Mobile Collaborative Secrecy Performance Prediction for Artificial IoT Networks

Lingwei Xu, *Member, IEEE,* Xinpeng Zhou, *Student Member, IEEE,* Xingwang Li, *Senior Member, IEEE,* Rutvij. H. Jhaveri, *Senior Member, IEEE,* Thippa Reddy Gadekallu, *Member, IEEE,* and Yuan Ding

***Abstract*—The integration of artificial intelligence (AI) and Internet of Things (IoT) has promoted the rapid development of artificial IoT (AIoT) networks. A wide range of AIoT applications have generated a great deal of data. The fifth-generation (5G) mobile communication has powerful data processing capabilities, and it is a key technology to enable AIoT big data processing. The explosive growth of the 5G users has made information security in AIoT networks a significant issue. Real-time security evaluation in AIoT networks is difficult due to user mobility and dynamic wireless environments. Thus, evaluation and prediction of secrecy performance is a very critical research. In this paper, new expressions for the non-zero secrecy capacity probability (NSCP) are derived to evaluate the mobile collaborative secrecy performance. An improved convolutional neural network (CNN) model, named as SI-CNN in this paper, is proposed to predict the NSCP performance. The SI-CNN model combines the SqueezeNet and InceptionNet, and it has four convolution layers, which all adopt the Same convolution model. For the first two layers, they employ a 2×1 convolution and a three-branch convolution, which not only increase the number of channels but also extract more features. For the last two layers, they employ the same structure, but different convolution kernels. The proposed SI-CNN prediction algorithm is shown to provide better NSCP performance prediction than other state-of-the-art methods. In particular, compared with wavelet neural network (WNN), the prediction precision of SI-CNN is improved by 26.8%.**

***Index Terms*—AIoT network, collaborative secrecy performance, improved CNN, intelligent prediction.**

This research was supported by the Shandong Province Natural Science Foundation (No. ZR2020QF003), Open Research Fund of Anhui Engineering Technology Research Center of Automotive New Technique (No.QCKJ202101), Opening Foundation of Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education (No. K93-9-2021-09), Doctoral Found of QUST(No. 1203043003480), Scientific Research Project of Education Department of Guangdong (No. 2021KCXTD061), Science and Technology Program of Guangzhou (No. 202207010389), Key project of Guizhou Science and Technology Support Program (No. Guizhou Key Science and Support [2021]- 001). (*Corresponding author: Xingwang Li*).

L. W. Xu and X. P. Zhou are with the Department of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China; Anhui Engineering Technology Research Center of Automotive New Technique, Anhui Polytechnic University, Wuhu 241000, China; Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, Nanjing 211189, China (email: xulw@qust.edu.cn, xpzhou17853321957@163.com).

X. W. Li is with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China (email: lixingwangbupt@gmail.com).

R. H. Jhaveri is with the Department of Computer Science & Engineering, Pandit Deendayal Energy University, Gandhinagar, India (email: Rutvij.Jhaveri@sot.pdpu.ac.in).

T. R. Gadekallu is with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India (email: thippareddy.g@vit.ac.in).

Y. Ding is with the Institute of Sensors, Signals and Systems (ISSS), Heriot-Watt University, Edinburgh, UK (email: yuan.ding@hw.ac.uk).

I. Introduction

THE wireless devices and the associated multiuser services are increasing at a rapid rate. The corresponding growth in data volumes promotes the rapid integration of artificial intelligence (AI) and Internet of Things (IoT), and artificial IoT (AIoT) networks begin to enter our everyday lives [1]. However, the big data processing poses significant challenges facing AIoT networks. The fifth-generation (5G) mobile communication technology has powerful data processing capabilities, and can be a key collaborative technology for AIoT networks [2]. However, the mobility and the resulting unpredictable wireless environments make 5G AIoT users more vulnerable to cyberattacks than other internet users. A diverse of 5G AIoT applications have reported a number of information security incidents [3]. As a result, the security of wireless communications, in particular 5G physical layer security, becomes critically important.

The 5G secrecy performance has been widely investigated in [4-7]. The secrecy outage probability (SOP) for an ambient backscatter system was investigated in [4]. A closed-form SOP expression over dual correlated Rayleigh fading channels and Nakagami-m model was derived in [5] and [6], respectively. The complexity of wireless environments makes reliable mobile communications challenging. In [7], an *N*-Nakagami model was employed to characterize practical mobile communication scenarios, which is thus selected in this paper to evaluate the secrecy performance of mobile AIoT networks.

Closed-form SOP or non-zero secrecy capacity probability (NSCP) expressions have been derived for several types of channels. However, these expressions are computationally complex, which makes real-time analysis of the secrecy performance inapplicable. To ensure efficient and reliable secure communications, it is necessary to predict the secrecy performance in real-time. Recently, wireless communication applications have successfully applied AI for performance evaluation [8]. C. Q. Luo *et al*. employed the convolutional neural network (CNN) to predict the 5G wireless communication states in [9]. F. Demir *et al*. used a SqueezeNet model to extract the feature and classify human emotion in [10]. AI provides a new way for real-time prediction of secrecy performance, replacing the conventional methods which have high computational complexity.

To the best of the authors' knowledge, the NSCP performance prediction in 5G AIoT environments has not yet been investigated. Motivated by the above results, we aim

to propose an NSCP performance prediction algorithm based on an improved CNN model. In this paper, we analyze the collaborative NSCP performance of mobile AIoT networks. To reduce communication complexity, the transmit antenna selection (TAS) is taken into account. Particularly, we derive analytical NSCP expressions. The main contributions of this work are the following:

1. TAS is employed to analyze the mobile NSCP performance, and novel NSCP expressions are derived. Collaborative secrecy performance can be evaluated by these NSCP results, which differ from those in [4-7].
2. To predict secrecy performance, an improved CNN model named SI-CNN is proposed in this work. The SI-CNN model combines the SqueezeNet and InceptionNet, and it has four convolution layers. Through the designed network structure, the SI-CNN model is compressed to reduce the amount of calculation. At the same time, it ensures the prediction precision of the network through three branches.
3. An SI-CNN prediction algorithm is further proposed to determine the NSCP performance in real-time. In training phases, the proposed algorithm employs the channel state information (CSI) obtained from the above derived theoretical results to make a reliable NSCP performance prediction.
4. The performance of the proposed prediction algorithm is compared with those using other state-of-the-art methods, like SqueezeNet, InceptionNet, wavelet neural network (WNN), and deep neural network (DNN). It is shown that the proposed algorithm provides better prediction precision. Compared with WNN method, the prediction precision is increased by 26.8%.

