Research Article

ASC Performance Prediction for Medical IoT Communication Networks

Fagen Yin, Pingping Xiao, and Zefeng Li

1 College of Physical Science and Engineering, Yichun University, Yichun 336000, Jiangxi, China
2 Institute of Data Science, City University of Macau, Macau 999078, Macau

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

Received 13 April 2021; Accepted 21 May 2021; Published 28 May 2021

Copyright © 2021 Fagen Yin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wearable devices are gradually entering the medical health field. Medical Internet of Things (IoT) has been widely used in all walks of medical health. With the complexity of medical health application scenarios, the medical IoT communication networks face complex environments. The secure communication issue is very important for medical IoT communication networks. This paper investigates the secrecy performance of medical IoT communication networks. To improve the secrecy performance, we adopt a cooperative communication strategy. We also use the average secrecy capacity (ASC) as a metric, and the expressions are first derived. Then, a secrecy performance intelligent prediction algorithm is proposed. The extensive simulations are used to verify the proposed method. Compared with other methods, the proposed algorithm realizes a better prediction precision.

1. Introduction

With explosive growth of medical health applications, the fifth-generation (5G) mobile communication has been widely used in medical Internet of Things (IoT) networks [1, 2]. Different 5G applications [3–5] widely appear in medical IoT communication networks, which can provide quick and convenient user experience and services [6]. However, due to the medical user mobility, the secure communication issue of medical IoT networks is facing many challenges [7].

For medical IoT communication networks, physical layer security is becoming more and more important [8]. With an eavesdropper, the authors [9] investigated the impact of antenna correlation. In [10], the authors developed a code scrambling scheme and analyzed secrecy performance. Considering the physical layer security, Yan et al. [11] studied the resource allocation problem for the cognitive relay networks. In [12], the authors proposed an optimal power allocation to achieve the secure transmission. Considering the cooperative jamming, Lu et al. [13] proposed a secure transmission scheme.

However, analyzing and predicting mobile secrecy performance are very difficult. Recently, machine learning techniques are applied in 5G wireless communications [14, 15]. In pattern classification, classifying the binary data was realized by the support vector machine (SVM) model in [16]. The extreme learning machine (ELM) model was proposed to detect anomaly states in [17]. In [18], the general regression (GR) model predicted the video transmission quality.

To date, no existing studies have considered the secrecy performance prediction of AF relaying medical IoT communication networks. As a consequence, we summarize the main contributions as follows:

1. The secrecy performance is analyzed with AF relaying scheme. Then, we use the average secrecy capacity (ASC) to evaluate secrecy performance and derive the exact expressions.

2. To realize real-time analysis of ASC, we propose an ASC prediction algorithm based on the BP network. ELM, SVM, and GR methods are examined and compared with the proposed method.
2. The Medical IoT Communication Network Model

In Figure 1, the medical IoT communication networks have a mobile source (MS), mobile eavesdropper (ME), mobile destination (MD), and mobile relay (MR). $W_{SR}$, $W_{RD}$, and $W_{RE}$ are the relative geometrical gains of MS $\rightarrow$ MR, MR $\rightarrow$ MD, and MR $\rightarrow$ ME links, respectively.

Transmission power is $E$, which is allocated by $K$. 2-Rayleigh distribution can express the channel coefficient $h$ \cite{19}.

Firstly, MR receives the signal $r_{SR}$ as \cite{20}

$$r_{SR} = \sqrt{W_{SR}}KEh_{SR}x + n_{SR},$$ \hspace{1cm} (1)

where $n_{SR}$ is Gaussian noise.

