Hindawi
Mobile Information Systems
Volume 2021, Article ID 4132622, 8 pages
https://doi.org/10.1155/2021/4132622

Research Article

Elman-Based Secure Data Transmission Quality Prediction for Complex IoT Networks

Fagen Yin

College of Physical Science and Engineering, Yichun University, Yichun 336000, Jiangxi, China

Correspondence should be addressed to Fagen Yin; ynx522@163.com

Received 18 June 2021; Revised 28 July 2021; Accepted 17 August 2021; Published 26 August 2021

Academic Editor: Qinglin Zhao

The information age has brought earth-shaking changes. For interconnection of all things, the data transmission has widely employed the Internet of Things (IoT). The IoT transmission faces complex environments. The secure data transmission is very important for mobile IoT networks. The secure data transmission quality prediction is investigated for mobile IoT networks. The probability of strictly positive secrecy capacity (SPSC) is used to evaluate the secure data transmission quality, and the expressions are first derived. Then, employing Elman network, a secure data transmission quality intelligent prediction approach is proposed. The extensive simulations are run to evaluate the proposed approach. The simulation results show that the Elman-based approach can achieve a higher quality precision than other methods. The Elman-based approach also can achieve a lower time complexity.

1. Introduction

With the explosive growth of mobile applications, Internet of things (IoT) networks are widely used to transmit data [1]. The fifth generation (5G) mobile communication also has been widely used in mobile IoT networks [2, 3]. Different 5G applications widely use sea-land-air mobile communication networks [4, 5]. The global and diversified application will provide quick and convenient services for IoT users. However, due to IoT mobility and the diversity of IoT networks, the physical layer security (PLS) of 5G mobile IoT networks is facing many challenges [6].

PLS of 5G IoT networks is a research hot spot [7]. Low-complexity schemes for IoT PLS were presented in [8]. In [9], power control mechanism and antenna transmission scheme were used to realize the secure data transmission in cognitive wiretap networks. Considering the mobile healthcare networks, Xu et al. [10] investigated the PLS performance using the deep learning method. In [11], the authors used compressed sensing and cooperative schemes to achieve the secure transmission. Considering the user and relay selection, Fan et al. [12] analyzed two criteria and investigated the achievable PLS performance. The authors of [13] analyzed the upper and lower bounds on PLS performance over dependent fading channels.

The IoT data transmission faces a wide variety of scenarios and complex environments. The PLS issue is more and more serious. However, predicting and evaluating the secure data transmission quality are very difficult. Recently, machine learning techniques are applied in 5G wireless communications [14, 15]. In medical IoT, support vector machine (SVM) model was used to train data privacy [16]. High-performance visual tracking was achieved by an extreme learning machine (ELM) model in [17]. In [18], general regression (GR) model was used to evaluate the video transmission quality. The radial basis function (RBF) network was optimized to reconstruct the image in [19].

The studies of secure data transmission quality prediction are rare. So, our paper investigates the secure data transmission quality prediction of mobile IoT networks. The main contributions are given as follows.

(1) With amplify-and-forward (AF) relaying scheme, we use SPSC to evaluate secure data transmission quality and derive the exact expressions.

(2) To realize real-time analysis of secure data transmission quality, we propose a secure data transmission quality prediction approach based on the Elman neural network. The proposed approach is compared with ELM, GR, and RBF methods.

(3) Through the extensive simulations, we verify the derived results. Compared with different methods, the quality assessment effect of Elman-based approach is better, and time complexity is lower.

2. The IoT System Model

The system has a mobile source (S), mobile destination (D), mobile eavesdropper (E), and mobile relay (R). Figure 1 shows the system model.

First, MR receives the signal r_{SR} as

$$r_{\mathrm{SR}} = \sqrt{M_{\mathrm{SR}}KE}h_{\mathrm{SR}}x + w_{\mathrm{SR}}, \tag{1}$$

where w_{SR} is Gaussian noise.