Table I gives the notations used in this work.

TABLE I
NOTATIONS

Symbols	Designation
E	Total transmit power
N	The number of Nakagami variable
m	Nakagami fading coeffcient
SNR	Signal-to-noise ratio
CDF	The cumulative distribution function
PDF	The probability density function
MSE	Mean squared error
AE	Absolute error
$\max(.)$	Maximum function
$G(.)$	Meijer's G-function

II. Related Work

The secrecy performance evaluation of 5G AIoT is a research hotspot of intelligent communications [11]. In a two-tier 5G heterogeneous network, Y. Huo *et al*. employed cooperative jamming to ensure secure communications in [12]. L. Kong *et al*. derived the SOP over Fox H-function model in [13]. In [14], considering the vehicle-to-vehicle communication scenarios, A. Pandey *et al*. derived the SOP expressions, and showed the impacts of the mobile relay positions on the secrecy performance. $n\times$Rayleigh model was investigated by Y. Alghorani *et al*. in [15], and NSCP results were obtained. In [16], a learning-based resource allocation scheme was proposed by S. H. Ahmed *et al*. for industrial IoT. H. L. He *et al*. employed cooperative jamming and artificial noise to realize the secure transmission in scenarios with the presence of multiple eavesdroppers [17]. With a multi-antenna eavesdropper, J. Y. Zhang *et al*. investigated the security performance employing reconfigurable intelligent surface, and derived the SOP results [18]. In [19], to improve the security performance, re-configurable intelligent surface and non-orthogonal multiple access were employed to fight against internal eavesdroppers. However, the calculation process of these SOP or NSCP expressions is very complicated, which is not practical to real-time secrecy performance analysis.

AI is widely used by wireless communication applications to improve the communication performance [20], which include CNN, SqueezeNet, InceptionNet, WNN, and Elman methods, to name a few. With a proposed adaptive security specification method, B. M. Mao *et al*. predicted the wireless power harvested for IoT networks [21]. In [22], a spatial-frequency CNN model was used for channel estimation in the millimeter wave transmissions. H. Lee *et al*. employed the CNN model to detect object in [23]. WNN model was used to estimate the hourly electricity price in [24]. N. S. Chandel *et al*. proposed an InceptionNet model to identify crop water stress in [25]. In [26] Elman model was employed to realize the outage probability prediction in IoT networks. In underwater acoustic sensor networks, S. S. Song *et al*. proposed a location prediction model employing a belief propagation neural network, which can obtain location information effectively in [27]. A. P. Hermawan *et al*. investigated the beyond 5G communications and proposed an automatic modulation classification model employing the CNN network in [28], which can obtain better classification accuracy than other machine learning methods.

From the above analysis, we can see that AI techniques have been widely employed to enhance communication performance. Mobile AIoT user information security faces severe challenges. However, there has been very little research on the mobile secrecy performance prediction in AIoT networks. To this end, we propose an SI-CNN approach to investigate the secrecy performance prediction. The SI-CNN employs four convolution layers and adopts a Same model, which includes 2×1 convolution kernels and an ReLU activation function. Same convolution model will not change size after convolution. For the first two layers, they employ a 2×1 convolution and a three-branch convolution, which not only increases the number of channels but is also able to extract more features. For the last two layers, they employ the same structure, but with different convolution kernels. Compared with other AI methods, the SI-CNN model can significantly reduce computational complexity.

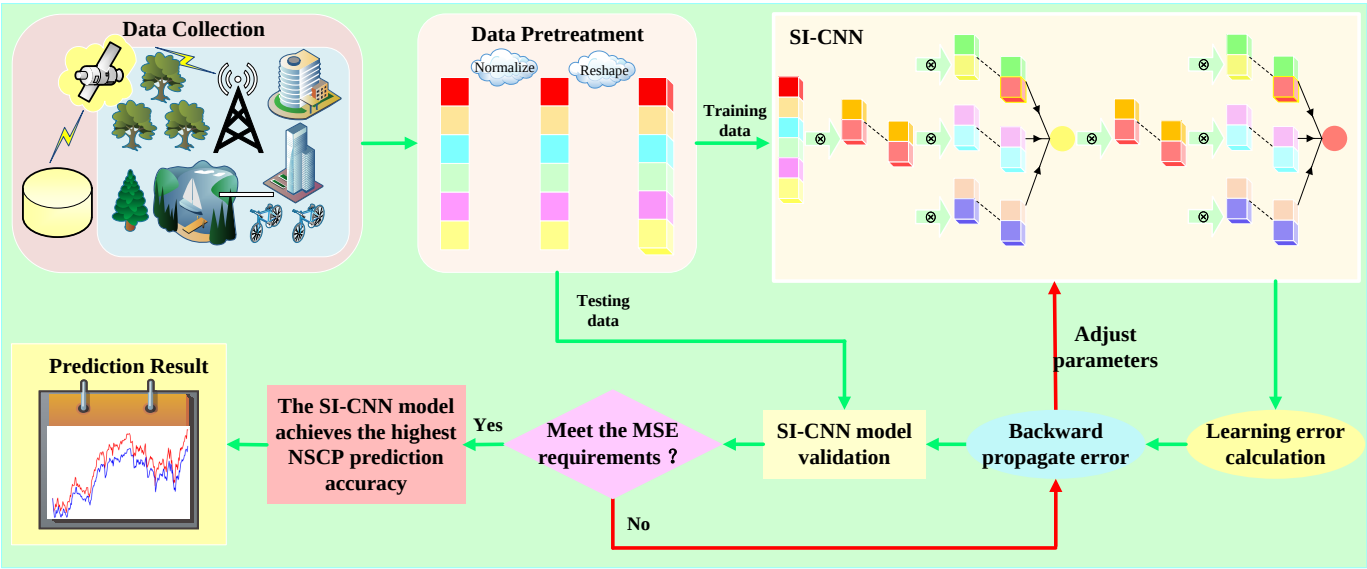


Fig. 1 The prediction algorithm

III. System Model

The system model consists of a mobile source (MS) equipped with N_{t} antennas, a mobile eavesdropper (ME), and a mobile destination (MD). We employ TAS to select the best antenna to transmit the signals. All wireless channels exhibit *N*-Nakagami model, which is more in line with the practical mobile communication environment.

