AF Relaying Secrecy Performance Prediction for 6G Mobile Communication Networks in Industry 5.0

Lingwei Xu, *Member, IEEE*, Xinpeng Zhou, *Student Member, IEEE*, Ye Tao, *Member, IEEE*, Xu Yu, *Member, IEEE*, Miao Yu, and Fazlullah Khan, *Senior Member, IEEE*

***Abstract*—Industry 5.0 has developed in full swing, and accelerated the process of the sixth-generation (6G) mobile communication. Physical layer security is important for complex 6G mobile communication networks. To process active complex events in 6G mobile cooperative networks, predicting secrecy performance in time is essential for the mobile communication quality evaluation. Using amplify-and-forward (AF) relaying, we propose a transmit antenna selection (TAS) based secrecy scheme in this article. To analyze the security of 6G mobile cooperative networks, signal-to-noise ratio of the end-to-end link is used to derive the novel expressions for secrecy outage probability (SOP). The theoretical results are confirmed by simulation results. Then, we use SOP as the important merit to evaluate the secrecy performance, and set up the dataset. To achieve secrecy performance prediction, a convolutional neural network (CNN) based SOP prediction algorithm is proposed. The designed CNN model has five convolution layers, which all use the same convolution in the padding and do not change data size. For this improved CNN structure, we adopt the idea of SqueezeNet, which belongs to the lightweight CNN. The improved CNN model can greatly reduce the parameters and network complexity on the premise of ensuring the prediction accuracy. We also examine the following state-of-the-art techniques, first, Elman, second, InceptionNet, third, deep neural network (DNN), and fourth, support vector machine methods. The proposed CNN algorithm can achieve better SOP prediction results than other existing methods. In particular, compared with DNN method, the prediction accuracy is increased by 66.7%.**

***Index Terms*—Improved convolutional neural network (CNN), physical layer security, secrecy performance prediction, sixth-generation (6G) mobile communication.**

Manuscript received May 29, 2021; revised August 5, 2021 and September 23, 2021; accepted October 6, 2021. Date of publication October 15, 2021; date of current version May 6, 2022. This work was supported in part by Shandong Province Natural Science Foundation under Grant ZR2020QF003, in part by the National Natural Science Foundation of China under Grant 6217072142, in part by the Opening Foundation of Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education under Grant K93-9-2021-09, in part by the Open Research Fund of Anhui Engineering Technology Research Center of Automotive New Technique under Grant QCKJ202101, in part by the Shandong Province Colleges and Universities Young Talents Initiation Program under Grant 2019KJN047, and in part by the Doctoral Found of QUST under Grant 1203043003480. Paper no. TII-21-2233. *(Corresponding author: Xu Yu.)*

Lingwei Xu, Xinpeng Zhou, Ye Tao, and Xu Yu are with the Department of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China, with the Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, Nanjing 211189, China, and also with the Anhui Engineering Technology Research Center of Automotive New Technique, Anhui Polytechnic University, Wuhu 241000, China (e-mail: xulw@qust.edu.cn; xpzhou17853321957@163.com; ye.tao@qust.edu.cn; yuxu0532@qust.edu.cn).

Miao Yu is with the College of Textiles and Clothing, Qingdao University, Qingdao 266071, China (e-mail: yumiao@qdu.edu.cn).

Fazlullah Khan is with the Department of Computing Science, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa 23200, Pakistan (e-mail: fazlullah@ieee.org).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3120511.

Digital Object Identifier 10.1109/TII.2021.3120511

I. Introduction

IN RECENT years, industry 5.0 has developed in full swing, and accelerated the process of human intelligent society. Industry 5.0 focuses a sustainable, human-centric, and resilient industry. In the era of information industry 5.0, via massive deployment of sensors, antennas, and actuators, the sixth-generation (6G) mobile communication is a key technology to achieve digital and intelligent communication [1], [2].

A. Survey of Current Literature

6G is widely used in the information industry 5.0. The combination of transportation and 6G will change the traditional passenger transport and bring different innovation experience; 6G+ smart medicine can support remote high-definition consultation and high-speed medical image transmission; 6G+ smart port can reduce security risk and labor cost. Sun *et al.* [3] employed the machine learning methods to protect privacy in 6G. Emerging 6G communication industries were used by Mao *et al.* [4] to optimize the security of Internet of Things systems.

The 6G communication faces the complex environments, and the secure communication is facing many challenges [5]. For packet transmission, Narsani *et al.* [6] proposed cooperative communication protocol. Atat *et al.* [7] developed a physical layer security (PLS) scheme under different metrics. Vuppala *et al.* [8] developed a mathematical framework to analyze the different metrics of the hybrid mmWave network. Hu *et al.* [9] used a cooperative jammer to achieve the secure downlink transmission. Taking the impact of antenna correlation into consideration, Sun *et al.* [10] analyzed the positive secrecy

probability over Nakagami-m model. Salem *et al.* [11] considered cooperative power line communication networks over log-normal model and analyzed the PLS performance.

To ensure secure communication, multiple-antenna technique and cooperative communication are effective ways. Salem *et al.* [12] analyzed the secrecy capacity of multiantenna amplify-and-forward (AF) relay network. For various multiple-antenna techniques, Chen *et al.* [13] investigated the secrecy performance. To enhance its secrecy performance, Feng *et al.* [14] proposed a decode-amplify-forward relaying scheme. Yao *et al.* [15] employed Stackelberg game approach to enhance secrecy performance.

Rayleigh and Nakagami models are focus of PLS research. In reality, mobile communication faces multiple scattering environment [16]. Hence, the N-Nakagami model has gained widespread applications in practical mobile scenarios [17]. The communication quality of mobile cooperative networks was investigated in [18]. However, due to the complex communication model, the derived PLS mathematical expressions are more and more complicated. The traditional mathematical methods analyze secrecy performance through the complex mathematical expressions, but the computational complexity is very high. Therefore, the traditional mathematical methods are difficult to realize the real-time evaluation of secrecy performance.

Information industry 5.0 faces complex and changeable application scenarios [19]. It needs to quickly evaluate the security situation to achieve the resource allocation for different application scenarios. Therefore, predicting secrecy performance in time is essential for the mobile communication quality evaluation. Convolutional neural network (CNN) model is very popular in engineering applications [20]. Chung *et al.* [21] employed the genetic algorithm to optimize the CNN model for stock market prediction. Ding *et al.* [22] proposed a CNN model to recognize video-based face. Based on CNN, a novel detection framework was proposed by Qiu *et al.* [23] for complex power quality disturbances. Therefore, the improved CNN model is very suitable for secrecy performance prediction in complex environments.