In the second time slot, D and E receive the signals r_{Rk}, $k \in \{\mathrm{D}, E\}$, as

$$r_{Rk} = \sqrt{M_{Rk}E}h_{\mathrm{SR}}h_{Rk}x + w_{Rk}. \tag{2}$$

The received SNR $W_{\mathrm{SR}k}$ is given as

$$W_{\mathrm{SR}k} = \frac{W_{\mathrm{SR}}W_{Rk}}{1 + \overline{W_{\mathrm{SR}}} + W_{Rk}}, \tag{3}$$

where

$$\begin{aligned} W_{\mathrm{SR}} &= M_{\mathrm{SR}}K\left|h_{\mathrm{SR}}\right|^2\overline{\gamma}, \\ W_{Rk} &= (1-K)M_{Rk}\left|h_{Rk}\right|^2\overline{\gamma}, \\ \overline{W_{\mathrm{SR}}} &= M_{\mathrm{SR}}K\overline{\gamma}. \end{aligned} \tag{4}$$

$W_{\mathrm{SR}k}$ is very complex. We approximate $W_{\mathrm{SR}k}$ as [22]

$$\begin{aligned} W_{\mathrm{SRA}k} &= \frac{W_{\mathrm{SR}}W_{Rk}}{1 + \overline{W_{\mathrm{SR}}} + \overline{W_{Rk}}}, \\ \overline{W_{Rk}} &= (1-K)M_{Rk}\overline{\gamma}. \end{aligned} \tag{5}$$

Bloch et al. [23] give the instantaneous secrecy capacity as

$$\gamma = \max\{\ln(1 + W_{\mathrm{SRAD}}) - \ln(1 + W_{\mathrm{SRAE}}), 0\}. \tag{6}$$

3. Secure Data Transmission Quality Analysis

The probability of SPSC F_{SPSC} is used to evaluate the secure data transmission quality. We will give the analysis.

According to the (6), F_{SPSC} is given as

$$\begin{aligned} F_{\mathrm{SPSC}} &= \Pr(\gamma > 0) = 1 - \Pr(\gamma < 0) \\ &= 1 - \int_0^{\infty} F_{\mathrm{SRAD}}(W_{\mathrm{SRAE}}) f_{\mathrm{SRAE}}(W_{\mathrm{SRAE}}) dW_{\mathrm{SRAE}}. \end{aligned} \tag{7}$$

With the help of [24], we obtain the PDF and CDF of $W_{\mathrm{SRA}k}$ as follows:

$$f_{W_{\mathrm{SRA}k}}(r) = \frac{1}{16r}G_{0,4}^{4,0}\left[\frac{81r}{\chi_k}\Big|_{3,3,3,3}^{-}\right], \tag{8}$$

$$F_{W_{\mathrm{SRA}k}}(r) = \frac{1}{16}G_{1,5}^{4,1}\left[\frac{81r}{\chi_k}\Big|_{3,3,3,3,0}^{1}\right], \tag{9}$$

$$\chi_k = \frac{\overline{W_{\mathrm{SR}}W_{Rk}}}{1 + \overline{W_{\mathrm{SR}}} + \overline{W_{Rk}}} \tag{10}$$

Substituting (8) and (9) into (7), F_{SPSC} is expressed as

$$\begin{aligned} F_{\mathrm{SPSC}} &= 1 - \frac{1}{256} \times \int_0^{\infty} \frac{1}{W_{\mathrm{SRAE}}} G_{1,5}^{4,1}\left[\frac{81W_{\mathrm{SRAE}}}{\chi_D}\Big|_{3,3,3,3,0}^{1}\right] \\ &\quad \times G_{0,4}^{4,0}\left[\frac{81W_{\mathrm{SRAE}}}{\chi_E}\Big|_{3,3,3,3}^{-}\right] dW_{\mathrm{SRAE}} \\ &= 1 - \frac{1}{256}G_{5,5}^{4,5}\left[\frac{\chi_E}{\chi_D}\Big|_{3,3,3,3,0}^{1,-2,-2,-2,-2}\right]. \end{aligned} \tag{11}$$

4. Secure Data Transmission Quality Prediction Approach

4.1. Data Sets. $T_i = (X_i, y_i)$. The input X_i includes 5 indicators. X_i is given as

$$X_i = (x_{i1}, x_{i2}, \ldots, x_{i5}). \tag{12}$$

The output y_i is the SPSC. By using (11), the corresponding y_i can be obtained.