When a signal x is transmitted from the ith MS antenna (MS_i), the received signals at the destination and eavesdropper are

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

$$r_{\mathrm{SE}i} = \sqrt{W_{\mathrm{SE}}E}h_{\mathrm{SE}i}x + n_{\mathrm{SE}i} \tag{2}$$

where $h_{\{\mathrm{SD,SE}\}i}$ is the MSi to {MD,ME} link channel coefficient, and $W_{\{\mathrm{SD,SE}\}}$ is the MS to {MD,ME} link relative geometrical gain. $n_{\mathrm{SD}i}$ and $n_{\mathrm{SE}i}$ are independent Gaussian noise.

The SNR at the mobile destination is

$$\gamma_{\mathrm{SD}i} = \frac{KW_{\mathrm{SD}}|h_{\mathrm{SD}i}|^2E}{N_0} \tag{3}$$

where K is the relative SNR gain, and average SNR is

$$\overline{\gamma_{\mathrm{SD}}} = KW_{\mathrm{SD}}\bar{\gamma} \tag{4}$$

$$\bar{\gamma} = \frac{E}{N_0} \tag{5}$$

The SNR at the mobile eavesdropper is

$$\gamma_{\mathrm{SE}i} = W_{\mathrm{SE}}\left|h_{\mathrm{SE}i}\right|^2\bar{\gamma} \tag{6}$$

with average SNR

$$\overline{\gamma_{\mathrm{SE}}} = W_{\mathrm{SE}}\bar{\gamma} \tag{7}$$

The instantaneous secrecy capacity is given as [29]

$$C_i = \max\{\ln(1+\gamma_{\mathrm{SD}i}) - \ln(1+\gamma_{\mathrm{SE}i}), 0\} \tag{8}$$

z is selected as the optimal antenna

$$z = \max_{1\le i\le N_t}(C_i) \tag{9}$$

IV. Non-Zero Secrecy Capacity Probability

Theorem 1 below provides the exact expression for NSCP, which captures the effect of fading parameters.

Theorem 1: The non-zero secrecy capacity probability (NSCP) is

$$F_{\mathrm{NSCP}} = 1 - \left(\frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{d=1}^{N}\Gamma(m_d)} G_{N+1,N+1}^{N+1,N} \times \left[\frac{\overline{\gamma_{\mathrm{SD}}}}{\overline{\gamma_{\mathrm{SE}}}} \frac{\prod_{d=1}^{N}\frac{m_d}{\Omega_d}}{\prod_{i=1}^{N}\frac{m_i}{\Omega_i}} \Big|_{m_1,\ldots,m_N,0}^{1-m_1,\ldots,1-m_N,1} \right] \right)^{N_{\mathrm{t}}} \tag{10}$$

where m is Nakagami fading coefficient.

proof. The NSCP can be expressed as

$$\begin{aligned} F_{\mathrm{NSCP}} &= \Pr\left(\max_{1\le i\le N_{\mathrm{t}}}(C_i) > 0\right) \\ &= 1 - \Pr\left(\max_{1\le i\le N_{\mathrm{t}}}(C_i) < 0\right) \\ &= 1 - (Q_1)^{N_{\mathrm{t}}} \end{aligned} \tag{11}$$

Q_1 in (11) is given as

$$\begin{aligned} Q_1 &= \Pr\left(C(\gamma_{\mathrm{SD}},\gamma_{\mathrm{SE}}) < 0\right) \\ &= \Pr\left(\gamma_{\mathrm{SD}} < \gamma_{\mathrm{SE}}\right) \\ &= \int_0^{\infty} F_{\gamma_{\mathrm{SD}}}(\gamma_{\mathrm{SE}}) f_{\gamma_{\mathrm{SE}}}(\gamma_{\mathrm{SE}}) d\gamma_{\mathrm{SE}} \end{aligned} \tag{12}$$

The CDF of γ_k, $k \in \{\mathrm{SD},\mathrm{SE}\}$ is then

$$F_{\gamma_k}(r) = \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)} G_{1,N+1}^{N,1}\left[\frac{r}{\overline{\gamma_k}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\Big|_{m_1,\ldots,m_N,0}^{1}\right] \tag{13}$$

and the corresponding PDF is

$$f_{\gamma_k}(r) = \frac{1}{r\prod_{i=1}^{N}\Gamma(m_i)} G_{0,N}^{N,0}\left[\frac{r}{\overline{\gamma_k}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\Big|_{m_1,\ldots,m_N}^{-}\right] \tag{14}$$