B. Contribution

Secrecy performance prediction is a very difficult task in the complex environments. CNN provides a new way for secrecy performance prediction. However, the related research work is very rare. Motivated by the abovementioned discussion, we investigate the secrecy outage probability (SOP) prediction of 6G mobile cooperative networks. We summary the main contributions as follows.

1) In order to improve SOP performance, a transmit antenna selection (TAS) based AF scheme is proposed. TAS can reduce the processing complexity of 6G mobile cooperative networks. Then, we use SOP to evaluate the secrecy performance, and derive the novel mathematical expressions, which are different from the existing works. The simulation results are compared with the derived theoretical results. Different fading parameters are employed to examine the effect on the SOP performance.

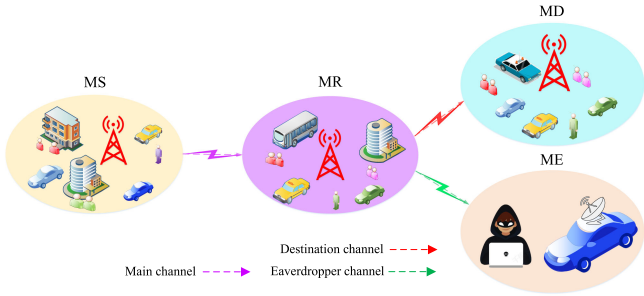

Fig. 1. Mobile cooperative model.

2) In order to better extract the characteristics of mobile signals, we propose an improved CNN model. The designed CNN model has five convolution layers, which all use the same convolution in the padding and do not change data size. For this improved CNN structure, we adopt the idea of SqueezeNet, which belongs to the lightweight CNN. It consists of many fire modules, which have a squeeze layer and a expand layer. In this way, we can greatly reduce the structure parameters and network complexity on the premise of ensuring the prediction accuracy.
3) A SOP prediction algorithm employing the improved CNN is proposed. Through mathematical derivation, we select five important influence parameters to set up a dataset. Through data training, we obtain the best CNN prediction model. The obtained CNN prediction model is employed to predict the SOP performance, and can reduce the computational complexity of the traditional approach employing complex mathematical expressions.
4) To verify the prediction effect, we test InceptionNet, Elman, and deep neural network (DNN) methods. Compared with InceptionNet, Elman, and DNN methods, the proposed algorithm achieves better prediction results. Compared with DNN method, the prediction accuracy is increased by 66.7%.

C. Article Organisation

The rest of this article is organized as follows. In Section II, we first give the mobile cooperative model. The SOP performance is investigated in Section III. A SOP prediction algorithm is proposed in Section IV. In Section V, we discuss the prediction results. Finally, Section VI concludes this article.

II. Mobile Cooperative Model

We consider a mobile cooperative model in Fig. 1. Mobile source (MS) can communicate with a mobile relay (MR), and mobile destination (MD). The mobile eavesdropper (ME) can eavesdrop on their communications. $W_{\{\mathrm{SR,RD,RE}\}}$ are the relative gains of different channels. The channel coefficients $h_{\{\mathrm{SR,RD,RE}\}}$ follow 2-Rayleigh distribution [18].

K is employed to allocate the total transmit power E. First, MS_i transmits the signal x. MR receives the signal r_{SR} as [24]

$$r_{\mathrm{SR}i} = \sqrt{W_{\mathrm{SR}}KE}h_{\mathrm{SR}i}x + n_{\mathrm{SR}i} \tag{1}$$

where $n_{\mathrm{SR}i}$ has the mean and variance as 0 and $N_0/2$.

Then, MR uses AF cooperation protocol. The signals received by MD and ME are $r_{\mathrm{R}ki}$, $k \in \{\mathrm{D}, \mathrm{E}\}$

$$r_{\mathrm{R}ki} = \sqrt{c_{ki}E}h_{\mathrm{SR}i}h_{\mathrm{R}ki}x + n_{\mathrm{R}ki} \tag{2}$$

where c_{ki} is given as

$$\begin{aligned} c_k &= \frac{K(1-K)V_{\mathrm{SR}}V_{\mathrm{R}k}E/N_0}{1+KV_{\mathrm{SR}}E/N_0+(1-K)W_{\mathrm{R}k}\left|h_{\mathrm{R}ki}\right|^2E/N_0} \\ &= \frac{K(1-K)V_{\mathrm{SR}}V_{\mathrm{R}k}\bar{\gamma}}{1+KV_{\mathrm{SR}}\bar{\gamma}+(1-K)V_{\mathrm{R}k}\left|h_{\mathrm{R}ki}\right|^2\bar{\gamma}}. \end{aligned} \tag{3}$$

The received SNR $\gamma_{\mathrm{SR}ki}$ is given as

$$\gamma_{\mathrm{SR}ki} = \frac{\gamma_{\mathrm{SR}i}\gamma_{\mathrm{R}ki}}{1+\overline{\gamma_{\mathrm{SR}i}}+\gamma_{\mathrm{R}ki}} \tag{4}$$

where

$$\gamma_{\mathrm{SR}i} = W_{\mathrm{SR}}K|h_{\mathrm{SR}}|^2\bar{\gamma} \tag{5}$$

$$\gamma_{\mathrm{R}ki} = (1-K)W_{\mathrm{R}k}|h_{\mathrm{R}ki}|^2\bar{\gamma} \tag{6}$$

$$\overline{\gamma_{\mathrm{SR}i}} = W_{\mathrm{SR}}K\bar{\gamma}. \tag{7}$$

With the help of [25], we approximate $\gamma_{\mathrm{SR}ki}$ as

$$\gamma_{\mathrm{SRA}ki} = \frac{\gamma_{\mathrm{SR}i}\gamma_{\mathrm{R}ki}}{1+\overline{\gamma_{\mathrm{SR}i}}+\overline{\gamma_{\mathrm{R}ki}}} \tag{8}$$

$$\overline{\gamma_{\mathrm{R}ki}} = (1-K)W_{\mathrm{R}ki}\bar{\gamma}. \tag{9}$$