4.2. Network Design. Figure 2 shows the Elman neural network [25].

4.3. Predictive Evaluation. For PP testing data, MSE and AE are used to evaluate the prediction effect:

$$\begin{aligned} \mathrm{MSE} &= \frac{\sum_{z=1}^{PP}(d^z - y^z)^2}{PP}, \\ \mathrm{AE} &= \left|d^z - y^z\right|. \end{aligned} \tag{13}$$

5. Numerical Results

In this section, E = 1 and $\mu = W_{\mathrm{RD}}/W_{\mathrm{RE}}$ (in decibels).

With parameters in Table 1, we evaluate the SPSC performance with $\overline{\gamma} = 10$ dB in Figure 3. Simulation results show the following: (1) increasing u improves the SPSC

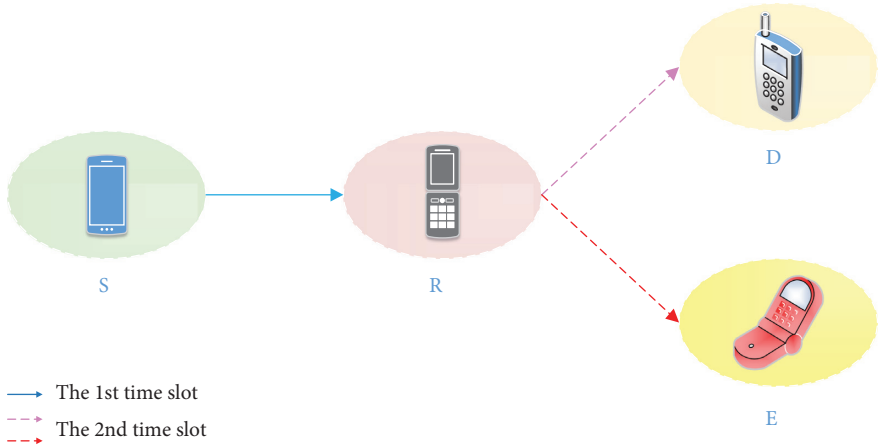

Figure 1: System model. E is the transmission power. For R and S, E is allocated with K. The channel coefficient h is 2-Nakagami distribution [20, 21]. M_{SR}, M_{RD}, and M_{RE} are the relative geometrical gains of S ⟶ R, R ⟶ D, and R ⟶ E links, respectively.