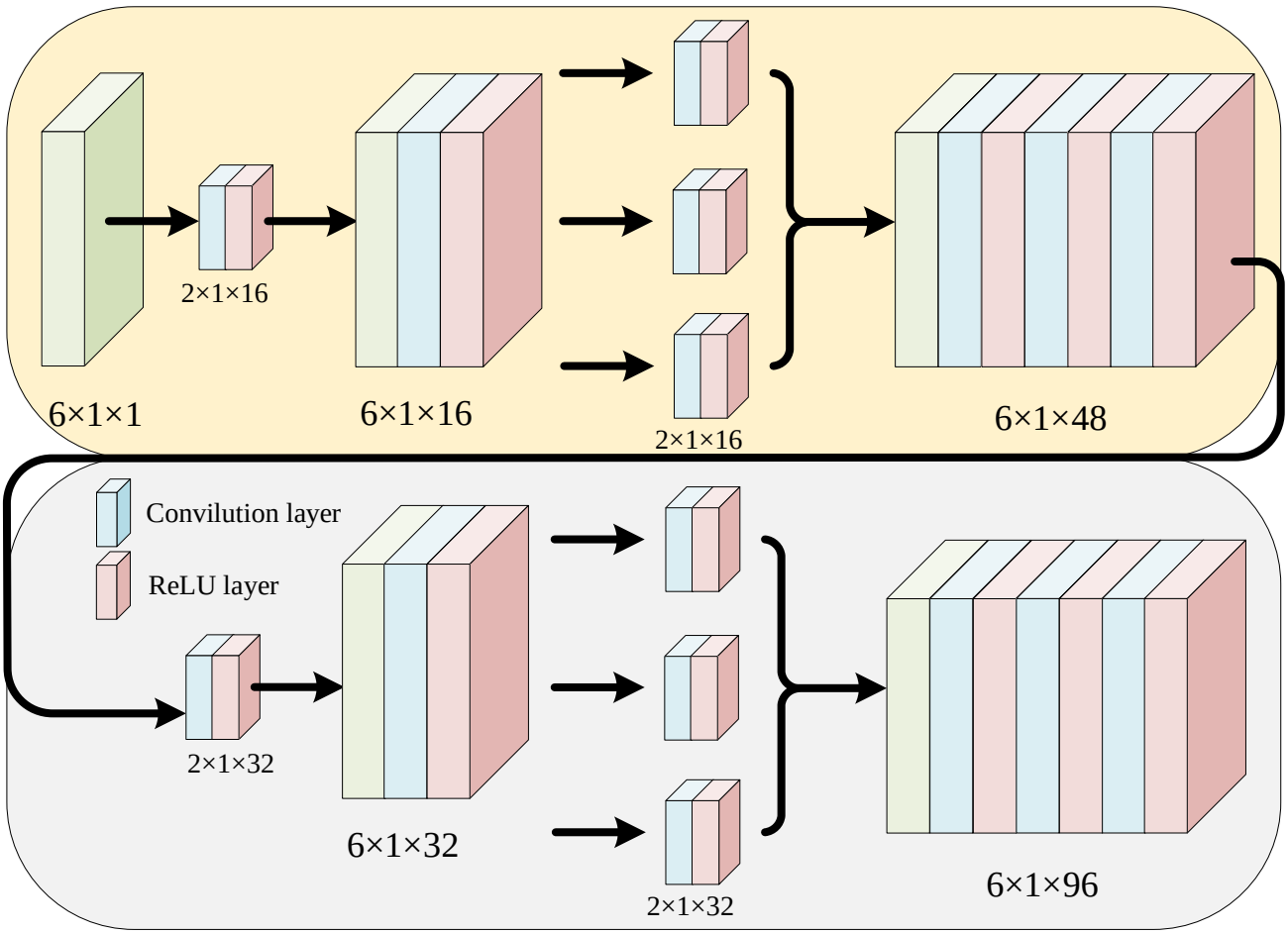


Fig. 2 The convolution layer of SI-CNN

Substituting (13), and (14) into (12) gives

$$Q_1 = \int_0^\infty \frac{1}{\prod_{d=1}^{N}\Gamma(m_d)} G_{1,N+1}^{N,1}\left[\frac{\gamma_{\rm SE}}{\overline{\gamma_{\rm SD}}}\prod_{d=1}^{N}\frac{m_d}{\Omega_d}\,|_{m_1,\ldots,m_N,0}^{1}\right] \times \frac{1}{\gamma_{\rm SE}\prod_{i=1}^{N}\Gamma(m_i)} G_{0,N}^{N,0}\left[\frac{\gamma_{\rm SE}}{\overline{\gamma_{\rm SE}}}\prod_{i=1}^{N}\frac{m_i}{\Omega_i}\,|_{m_1,\ldots,m_N}^{-}\right] d\gamma_{\rm SE}$$
$$= \frac{1}{\prod_{i=1}^{N}\Gamma(m_i)\prod_{d=1}^{N}\Gamma(m_d)} G_{N+1,N+1}^{N+1,N}\left[\begin{matrix}\frac{\overline{\gamma_{\rm SD}}}{\overline{\gamma_{\rm SE}}}\prod_{d=1}^{N}\frac{m_d}{\Omega_d} \\ \prod_{i=1}^{N}\frac{m_i}{\Omega_i}\end{matrix}\Big|_{m_1,\ldots,m_N,0}^{1-m_1,\ldots,1-m_N,1}\right] \quad (15)$$

and then (10) can be obtained by substituting (15) into (11).

V. Secrecy Performance Prediction Algorithm

Based on a novel SI-CNN model, a new NSCP performance prediction algorithm is proposed and illustrated in Fig. 1.

A. Data sets

Data sets is $T_i = (X_i, y_i)$. The 6 parameters $W_{\rm SD}$, $W_{\rm SE}$, m, K, N, $\bar{\gamma}$ construct the input vector

$$X_i = (x_{i1}, x_{i2}, \ldots, x_{i6}) \quad (16)$$

and this is used in (10) to obtain the NSCP y_i.

B. SI-CNN Structure

To predict NSCP performance, a novel SI-CNN model is proposed in this work. The designed SI-CNN model combines the SqueezeNet and InceptionNet, which can better extract features and obtain better prediction results than other methods. The InceptionNet employs the parallel multiple branches structure. The multiple branches are combined horizontally and finally concatenated according to the depth direction, which increases the number and accuracy of feature extraction. The SqueezeNet provides the idea of lightweight network and employs the method of compressed channel re-expansion. By compressing the dimension of the characteristic graph, it can reduce the network weight parameters and do not affect the performance of the network.

For the SI-CNN network, it uses the Adam optimizer. The batch size is 50, learning rate is 0.000056, and epochs are 30000.

1) Input layer: T_i is 6×1 data. Therefore, the 6×1 is transformed into 6×1×1 in the data preprocessing. Input layer has 6 neurons. Tthe 6×1×1 data is then fed into the input layer.