We first obtain the PDF of $\gamma_{\mathrm{SRA}ki}$ as follows:

$$f_{\gamma_{\mathrm{SRA}ki}}(r) = \frac{1}{r}G_{0,4}^{4,0}\left[\frac{r(1+\overline{\gamma_{\mathrm{SR}i}}+\overline{\gamma_{\mathrm{R}ki}})}{\overline{\gamma_{\mathrm{SR}i}}\times\overline{\gamma_{\mathrm{R}ki}}}\Big|_{1,1,1,1}^{-}\right]. \tag{10}$$

Then, we obtain the CDF by integrating the (10)

$$F_{\gamma_{\mathrm{SRA}ki}}(r) = G_{1,5}^{4,1}\left[\frac{r(1+\overline{\gamma_{\mathrm{SR}i}}+\overline{\gamma_{\mathrm{R}ki}})}{\overline{\gamma_{\mathrm{SR}i}}\times\overline{\gamma_{\mathrm{R}ki}}}\Big|_{1,1,1,1,0}^{1}\right]. \tag{11}$$

The instantaneous secrecy capacity is given as [26]

$$C_i = \max\left\{\ln(1+\gamma_{\mathrm{SRAD}i})-\ln(1+\gamma_{\mathrm{SRAE}i}),0\right\}. \tag{12}$$

To reduce computational complexity, we use the TAS scheme to select w as

$$w = \max_{1\le i\le N_{\mathrm{t}}}(C_i). \tag{13}$$

III. SOP Analysis

The SOP is given as

$$\begin{aligned} F &= \Pr\left(\max_{1\le i\le N_{\mathrm{t}}}(C_i) < \gamma_{\mathrm{th}}\right) \\ &= \left(\max\{\ln(1+\gamma_{\mathrm{SRSD}})-\ln(1+\gamma_{\mathrm{SRSE}}),0\} < \gamma_{\mathrm{th}}\right)^{N_{\mathrm{t}}} \\ &= (Q_1)^{N_{\mathrm{t}}} \end{aligned} \tag{14}$$

where γ_{th} is a secrecy capacity threshold.

Q_1 is given as

$$\begin{aligned} Q_1 &= \Pr\left(C_{\mathrm{S}}(\gamma_{\mathrm{SRAD}},\gamma_{\mathrm{SRAE}}) < \gamma_{\mathrm{th}}\right) \\ &= \Pr\left(\gamma_{\mathrm{SRAD}} < \beta\gamma_{\mathrm{SRAE}}+\beta-1\right) \\ &= \int_0^{\infty} F_{\mathrm{SRAD}}(\beta\gamma_{\mathrm{SRAE}}+\beta-1)f_{\mathrm{SRAE}}(\gamma_{\mathrm{SRAE}})d\gamma_{\mathrm{SRAE}} \end{aligned} \tag{15}$$

$$\beta = \exp(\gamma_{\mathrm{th}}). \tag{16}$$

Equation (15) is hard to obtain a closed expression. From another angle, we obtain a lower bound on the Q_1 as

$$\begin{aligned} Q_1 &= \Pr\left(\gamma_{\mathrm{SRAD}} < \beta\gamma_{\mathrm{SRAE}}\right) \\ &= \int_0^{\infty} F_{\mathrm{SRAD}}(\beta\gamma_{\mathrm{SRAE}})f_{\mathrm{SRAE}}(\gamma_{\mathrm{SRAE}})d\gamma_{\mathrm{SRAE}} \\ &= \int_0^{\infty}\frac{1}{\gamma_{\mathrm{SRAE}}}G_{1,5}^{4,1}\left[\frac{\beta(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RD}}})}{\overline{\gamma_{\mathrm{SR}}}\times\overline{\gamma_{\mathrm{RD}}}}\gamma_{\mathrm{SRAE}}\Big|_{1,1,1,1,0}^{1}\right] \\ &\quad\times G_{0,4}^{4,0}\left[\frac{\beta(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RE}}})}{\overline{\gamma_{\mathrm{SR}}}\times\overline{\gamma_{\mathrm{RE}}}}\gamma_{\mathrm{SRAE}}\Big|_{1,1,1,1}^{-}\right]d\gamma_{\mathrm{SRAE}} \\ &= G_{5,5}^{4,5}\left[\frac{\beta\overline{\gamma_{\mathrm{RE}}}(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RD}}})}{\overline{\gamma_{\mathrm{RD}}}(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RE}}})}\Big|_{1,1,1,1,0}^{1,0,0,0,0}\right]. \end{aligned} \tag{17}$$

We obtain the lower bound on SOP as

$$\begin{aligned} F_{\mathrm{L}} &= (Q_{\mathrm{L}})^{N_{\mathrm{t}}} \\ &= \left(G_{5,5}^{4,5}\left[\frac{\beta\overline{\gamma_{\mathrm{RE}}}(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RD}}})}{\overline{\gamma_{\mathrm{RD}}}(1+\overline{\gamma_{\mathrm{SR}}}+\overline{\gamma_{\mathrm{RE}}})}\Big|_{1,1,1,1,0}^{1,0,0,0,0}\right]\right)^{N_{\mathrm{t}}}. \end{aligned} \tag{18}$$

IV. SOP Prediction Based on CNN Model

We design an improved CNN model, and propose an SOP prediction algorithm in Fig. 2. For this improved CNN structure, we adopt the idea of SqueezeNet, which belongs to the lightweight CNN. In this way, we can greatly reduce the parameters and network complexity. At the same time, we can also ensure the prediction accuracy.

A. Input and Output Selection

From the derived SOP expressions, we select five indicators W_{SR}, W_{RD}, W_{RE}, γ_{th}, $\bar{\gamma}$ as the input X, which is given as

$$X = (x_1, x_2, \ldots, x_5). \tag{19}$$

The output y can be obtained by (18).

B. CNN Structure

1) Data Preprocessing: Before training, we need to preprocess the data. The min–max standardization method is employed to implement data preprocessing and map the results to [0, 1]. The process is as follows:

$$y_{ij} = \frac{x_{ij}-\min(x_j)}{\max(x_j)-\min(x_j)}. \tag{20}$$

T_i is 5×1 data. It is transformed into $5\times1\times1$ after standardization. The characteristics of the data do not change, but it logically changes from 2-D to 3-D. Taking the $5\times1\times1$ matrix as an example, if each pixel is regarded as a value, the image data contains 25 pixels, and a strip of data is put into it in turn. In Fig. 3, the data transformation process is as follows.