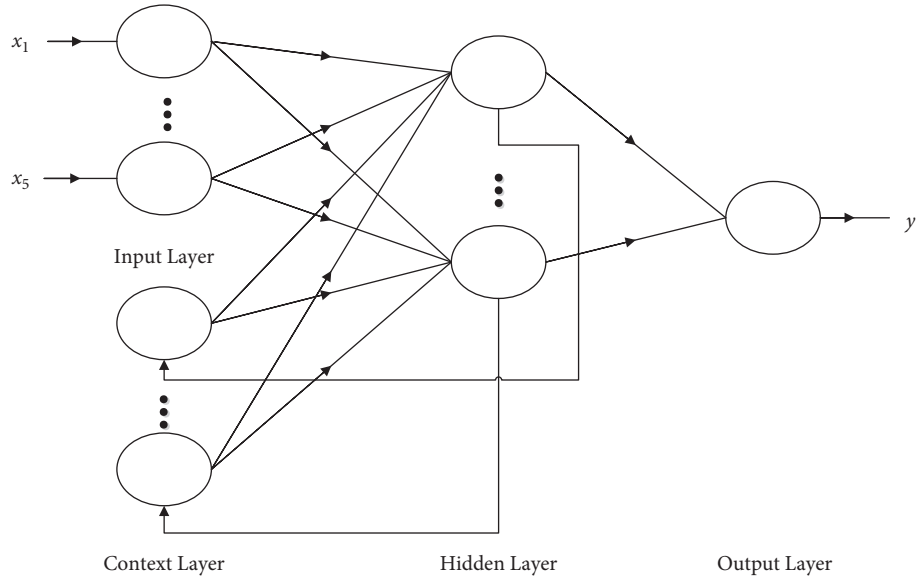

Figure 2: The Elman structure.

Table 1: Simulation parameters.

m_{SR}	1, 3
m_{RE}	1, 3
m_{RD}	1, 3
W_{SR}	5 dB
W_{RE}	5 dB
K	0.6

performance; (2) for Nakagami channels, the secure data transmission quality is the best. This is because a higher u improves the S ⟶ R⟶ D channel while degrading the S⟶R⟶E channel.

In Figures 4–11, ELM, GR, and RBF methods are compared with the Elman approach. Table 2 gives the simulation parameters. The MSE and AE of Elman approach are 0.00014 and 0.011, which are the lowest MSE and AE in the five methods. This is because Elman is a typical dynamic recurrent neural network and can adapt to the time-varying characteristics by adding a context layer.

The MSE is compared in Figure 12. Compared with GR, Elman has a better MSE performance, but the running time is longer than GR. Furthermore, compared with other methods, Elman has a higher quality precision and a lower time complexity.

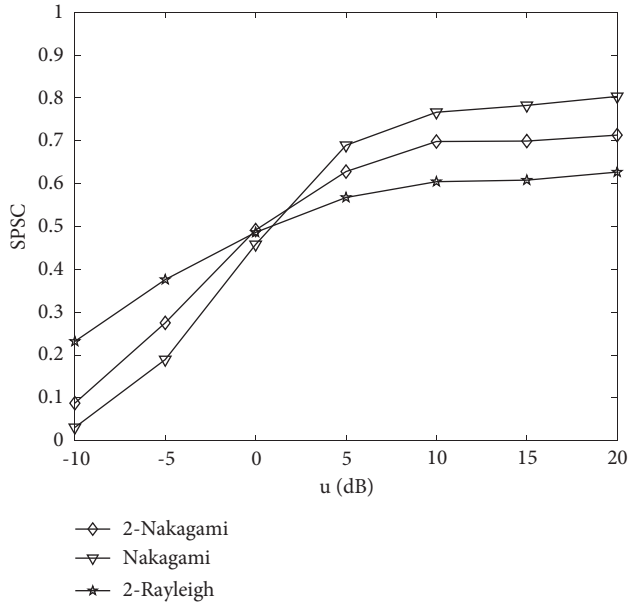

Figure 3: The SPSC performance versus u for different channels.

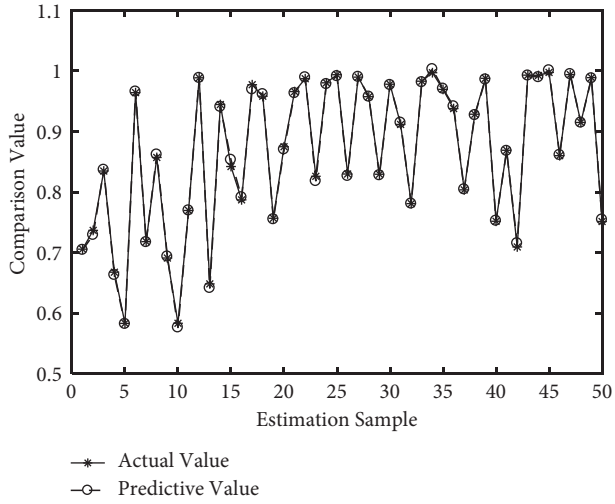

Figure 4: Prediction of elman.