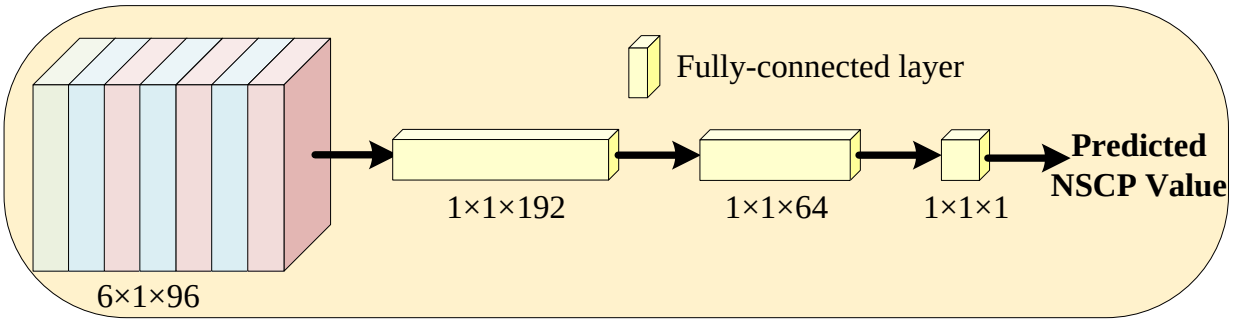


Fig. 3 The fully connected layer

2) Convolution layers: The SI-CNN has four convolution layers, which are shown in Fig. 2. The convolution layer *conv1* has 16 convolution kernels and 1 channel. Through the *conv1*, a $6 \times 1 \times 16$ matrix is obtained. The convolution layer *conv2* has three branches. Each branch has 16 convolution kernels and 16 channels. Next, it concatenates the data from three branches to obtain a $6 \times 1 \times 48$ matrix. The convolution layer *conv3* (32 convolution kernels and 48 channels) processes the $6 \times 1 \times 48$ matrix, and it can obtain a $6 \times 1 \times 32$ matrix. After that, the convolution *conv4* processes $6 \times 1 \times 32$ matrix. It has three branches, each branch has 32 convolution kernels and 32 channels. Finally, it can acquire a $6 \times 1 \times 96$ matrix.

3) Fully Connected Layer: It receives the $6 \times 1 \times 96$ matrix from the convolution layers, and then it flattens the data into one dimension data. There are two hidden layers, and the neurons are 192 and 64, respectively. The Sigmoid function is used at the end of the calculation. Fig. 3 shows the fully connected layer.

C. Secrecy performance prediction based on SI-CNN

The metrics, mean square error (MSE) and abusolute error (AE), are given as

$$\mathrm{MSE} = \frac{\sum_{z=1}^{P} (d^z - y^z)^2}{P} \tag{17}$$

and

$$\mathrm{AE} = |d^\beta - y^\beta| \tag{18}$$

where d^z is the desired result, y^z is the actual value, and P is the size of testing data.

Algorithm 1 provides the pseudo code of the proposed SI-CNN prediction algorithm.

VI. Result Analysis

In this section, we assume the total energy $E = 1$. All simulations are performed using MATLAB R2015b.

Fig. 4 presents the NSCP versus K with $\bar{\gamma} = 10$ dB. Other parameters are given in Table II. Fig. 4 shows that the simulation results match the analytical results very well. As expected, increasing N_t improves the secrecy performance. When N_t is fixed, lager K increases the NSCP. This is because a higher K improves the MS to MD channel while degrades the MS to ME channel.

Algorithm 1 The Proposed SI-CNN Prediction Algorithm

Input: The ranges $r_1, r_2, \ldots, r_6$ of the selected 6 variables, $W_{\mathrm{SD}}, W_{\mathrm{SE}}, m, N, K, \gamma_{\mathrm{th}}$;
Output: The prediction value of NSCP Y';
Data set establishment. Data set T is divided into a training set T_1 and a testing set T_2;
for $i = 1 : 6$ **do**
  x_i=rand(r_i, q);
end for
$Y = \mathrm{Eq.}(10)(x_1, \ldots, x_6)$;
$X = [x_1, \ldots, x_6]$;
$T = [X, Y]$;
Network initialization. It sets the values of the maximum number of iterations, and the learning rate. The weights and biases are calculated as follows
//Generate normal distribution random numbers;
w_j=random.normal$(r_j,\ n)$;
//Generate biases b with an initial value of 0;
b_j=zero(r_j, n);
Network training. During training, the outputs of each layer are obtained, and it calculates the training error loss.
  //Convolution layers
for $ii = 1 : 30000$ **do**
  $XX_0 = T_1$;
  //2D-convolution
  for $j = 0 : 3$ **do**
    $conv_{j+1} = \mathrm{conv2d}(XX_j, w_{j+1})$;
    $XX_{j+1} = \mathrm{ReLU}(\mathrm{bias\_add}(conv_{j+1}, b_{j+1}))$;
  end for
  //Fully connected layers
  $fc_1 = \mathrm{ReLU}(\mathrm{matmul}(XX_4, w_j) + b_j)$;
  $fc_2 = \mathrm{ReLU}(\mathrm{matmul}(fc_1, w_j) + b_j)$;
  $\hat{Y} = \mathrm{Sigmoid}(\mathrm{matmul}(fc_2, w_j) + b_j)$;
  $\mathrm{loss} = \left(Y - \hat{Y}\right)^2$;
end for
Network testing. T_2 is used to evaluate the training SI-CNN model. If these requirements are met, the training SI-CNN model can be used for NSCP prediction;
$M = \mathrm{Testing}(T_2)$;
$\mathrm{MSE} = \frac{\sum_{i=1}^{P} \left(d^i - y^i\right)^2}{P}$;
$Y' = M(X')$;

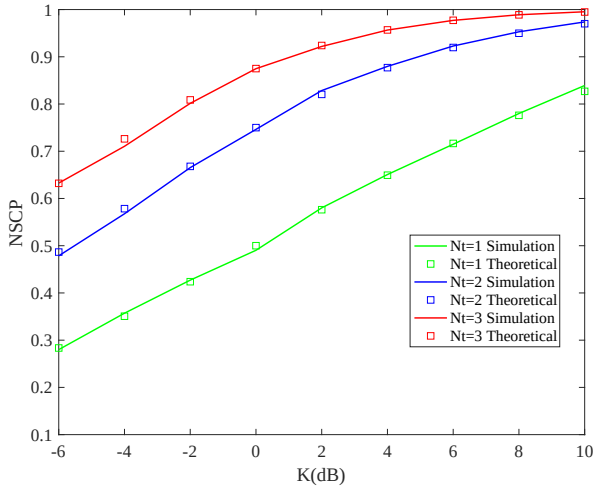


Fig. 4 The NSCP versus N_{t}.