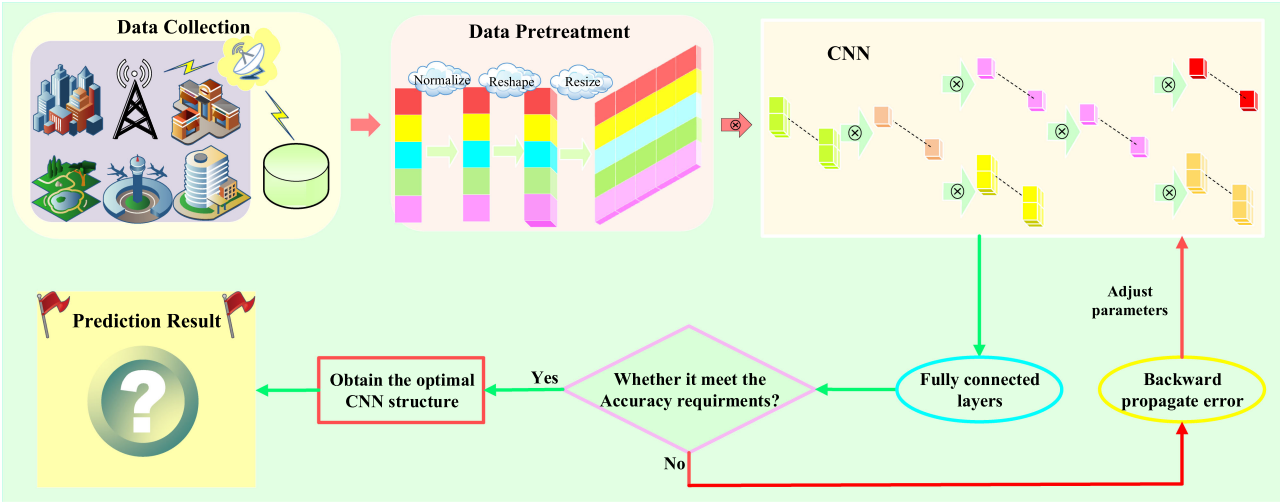

Fig. 2. SOP prediction algorithm.

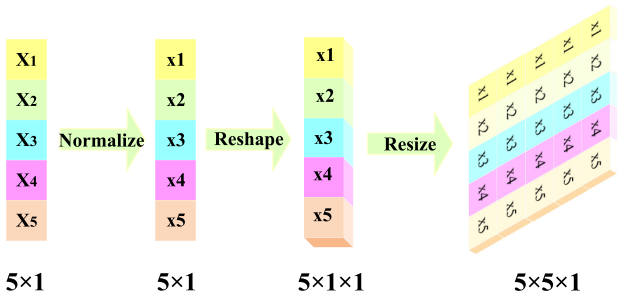

Fig. 3. Data preprocessing.

2) Input Layer: Input layer has five neurons. The $5 \times 5 \times 1$ data enters the input layer.

3) Convolution Layers: In Fig. 4, the designed CNN has five convolution layers. For five convolution layers, they all use the Same convolution in the padding which do not change data size.

For convolution layer conv1, there are 16 convolution kernels, which have a size 2×2. The number of channel is 1. The conv1 obtains a $5 \times 5 \times 16$ matrix. Next, $5 \times 5 \times 16$ matrix enters conv2, from which it can implement feature compression on data to obtain a $5 \times 5 \times 8$ matrix. The conv2 has 8 convolution kernels, which have a size 1×1. The channel number is 16.

Then, the $5 \times 5 \times 8$ matrix is sent to conv3, which has two branches. For the first branch, it employs 16 convolution kernels, and the size is 1×1. For the second branch, the size is 2×2. Through concatenating the feature map of the outputs for the first and second branch, a $5 \times 5 \times 32$ matrix is obtained. For the conv4, it employs 16 convolution kernels and the size is 1×1. A total of 16 convolution kernels are used to compress features. After rectified linear units (ReLU) function, it can obtain a $5 \times 5 \times 16$ matrix. Then, the $5 \times 5 \times 16$ matrix goes through conv5, which has two branches. For the first branch, it employs 132 convolution kernels. For the second branch, 32 convolution kernels are used, and the size is 2×2. Finally, it concatenates the feature map of the outputs for the first and second branch, and obtains a $5 \times 5 \times 64$ matrix.

4) Fully Connected Layer: The fully connected layer has two hidden layers, which are composed of 192 and 64 neurons, respectively. Then, the data passes through the Sigmoid function. Fig. 5 shows the fully connected layer. It can transform the convolution 3-D data into 1-D data.

C. Metric

We use R^2 to evaluate the SOP prediction. R^2 is

$$R^2 = 1 - \frac{\sum_{i=1}^{\mathrm{PP}} (d_i - y_i)^2}{\sum_{i=1}^{PP} (d_i - \bar{y_i})^2} \tag{21}$$

where PP is the number of testing data, y_i and d_i are the actual and predicted outputs, respectively.

D. SOP Prediction Based on CNN

Fig. 6 shows the SOP prediction algorithm, and the steps are as follows.

1) Feature data extraction and dataset building. We select $W_{\mathrm{SR}}, W_{\mathrm{RD}}, W_{\mathrm{RE}}, \gamma_{\mathrm{th}}, \bar{\gamma}$ as input X, and (18) can obtain the output y. Then, we employ (X, y) to build the dataset, which has 4860 groups of data.
2) Data preprocessing and splitting. The min–max standardization method is employed to implement data preprocessing. Then, the dataset is divided into 4810 groups for training and 50 groups for testing.
3) CNN construction and initialization. After building the CNN model, we generate the random numbers which obey the normal distribution. They are used to initialize the weights and biases. Then, we set the threshold, learning rate, and other parameters.
4) CNN training. In the training process, we need to calculate the results of each layer and the training error is used to adjust the structural parameters. Until the error is less than the threshold, the training process stops.
5) CNN testing. We employ the testing data to evaluate the proposed CNN model. If R^2 meets the requirement of