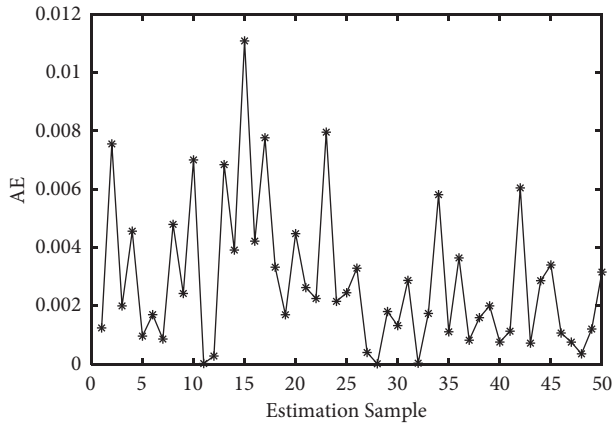

Figure 5: Ae of elman.

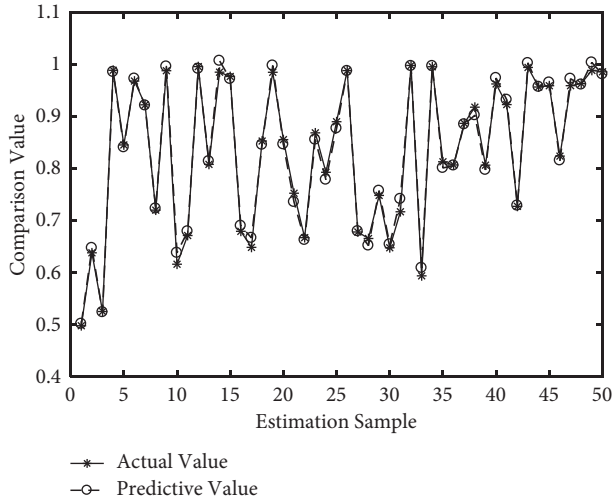

Figure 6: Prediction of RBF.

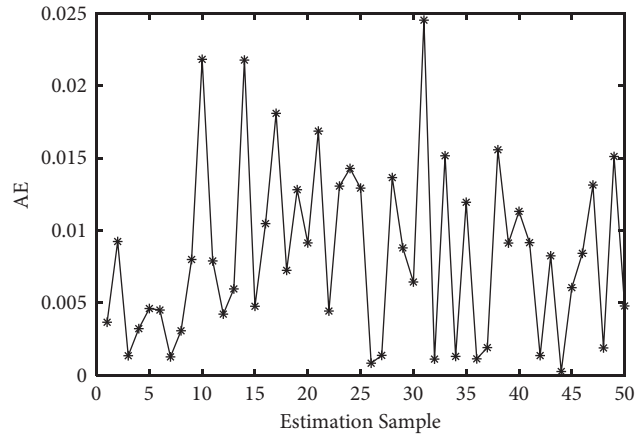

Figure 7: Ae of RBF.

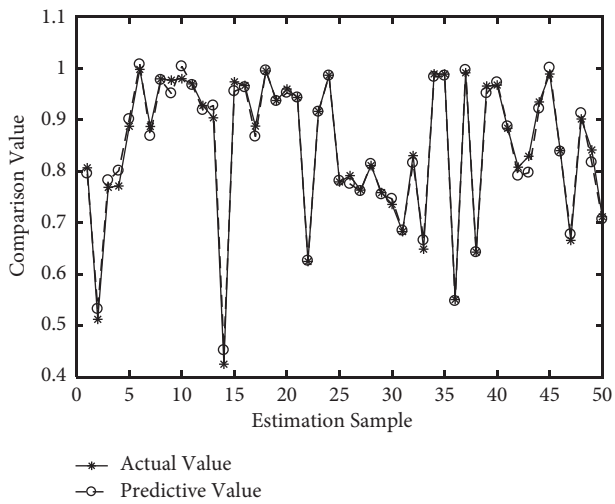

Figure 8: Prediction of ELM.