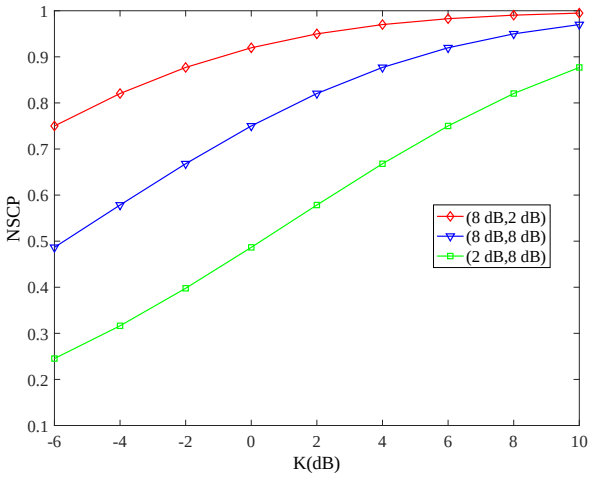


Fig. 5 The NSCP for the three values of (W_{SD}, W_{SE})

TABLE II
SIMULATION PARAMETERS FOR FIGS. 4,5

Parameter	Value
m_{SD}	1
m_{SE}	1
W_{SD}	2 dB, 5 dB, 8 dB
W_{SE}	2 dB, 5 dB, 8 dB
N_{SD}	2
N_{SE}	2
N_{t}	1,2,3
γ_{th}	0 dB

Fig. 5 presents the NSCP versus K for the three values of (W_{SD}, W_{SE}) with $\bar{\gamma} = 10$ dB. For a fixed K, increasing W_{SD} and decreasing W_{SE} improve the NSCP. The NSCP for (8 dB, 2 dB) is better than that with (8 dB, 8 dB) or (2 dB, 8 dB). This is because increasing W_{SD} means the MD is closer to the MS than the ME, *i.e.* the SNR of the {MS, MD} link is higher than that of the {MS, ME} link. Further, larger K improves the NSCP.

The prediction results of SI-CNN are presented in Fig. 6, which are better than any of the other methods. This is because the proposed SI-CNN algorithm employs a 2×1 convolution and a three-branch convolution, which not only increase the number of channels, but also extract more features. The SI-CNN model is compressed to reduce the burden of computation. At the same time, it ensures the prediction precision of the SI-CNN model through three branches.

Comparisons of the AEs and MSEs for the five algorithms are given in Figs. 7 and 8. In Fig. 7, the MSE with the SI-CNN algorithm is only 0.00951 and is lower than other methods. Compared with WNN, it shows that the SI-CNN algorithm enjoys a 26.8% improvement. In Fig. 8, the SI-CNN algorithm has the best AE. Compared with WNN algorithm, the SI-CNN has a 45% reduction. All these makes the SI-CNN the best prediction model.

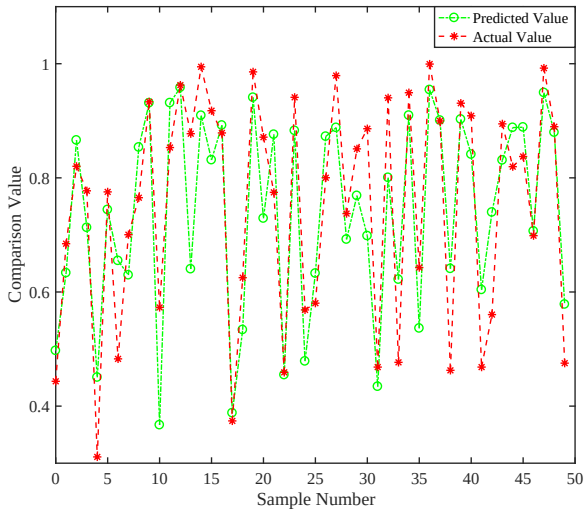


Fig. 6 Prediction of SI-CNN.

VII. CONCLUSION

The NSCP performance prediction of mobile AIoT networks was investigated in this paper. Novel expressions for the NSCP were derived. Furthermore, an SI-CNN algorithm was presented for NSCP performance prediction. The SI-CNN has four convolution layers, which all employ the Same convolution model. At the same time, it can ensure the prediction precision through three branches with 32 convolution kernels and 32 channels. Compared with DNN, SqueezeNet, InceptionNet, and WNN methods, the proposed SI-CNN algorithm provided better MSE and AE results. Compared with WNN method, the MSE and AE had a 26.8% and 45% improvement, respectively.

In future work, we will consider designing the lightweight network model, which can achieve a balance between prediction accuracy and network complexity.