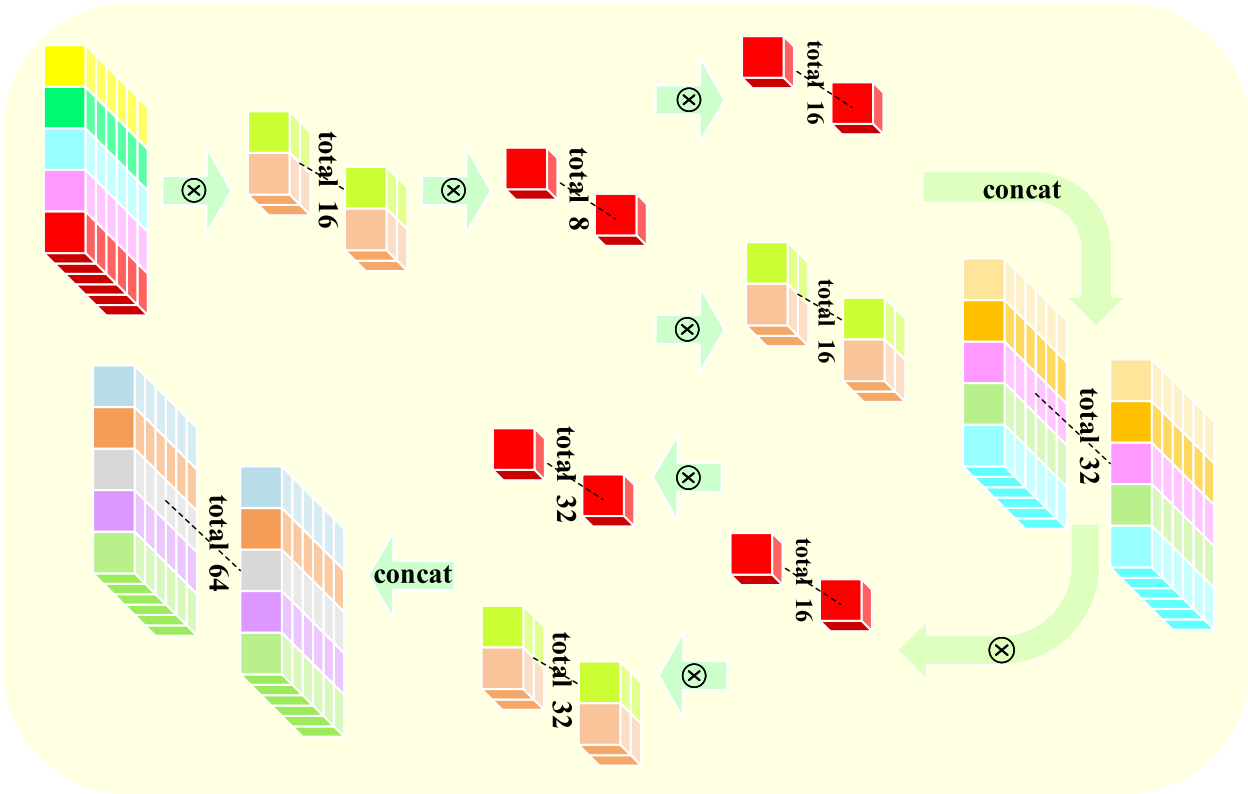

Fig. 4. CNN structure.

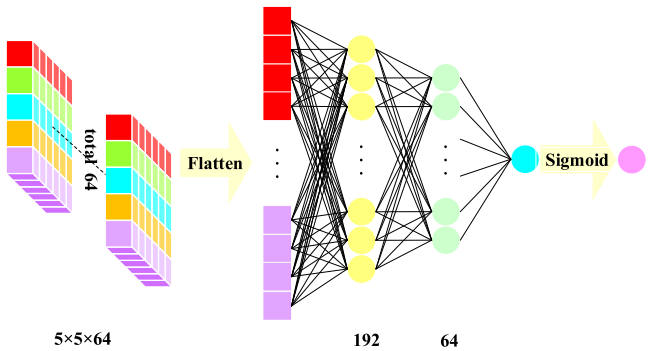

Fig. 5. Fully connected layer.

prediction, the CNN model is employed to predict the SOP performance.

The pseudocode is showed in Algorithm 1.

Algorithm 1: The SOP Prediction Algorithm.

Input: The ranges $r_1, r_2, \ldots, r_5$ of the selected 5 variables, $W_{\mathrm{SR}}, W_{\mathrm{RD}}, W_{\mathrm{RE}}, \gamma_{\mathrm{th}}, \bar{\gamma}$;
Output: The prediction value of SOP;
for $i = 1 : 5$ **do**
  x_i=rand(r_i, s);
end for
$y = \mathrm{Eq.}(14)(r_1, r_2, \ldots, r_5)$;
$T = [x_1, \ldots, x_5, y]$;
T is divided into a training set T_1 and a testing set T_2;
Initialize the weights of the CNN model with random numbers;
$M = \mathrm{CNN\text{-}Training}(T_1)$;
$yy = M(T_2)$;
$R^2 = 1 - \frac{\sum_{i=1}^{PP}(d_i - yy_i)^2}{\sum_{i=1}^{PP}(d_i - y\bar{y}_i)^2}$;
$y' = M(X')$;

V. Performance Results

In this section, we set $E = 1$, and define $\mu = W_{\mathrm{RD}}/W_{\mathrm{RE}}$. $\bar{\gamma} = 10$ dB. In Fig. 7, we evaluate the lower bound on SOP. The parameters are given in Table I. As u increases, the SOP performance is improved. The increase in u can improve the MR $\rightarrow$ MD channel communication condition. When $N_{\mathrm{t}} = 3$, the SOP performance is better than $N_{\mathrm{t}} = 1, 2$. The increase in N_{t} can improve the communication quality of MS $\rightarrow$ MR$\rightarrow$MD channel.