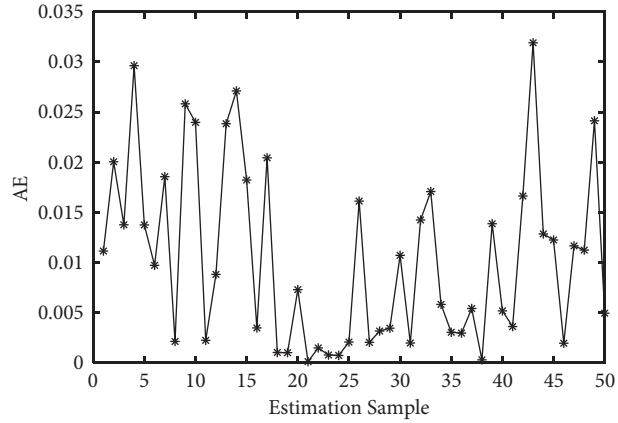

Figure 9: Ae of ELM.

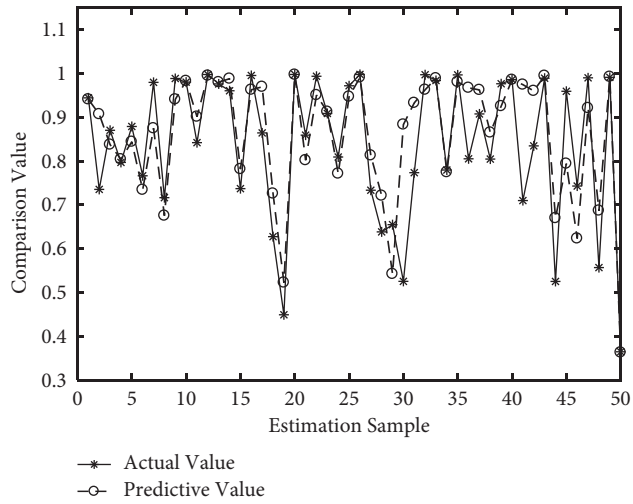

Figure 10: Prediction of GR.

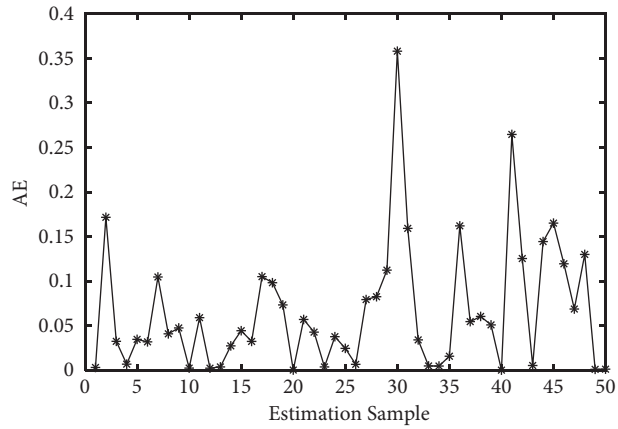

Figure 11: Ae of GR.

Table 2: The parameters for different methods.

Algorithm	Elman	ELM	RBF	GR
	Training data: 3000		Testing data: 50	
	q:10 η_1:0.01 η_2:0.01	q:15000	τ:20	τ:0.01

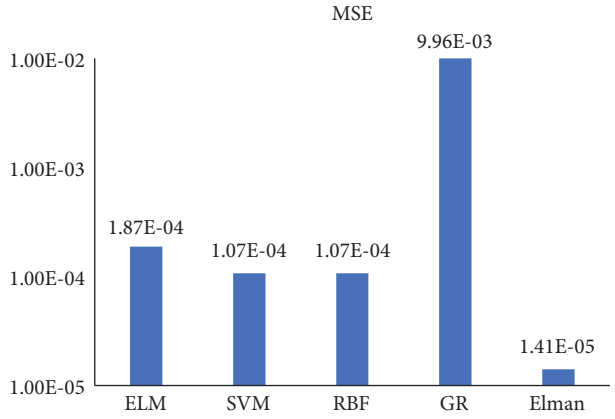

Figure 12: The MSE comparison.