TABLE III
PARAMETERS FOR THE FIVE ALGORITHMS

Algorithm	**SI-CNN**	**SqueezeNet**	**InceptionNet**	**WNN**	**DNN**
		Trainning set: 11830		Testing set: 50	
$\|X\|$	6	6	6	6	6
$\|y\|$	1	1	1	1	1
	q : [16; 16, 16, 16; 32; 32, 32, 32;]	q : [16; 16; 32; 64, 64]	q : [16; 32; 32; 32; 32, 64; 32, 64; 32]	τ_1 : 0.01	[16; 32]
	$learning\ rate$: 0.00009	$learning\ rate$: 0.000048	$learning\ rate$: 0.000056	τ_2 : 0.001	$learning\ rate$: 0.00012

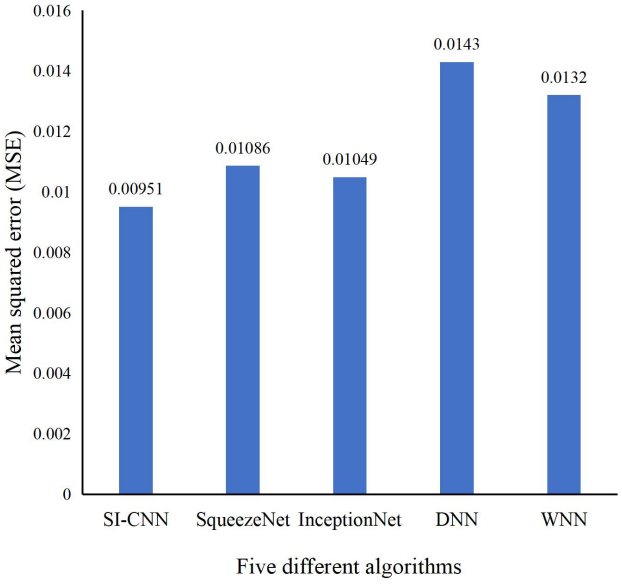


Fig. 7 MSE comparison for the five algorithms

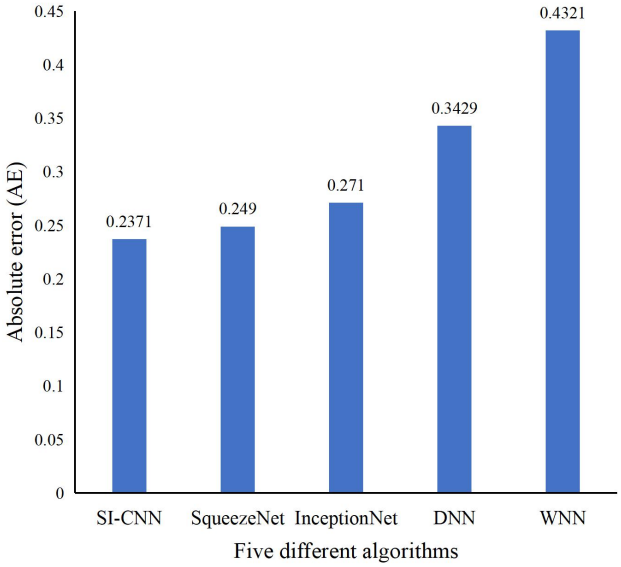


Fig. 8 AE comparison for the five algorithms

REFERENCES

[1] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Cognitive radio in low power wide area network for IoT applications: Recent approaches, benefits and challenges," *IEEE Trans. Industrial Inform.*, vol. 16, no. 12, pp. 7489 - 7498, Dec. 2020.

[2] J. Nightingale, P. S. Garcia, J. M. A. Calero, and Q. Wang, "5G-QoE: QoE modelling for ultra-HD video streaming in 5G networks," *IEEE Trans. Broadcast.*, vol. 64, no 2, pp. 621 - 634, June. 2018.

[3] 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 of Things J.*, vol. 5, no. 1, pp. 295 - 309, Jan. 2018.

[4] X. W. Li, M. L. Zhao, Y. W. Liu, L. H. Li, Z. G. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Trans. Veh. Technol*, vol. 69, no. 10, pp. 12286 - 12290, Oct. 2020.

[5] K. N. Le, "Secrecy and end-to-end analyses employing opportunistic relays under outdated channel state information and dual correlated Rayleigh fading," *IEEE Trans. Veh. Technol*, vol. 67, no. 11, pp. 10504 - 10518, Nov. 2018.

[6] C. Yu, H. L. Ko, X. Peng, and W. W. Xie, "Secrecy outage performance analysis for cooperative NOMA over Nakagami-m channel," *IEEE Access*, vol. 7, pp. 79866 - 79876, Jun. 2019.

[7] 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.

[8] L. Wen, X. Y. Li, L. Gao, and Y. Y. Zhang, "A new convolutional neural network-based data-driven fault diagnosis method," *IEEE Trans. Industrial Inform.*, vol. 65, no. 7, pp. 5990 - 5998, Jul. 2018.

[9] C. Q. Luo, J. L. Ji, Q. L. Wang, X. H. Chen, and P. Li, "Channel state information prediction for 5G wireless communications: A deep learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 227 - 236, Jan. 2020.

[10] F. Demir, N. Sobahi, S. Siuly, and A. Sengur, "Exploring deep learning features for automatic classification of human emotion using EEG rhythms," *IEEE Sens. J.*, vol. 21, no. 13, pp. 14923 - 14930, Jul. 2021.

[11] H. Yu, and J. Joung, "Design of the power and dimension of artificial noise for secure communication systems," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4001 - 4010, Jun. 2021.

[12] Y. Huo, X. Fan, L. Ma, X. Z. Cheng, Z. Tian, and D. C. Chen, "Secure communications in tiered 5G wireless networks with cooperative jamming," *IEEE Trans. Wirel. Commun.*, vol. 18, no. 6, pp. 3265 - 3280, Jun. 2019.

[13] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over Fox's H-function wiretap fading channels," *IEEE Trans. Veh. Technol*, vol. 68, no. 7, pp. 6608 - 6621, Jul. 2019.

[14] 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.

[15] Y. Alghorani, G. Kaddoum, S. Muhaidat, S. Pierre, and N. Al-Dhahir, "On the performance of multihop-intervehicular communications systems over n×Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 116 - 119, Feb. 2016.

[16] H. J. Liao, Z. Y. Zhou, X. W. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S. H. Ahmed, and A. K. Bashir, "Learning-based context-aware resource allocation for edge computing-empowered industrial IoT," *IEEE Internet of Things J.*, vol. 7, no. 5, pp. 4260 - 4277, May. 2020.

[17] H. L. He, X. Z. Luo, J. Weng, and K. M. Wei, "Secure transmission in multiple access wiretap channel: Cooperative jamming without sharing CSI," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 5, pp. 3401 - 3411, May. 2021.