TABLE I
Simulation Parameters

Parameter	Values
m_{SR}	1
m_{RE}	1
m_{RD}	1
W_{SR}	5 dB
W_{RE}	5 dB
N_{t}	1,2,3
K	0.6
γ_{th}	0 dB

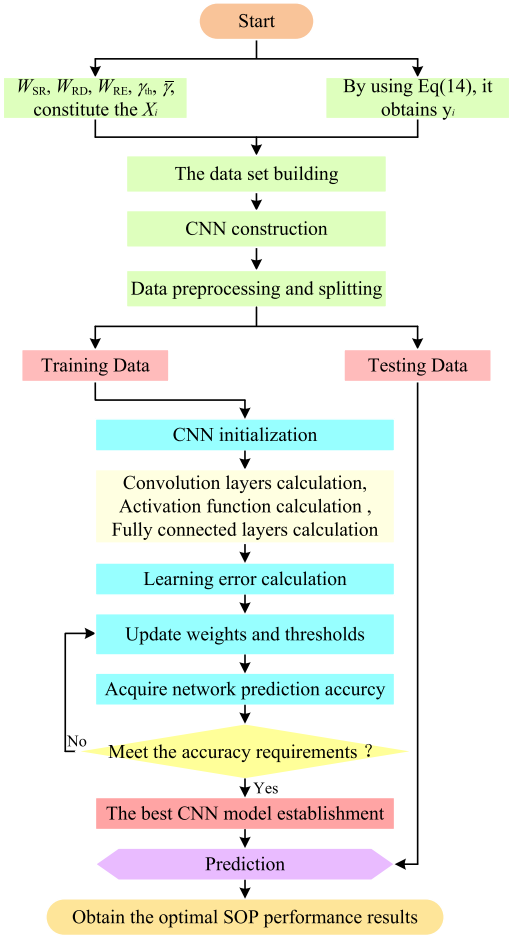

Fig. 6. SOP prediction algorithm.

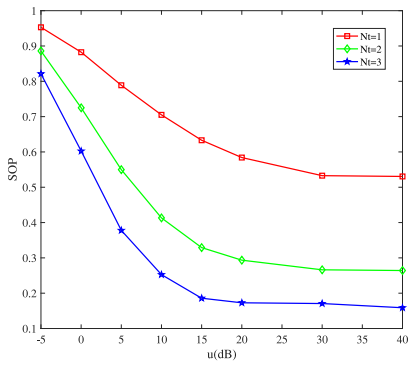

Fig. 7. Lower bound on SOP versus N_{t}.

For different TAS schemes, Fig. 8 presents the SOP performance. The parameters are in Table II. For the random TAS scheme, it randomly selects a single antenna. For a fixed u, the optimal TAS scheme can select the best antenna, which can provide the best MS $\rightarrow$ MR$\rightarrow$MD channel, and obtain the best SOP performance. Compared with the suboptimal TAS scheme, it has a 40% improvement. Furthermore, increasing u improves the SOP performance.

We compare CNN with DNN [27], InceptionNet [28], support vector machine [29], and Elman [30] methods in Figs. 9–18.

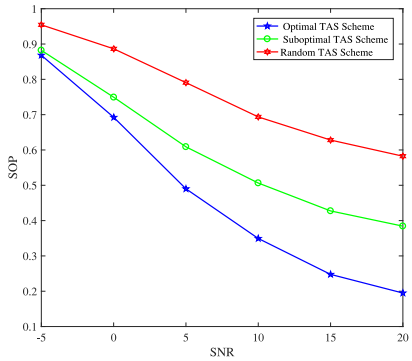

Fig. 8. SOP performance for different TAS schemes.

TABLE II
SIMULATION PARAMETERS

Parameter	Values
m_{SR}	1
m_{RE}	1
m_{RD}	1
W_{SR}	5 dB
W_{RE}	5 dB
N_{t}	2
K	0.6
γ_{th}	0 dB

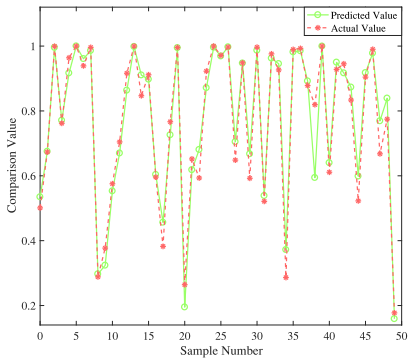

Fig. 9. CNN Prediction.

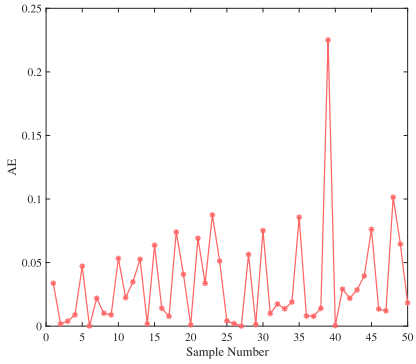

Fig. 10. CNN AE.

The parameters are given in Table III. Compared with DNN, InceptionNet, Elman, and SVM methods, the CNN algorithm can achieve better SOP prediction results. This is because the designed CNN can better adapt to complex mobile signals and extract signal features for SOP prediction.

TABLE III
SIMULATION PARAMETERS

Parameters	CNN	InceptionNet	DNN	Elman	SVM
	Trainning set: 4810		Testing set: 50		
Parameter 1	X: 5	X: 5	X: 5	X: 5	X: 5
Parameter 2	y: 1	y: 1	y: 1	y: 1	y: 1
Parameter 3	q: {16; 8; 16, 16; 16; 32, 32;}	q: {16; 32; 32; 32, 64; 32, 64; 32;}	q: {256;512;1024;}	q: {30}	c: 2
Parameter 4	lr: 0.00016	lr: 0.000056	lr: 0.00024	lr: 0.02	g: 0.3536

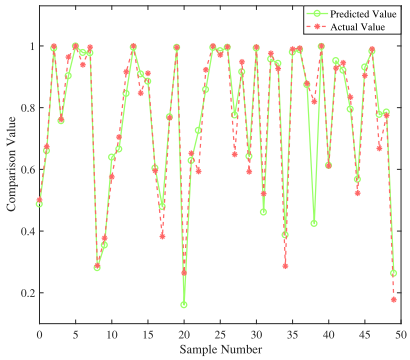

Fig. 11. InceptionNet prediction.

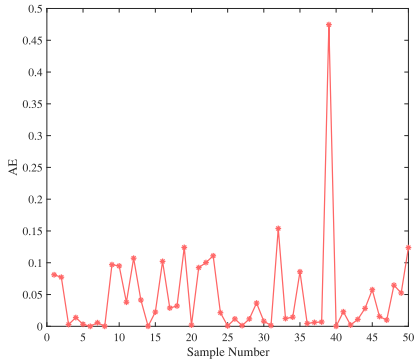

Fig. 14. DNN AE.

