-enabled relay selection for qos-olsr in urban vanet: A stackelberg game model, Ad Hoc Netw. (2021) 102502.
[35] H. Chai, S. Leng, Y. Chen, K. Zhang, A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles, IEEE Trans. Intell. Transp. Syst. (2020) 1–12.
[36] Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles, IEEE Trans. Veh. Technol. 69 (4) (2020) 4298–4311.
[37] Y. Qu, L. Gao, T.H. Luan, Y. Xiang, S. Yu, B. Li, G. Zheng, Decentralized privacy using blockchain-enabled federated learning in fog computing, IEEE Internet Things J. 7 (6) (2020) 5466–5480.
[38] J. Luo, Q. Chen, F.R. Yu, L. Tang, Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning, IEEE Internet Things J. 7 (6) (2020) 5466–5480.
[39] J. Zhang, M. Zulkernine, A. Haque, Random-forests-based network intrusion detection systems, IEEE Trans. Syst. Man Cybern. C (Appl. Rev.) 38 (5) (2008) 649–659.

Asma Belhadi obtained the Ph.D. in Computer Engineering from the University of Science and Technology USTHB Algiers, Algeria, in 2016. She is a postdoctoral researcher at Kristiania University College in Oslo, Norway. She is working on topics related to artificial intelligence and data mining, with focus on logic programming. Dr. Belhadi has published over 25 refereed research articles in the areas of artificial intelligence, and smart city applications.

Youcef Djenouri obtained the Ph.D. in Computer Engineering from the University of Science and Technology USTHB, Algiers, Algeria, in 2014. He is currently a research scientist at SINTEF Digital in Oslo, Norway. He is working on topics related to artificial intelligence and data mining, with focus on association rules mining, frequent itemsets mining, parallel computing, swarm and evolutionary algorithms and pruning association rules. Dr. Djenouri has published more than 70 refereed research papers, in the areas of data mining, parallel computing and artificial intelligence.

Gautam Srivastava was awarded his B.Sc. degree from Briar Cliff University in the U.S.A. in the year 2004, followed by his M.Sc. and Ph.D. degrees from the University of Victoria in Victoria, British Columbia, Canada in the years 2006 and 2012, respectively. From there in the year 2014, he joined a tenure-track position at Brandon University in Brandon, Manitoba, Canada, where he currently is active in various professional and scholarly activities. He was promoted to the rank of Associate Professor in January 2018. Dr. G, as he is popularly known, is active in research in the field of Cryptography, Data Mining, Security and Privacy, and Blockchain Technology. In his 5 years as a research academic, he has published a total of 70 papers in high-impact conferences in many countries and in high status journals (SCI, SCIE) and has also delivered invited guest lectures on Big Data, Cloud Computing, Internet of Things, and Cryptography at many universities worldwide. He is an Editor of several SCI/SCIE journals. He is an IEEE Senior Member and also an Associate editor of the world renowned IEEE Access journal.

Alireza Jolfaei received the Ph.D. degree in Applied Cryptography from Griffith University, Gold Coast, Australia. He is the Program Leader of Master of IT in Cyber Security at Macquarie University, Sydney, Australia. His main research interests are in Cyber and Cyber–Physical Systems Security. He has participated in several projects involving different aspects of Cyber Security. On these topics he has published over 100 papers appeared in journals, conference proceedings, and books. Before Macquarie University, he worked as a Lecturer at Federation University Australia and as an Assistant Professor of Computer Science at Temple University, Philadelphia, PA, USA. He has received multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He received the prestigious IEEE Australian council award for his research paper published in the IEEE Transactions on Information Forensics and Security. He served as the Chairman of the Computational Intelligence Society in the IEEE Victoria Section and also as the Chairman of Professional and Career Activities for the IEEE Queensland Section. He has served as the associate editor of IEEE journals and transactions, including the IEEE IoT Journal, IEEE Sensors Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industry Applications, IEEE Transactions on Intelligent Transportation Systems, and IEEE Transactions on Emerging Topics in Computational Intelligence. He has served as a program co-Chair, a track Chair, a session Chair, and a Technical Program Committee member, for major conferences in Cyber Security, including IEEE TrustCom. He is the General Chair of the 6th IEEE International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2020) in Fiji. He is a Distinguished Speaker of the Association for Computing Machinery (ACM) on the topic of Cyber Security and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

Jerry Chun-Wei Lin received his Ph.D. from the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan in 2010. He is currently a full Professor with the Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway. He has published more than 400 research articles in refereed journals (IEEE TKDE, IEEE TCYB, IEEE TII, IEEE TITS, IEEE TIAS, IEEE TETCI, IEEE SysJ, IEEE SensJ, IEEE IOTJ, ACM TKDD, ACM TDS, ACM TMIS, ACM TOIT) and international conferences (IEEE ICDE, IEEE ICDM, PKDD, PAKDD), as well as 11 edited books and 33 patents (held and filed, 3 US patents). His research interests include data mining, soft computing, artificial intelligence and machine learning, and privacy preserving and security technologies. He is the Editor-in-Chief of the International Journal of Data Science and Pattern Recognition, the Guest Editor/Associate Editor of IEEE TFS, IEEE TII, ACM TMIS, ACM TOIT, Connection Science, IEEE Access, JIT, Applied Sciences, Sensors, PlosOne, IDA, and IJIMAI. He has recognized as the most cited Chinese Researcher respectively in 2018 and 2019 by Scopus. He is the Fellow of IET (FIET), senior member for both IEEE and ACM.