[18] J. Y. Zhang, H. Y. Du, Q. Sun, B. Ai, D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided

networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 5, pp. 3480 - 3495, May. 2021.
[19] Z. Zhang, C. S. Zhang, Ch. J. Jiang, F. Jia, J. H. Ge, and F. K. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451 - 4463, May. 2021.
[20] G. Gui, F. Liu, J. L. Sun, J. Yang, Z. Q. Zhou, and D. X. Zhao, "Flight delay prediction based on aviation big data and machine learning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 140 - 149, Jan. 2020.
[21] B. M. Mao , Y. Kawamoto, and N. Kato , "AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things," *IEEE Internet of Things J.*, vol. 7, no. 10, pp. 7032 - 7042, Aug. 2020.
[22] P. H. Dong, H. Zhang, G. Y. Li, I. S. Gaspar, and N. N. Alizadeh, "Deep CNN-based channel estimation for mmWave massive MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 5, pp. 989 - 1000, Sept. 2019.
[23] H. Lee, S. Eum, and H. Kwon, "ME R-CNN: Multi-expert R-CNN for object detection," *IEEE Trans. Image Process.*, vol. no. 9, pp. 1030 - 1044, Sept. 2020.
[24] M. Rafiei, T. Niknam, and M. H. Khooban, "Probabilistic forecasting of hourly electricity price by generalization of ELM for usage in improved wavelet neural network," *IEEE Trans. Industrial Inform.*, vol. 13, no. 1, pp. 71 - 79, Feb. 2017.
[25] 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. Applic.*, vol. 33, no. 10, pp. 5353 - 5367, May. 2021.
[26] 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, Feb. 2021.
[27] S. S. Song, J. Liu, J. N. Guo, C. Zhang, T. T. Yang, and J. H. Cui, "Efficient velocity estimation and location prediction in underwater acoustic sensor networks," *IEEE Internet of Things J.*, Jul. 2021. doi: 10.1109/JIOT.2021.3094305.
[28] A. P. Hermawan, R. R. Ginanjar, D. S. Kim, and J. M. Lee, "CNN-based automatic modulation classification for beyond 5G communications," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1038 - 1041, May. 2020.
[29] 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.

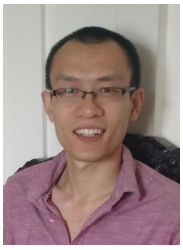
Lingwei Xu (M'18) received his Ph.D. degree in Intelligent Information and Communication System, Ocean University of China, Qingdao, China, in 2016. From 2016 to now, he is an associate professor of the College of Information Science and Technology, Qingdao University of Science and Technology. He has published about 50 research papers in international SCI/EI journals and conferences. His research interests include AI-based networking and wireless communications, and 5G mobile wireless communications. He has served as an editor for Computational Intelligence and Neuroscience, International Arab Journal of Information Technology.

Xinpeng Zhou (S'20) was born in Sichuan, China, in 1998. He is currently pursuing the master' s degree with the College of Information Science & Technology, Qingdao University of Science & Technology, Qingdao, China. His research is physical layer security performance prediction and analysis based on deep learning.

Xingwang Li (S'12-M'15-SM'20) received the M. Sc. and Ph. D. degrees from University of Electronic Science and Technology of China and Beijing University of Posts and Telecommunications in 2010 and 2015. From 2010 to 2012, he worked at Comba Telecom Ltd. In Guangzhou China, as an engineer. He spent one year from 2017 to 2018 as a visiting scholar at Queen's University Belfast, Belfast, UK. He is also a visiting scholar at State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications from 2016 to 2018. He is currently an Associated Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo China. His research interests include backscatter communication, Intelligent reflecting surface, artificial intelligence, hardware constrained communication, non-orthogonal multiple access, physical layer security, cooperative communication, unmanned aerial vehicles, MIMO communication, and the Internet of Things. He has served as many TPC members, such as the IEEE Globecom, IEEE WCNC, IEEE VTC, IEEE ICCC and so on. He has also served as the Co-Chair for the IEEE/IET CSNDSP 2020 of the Green Communications and Networks Track. He also serves as an Editor on the Editorial Board for IEEE Access, Computer Communications, Physical Communication, KSII Transaction on Internet and Information Systems, IET Networks and IET Quantum Communication. He is also the Guest Editor of the special issue on Computational Intelligence and Advanced Learning for Next-Generation Industrial IoT of IEEE Transactions on Network Science and Engineering.

Rutvij H. Jhaveri (Senior Member IEEE) is assistant professor in the Department of Computer Science & Engineering, Pandit Deendayal Energy University, Gandhinagar, India.In 2017, he was awarded Pedagogical Innovation Award by Gujarat Technological University, India. He authored 90+ publications in various prestigious journals and conferences. His research publications are cited 1700+ times with h-index 20. He is editorial board member and reviewer of several journals of international repute. He is also serving as a guest editor in several international journals of repute. Apart from this, he also served as a committee member in "Smart Village Project" - Government of Gujarat, India at Bharuch district during the year 2017. He is a life member of several professional bodies such as CSI and ISTE. His research interests include Network Security, Software-Defined Networking in IIoT/CPS with Machine Learning and Data Analytics.

Thippa Reddy Gadekallu is currently working as Associate Professor in School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India. He completed his Ph.D in VIT, Vellore, Tamil Nadu, India. He has published more than 90 international/national publications. Currently, his areas of research include Machine Learning, Internet of Things, Deep Neural Networks, Blockchain, Computer Vision.



Yuan Ding received his Bachelor' s degree from Beihang University (BUAA), Beijing, China, in 2004, Master' s degree from Tsinghua University, Beijing, China, in 2007, and Ph.D. degree from Queen' s University of Belfast, Belfast, UK, in 2014, all in Electronic Engineering. He is now an Assistant Professor at the Institute of Sensors, Signals and Systems (ISSS) in Heriot-Watt University, Edinburgh, UK. His research interests are in IoT-related physical-layer designs, antenna array, physical layer security, and 5G related areas. He was the recipient of the IET Best Student Paper Award at LAPC 2013 and the recipient of the Young Scientists Awards in General Assembly and Scientific Symposium (GASS), 2014 XXXIst URSI.