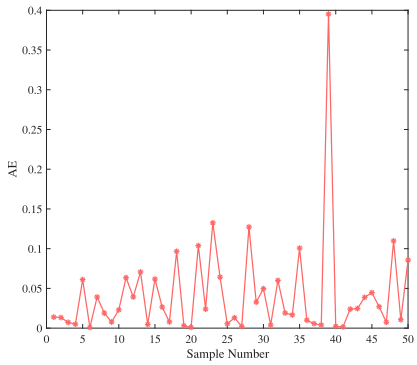

Fig. 12. InceptionNet AE.

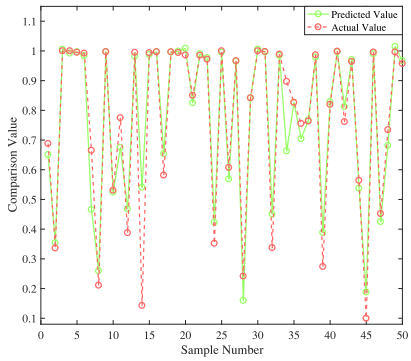

Fig. 15. Elman prediction.

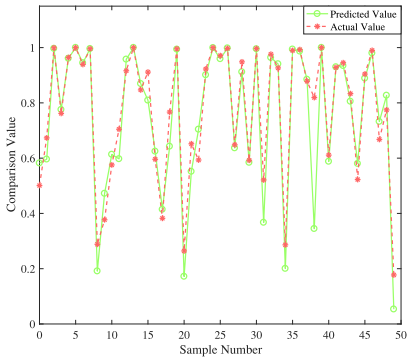

Fig. 13. DNN prediction.

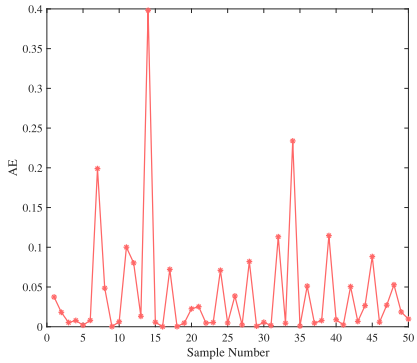

Fig. 16. Elman AE.

Figs. 19–22 show the AE, R^2, MSE, and running time comparisons for five algorithms. By analyzing Fig. 19, we obtain that, the AE of the CNN algorithm is 0.2251, which is lower than those of DNN, InceptionNet, Elman, and SVM methods. In Fig. 20, the R^2 of the CNN algorithm is 0.9526, which is the best in the five methods. Compared with DNN method, the CNN has a 6.9% improvement. In Fig. 21, the CNN algorithm has the best MSE performance 0.0026. Compared with DNN method, it has a 66.7% improvement. In Fig. 22, compared with Elman, DNN, InceptionNet, and SVM methods, the CNN algorithm has

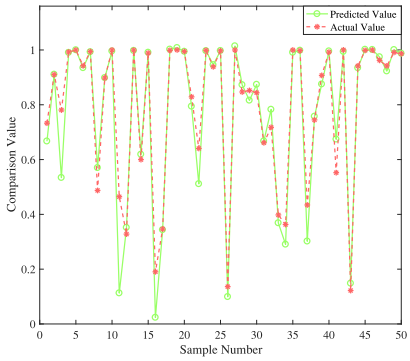

Fig. 17. SVM prediction.

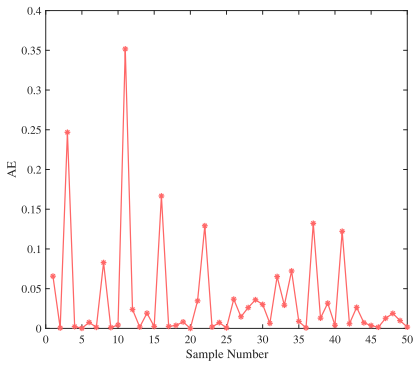

Fig. 18. SVM AE.

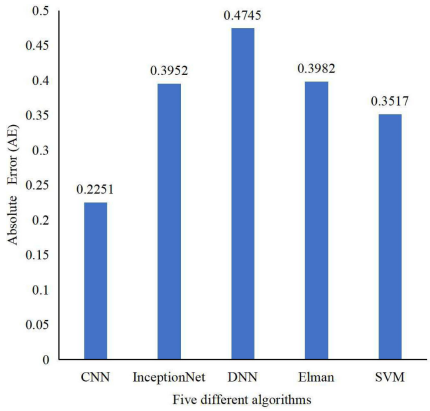

Fig. 19. AE comparison for the five algorithms.

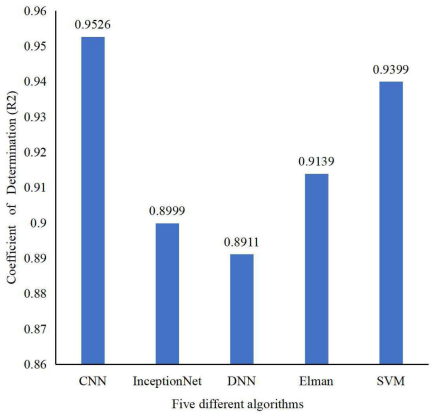

Fig. 20. R^2 comparison for the five algorithms.

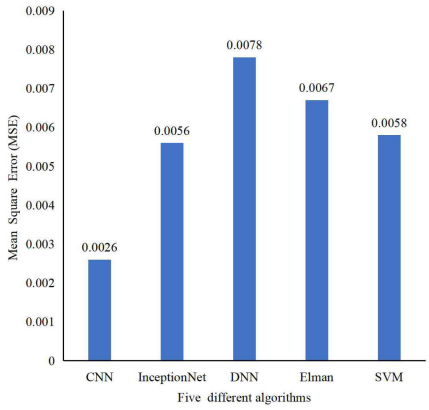

Fig. 21. MSE comparison for the five algorithms.