6. Conclusion

This paper investigated the SPSC prediction of mobile IoT Networks. The exact expressions for SPSC were derived. Furthermore, based on the Elman network, we proposed an intelligent secure data transmission quality prediction algorithm. The theoretical analysis showed the following: (1) the SPSC performance over Nakagami channels was the best; (2) compared with different methods, the Elman algorithm can achieve a higher quality precision.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon reasonable request and with permission of funders.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (no. 11664043).

References

[1] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for the internet of vehicles towards intelligent transportation systems: a survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2021.

[2] L. Chettri and R. Bera, "A comprehensive survey on internet of things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.

[3] H. Wang, L. Xu, Z. Yan, and T. A. Gulliver, "Low-complexity MIMO-FBMC sparse channel parameter estimation for industrial big data communications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3422–3430, 2021.

[4] L. Xu, H. Wang, and T. A. Gulliver, "Outage probability performance analysis and prediction for mobile IoV networks based on ICS-BP neural network," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3524–3533, 2021.

[5] G. Liu, Y. Liu, K. Zheng et al., "MCS-GPM: multi-constrained simulation based graph pattern matching in contextual social graphs," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 6, pp. 1050–1064, 2018.

[6] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, pp. 2565–2578, 2019.

[7] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: a review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.

[8] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[9] Y. Chen, T. Zhang, X. Qiao, H. Wu, and J. Zhang, "Secure cognitive MIMO wiretap networks with different antenna transmission schemes," *IEEE Access*, vol. 9, pp. 5779–5790, 2021.

[10] L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent security performance prediction for IoT-enabled healthcare networks using improved CNN," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[11] L. Qing, H. Xiaomei, and X. M. Fu, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Communications Letters*, vol. 22, no. 9, pp. 1882–1885, 2018.

[12] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer

security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[13] K.-L. Besser and E. A. Jorswieck, "Bounds on the secrecy outage probability for dependent fading channels," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 443–456, 2021.

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

[15] H. Huang, Y. Peng, J. Yang, W. Xia, and G. Gui, "Fast beamforming design via deep learning," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1065–1069, 2020.

[16] J. Wang, L. Wu, H. Wang, K.-K. R. Choo, and D. He, "An efficient and privacy-preserving outsourced support vector machine training for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 458–473, 2021.

[17] C. Deng, Y. Han, and B. Zhao, "High-performance visual tracking with extreme learning machine framework," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2781–2792, 2020.

[18] L. Xu, H. Wang, H. Li, W. Lin, and T. A. Gulliver, "QoS intelligent prediction for mobile video networks: a GR approach," *Neural Computing & Applications*, vol. 33, no. 9, pp. 3891–3900, 2021.

[19] H. Wang, K. Liu, Y. Wu et al., "Image reconstruction for electrical impedance tomography using radial basis function neural network based on hybrid particle swarm optimization algorithm," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 1926–1934, 2021.

[20] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "N∗Nakagami: $N{\ast}$Nakagami: a novel stochastic model for cascaded fading channels," *IEEE Transactions on Communications*, vol. 55, no. 8, pp. 1453–1458, Aug 2007.

[21] Z. X. Li, L. Z. Jia, F. Li, and H. Y. Hu, "Outage performance analysis in relay-assisted inter-vehicular communications over double-Rayleigh fading channels," in *Proceedings of the CMC*, pp. 266–270, Shenzhen, China, September 2010.

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

[23] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic, San Diego, CA, USA, 7th edition, 2007.

[25] H. Y. Jin and X. M. Zhao, "Complementary sliding mode control via Elman neural network for permanent magnet linear servo system," *IEEE Access*, vol. 7, pp. 2169–3536, 2019.