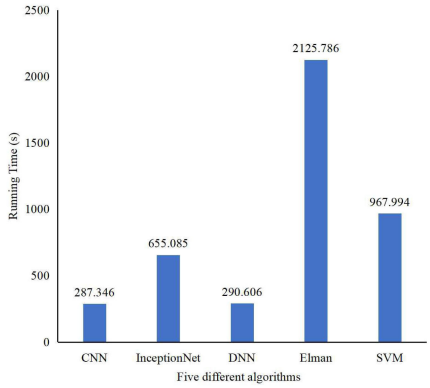

Fig. 22. Time comparison for the five algorithms.

shorter running time, which has a 86.5% reduction. Through AE, R^2, MSE, and running time comparisons, we can obtain that the improved CNN is the best forecasting model, which is more accurate and efficient than other algorithms. This is because the improved CNN employs SqueezeNet, which can reduce the network complexity and ensure the prediction accuracy.

VI. Conclusion

A TAS-based AF secrecy scheme was proposed in this article. We employed a strict mathematical analysis, and derived the lower bound on SOP. The derived SOP results were verified by simulation results, and employed to establish communication dataset. Then, a CNN-based prediction algorithm was proposed to predict the SOP. We designed the CNN model for SOP prediction. The designed CNN model can predict the SOP performance in real time, and reduce the computational complexity of complex mathematical expressions. Finally, we tested SVM, Elman, InceptionNet, and DNN methods. Compared with SVM, Elman, InceptionNet, and DNN methods, the CNN-based prediction algorithm can achieve better SOP prediction results. In particular, compared with DNN method, the MSE had a 66.7% improvement. Compared with Elman method, the running time had a 86.5% reduction.

REFERENCES

[1] C. D. Alwis *et al.*, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, no. 4, pp. 836–886, Apr. 2021.

[2] M. A. Togou *et al.*, "DBNS: A distributed blockchain-enabled network slicing framework for 5 G networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 90–96, Nov. 2020.

[3] Y. Y. Sun, J. J. Liu, J. D. Wang, Y. R. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Commun. Surv. Tut.*, vol. 22, no. 4, pp. 2694–2724, Dec. 2021.

[4] B. M. Mao, Y. C. Kawamoto, and N. Kato, "AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7032–7042, Aug. 2020.

[5] F. X. Tang, Y. C. Kawamoto, N. Kato, and J. J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE.*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[6] H. K. Narsani, P. Raut, K. Dev, K. Singh, and C. P. Li, "Interference limited network for factory automation with multiple packets transmissions," in *Proc. IEEE Int. Conf. Consum. Commun. Netw.*, Las Vegas, NV, USA, 2021, pp. 1–6.

[7] R. Atat, L. J. Liu, J. Ashdown, M. J. Medley, J. D. Matyjas, and Y. Yi, "A physical layer security scheme for mobile health cyber-physical systems," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 295–309, Jan. 2018.

[8] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[9] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Jan. 2018.

[10] G. C. Sun, Z. Han, J. B. Jiao, Z. Y. Wang, and D. G. Wang, "Physical layer security in MIMO wiretap channels with antenna correlation," *China Commun.*, vol. 14, no. 8, pp. 149–156, Aug. 2017.

[11] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13909–13921, 2017.

[12] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[13] X. M. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1027–1053, Feb. 2017.

[14] Y. H. Feng, S. H. Yan, Z. Yang, N. Yang, and W. P. Zhu, "TAS-Based incremental hybrid decode-amplify-forward relaying for physical layer security enhancement," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3876–3891, Sep. 2017.

[15] Y. J. Yao, W. Y. Zhou, B. H. Kou, and Y. Q. Wang, "Dynamic spectrum access with physical layer security: A game-based jamming approach," *IEEE Access*, vol. 6, pp. 12052–12059, 2018.

[16] H. Ilhan, M. Uysal, and I. Altunbas, "Cooperative diversity for intervehicular communication: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3301–3310, Jul. 2009.

[17] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "N-Nakagami: A novel stochastic model for cascaded fading channels," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1453–1458, Aug. 2007.

[18] A. Pandey and S. Yadav, "Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10615–10630, Nov. 2018.

[19] M. A. Togou *et al.*, "A distributed blockchain-based broker for efficient resource provisioning in 5G networks," in *Proc. IEEE Int. Conf. Wireless Commun. Mobile Comput.*, Limassol, Cyprus, 2020, pp. 1485–1490.

[20] L. Ren, J. B. Dong, X. K. Wang, Z. H. Meng, L. Zhao, and M. J. Deen, "A data-driven auto-CNN-LSTM prediction model for lithium-ion battery remaining useful life," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3478–3487, May 2021.

[21] H. Chung and K. Shin, "Genetic algorithm-optimized multi-channel convolutional neural network for stock market prediction," *Neural Comput. Appl.*, vol. 32, no. 12, pp. 7897–7914, Jun. 2020.

[22] C. X. Ding and D. C. Tao, "Trunk-branch ensemble convolutional neural networks for video-based face recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 4, pp. 1002–1014, Apr. 2018.

[23] W. Qiu, Q. Tang, J. Liu, and W. X. Yao, "An automatic identification framework for complex power quality disturbances based on multifusion convolutional neural network," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3233–3241, May 2020.

[24] A. Pandey, S. Yadav, D. T. Do, and R. Kharel, "Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15095–15112, Dec. 2020.

[25] F. K. Gong, P. Ye, Y. Wang, and N. Zhang, "Cooperative mobile-to-mobile communications over double Nakagami-m fading channels," *IET Commun.*, vol. 6, no. 18, pp. 3165–3175, Sep. 2012.

[26] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Veh. Technol.*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[27] W. C. He, S. Y. Guo, S. Guo, X. S. Qiu, and F. Qi, "Joint DNN partition deployment and resource allocation for delay-sensitive deep learning inference in IoT," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9241–9254, Oct. 2020.

[28] N. S. Chandel, S. K. Chakraborty, Y. A. Rajwade, K. Dubey, and M. K. T. D. Jat, "Identifying crop water stress using deep learning models," *Neural Comput. Appl.*, vol. 33, no. 10, pp. 5353–5367, May 2021.

[29] X. F. Li, X. P. Jia, L. G. Wang, and K. Zhao, "On spectral unmixing resolution using extended support vector machines," *IEEE Trans. Geosci. Remote*, vol. 53, no. 9, pp. 4985–4996, Sep. 2019.

[30] L. W. Xu, X. Yu, and T. A. Gulliver, "Intelligent outage probability prediction for mobile IoT networks based on an IGWO-Elman neural network," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1365–1375, Mar. 2021.