In the second time slot, AF is used at MR. MD and ME receive the signals $r_{RD}$, $k\in$\{D, E\}, as

$$r_{RD} = \sqrt{c}Eh_{RD}h_{SR}x + n_{RD}.$$ \hspace{1cm} (2)

The received SNR $\gamma_{SRA_k}$ is given as

$$\gamma_{SRA_k} = \frac{\gamma_{SRA_k}}{1 + \gamma_{SR} + \gamma_{Rk}},$$ \hspace{1cm} (3)

where

$$\gamma_{SR} = W_{SR}K|h_{SR}|^2\chi,$$ \hspace{1cm} (4)

$$\gamma_{Rk} = (1 - K)W_{RK}|h_{Rk}|^2\chi,$$ \hspace{1cm} (5)

$$\overline{\gamma_{SR}} = W_{SR}K\chi.$$ \hspace{1cm} (6)

\[\gamma_{SRA_k}\] is hard to calculate exactly. We approximate $\gamma_{SRA_k}$ as \cite{21}

$$\gamma_{SRA_k} = \frac{\gamma_{SRA_k}}{1 + \gamma_{SR} + \gamma_{Rk}},$$ \hspace{1cm} (7)

$$\overline{\gamma_{Rk}} = (1 - K)W_{RK}\chi.$$ \hspace{1cm} (8)

With the help of \cite{22}, the PDF and CDF of $\gamma_{SRA_k}$ are as follows:

$$f_{\gamma_{SRA_k}} = \frac{1}{\chi_k^4}G_{0.4}^4\left[\frac{r}{\chi_k}, 1, 1, 1, 1\right],$$ \hspace{1cm} (9)

$$F_{\gamma_{SRA_k}} = G_{1.4}^4\left[\frac{r}{\chi_k}, 1, 1, 1, 1, 0\right],$$ \hspace{1cm} (10)

where

$$\chi_k = \frac{\gamma_{SR}\gamma_{Rk}}{1 + \gamma_{SR} + \gamma_{Rk}}.$$ \hspace{1cm} (11)

The instantaneous secrecy capacity is given as \cite{23}

$$C = \max \left[\ln \left(1 + \gamma_{SRA_D}\right) - \ln \left(1 + \gamma_{SRA_E}\right)\right].$$ \hspace{1cm} (12)

3. Average Secrecy Capacity

The ASC is derived as

$$\overline{C} = \int_0^\infty \int_0^\infty C(\gamma_{SRA_D}, \gamma_{SRA_E})f(\gamma_{SRA_D}, \gamma_{SRA_E})d\gamma_{SRA_D}d\gamma_{SRA_E} = A_1 + A_2 - A_3.$$ \hspace{1cm} (13)

$A_1$ is given as

$$A_1 = \int_0^\infty \frac{1}{\gamma_{SRA_D}}G_{1.2}^{1.2}(\gamma_{SRA_D}, 1, 0, 1)G_{0.4}^{4.0}\left[\gamma_{SRA_D}, 1, 1, 1, 1\right]G_{1.4}^{4.1}\left[\gamma_{SRA_D}, 1, 1, 1, 0\right]d\gamma_{SRA_D}.$$ \hspace{1cm} (14)
We obtain the $A_2$ as

\[
A_2 = \int_0^\infty \frac{1}{G_{2,2}^{1,2}(\gamma_{\text{SRAE}}|1,0,1,1)} \frac{1}{\gamma_{\text{SRAE}}} G_{0,4}^{1,0} \left[ \frac{\gamma_{\text{SRAE}}}{\chi_E} \right] G_{1,5}^{1,1} \left[ \frac{\gamma_{\text{SRAE}}}{\chi_D} \right] d\gamma_{\text{SRAE}}
\]

\[
= G_{2,2}^{2,1; 4,0; 4,1} \begin{bmatrix} 0,1 & - & 1 \\ 0,0 & 1,1,1,1 & 1,1,1,1,0 \end{bmatrix}.
\]

We obtain the $A_3$ as

\[
A_3 = \int_0^\infty \frac{1}{\gamma_{\text{SRAE}}} G_{2,2}^{1,2}(\gamma_{\text{SRAE}}|1,0,0) G_{0,4}^{1,0} \left[ \frac{\gamma_{\text{SRAE}}}{\chi_E} \right] G_{2,6}^{1,1} \left[ \frac{1}{\chi_E} \right] d\gamma_{\text{SRAE}} = G_{2,6}^{1,1} \left[ \frac{1}{\chi_E} \right]_{1,1,1,1,0,0,1}.
\]
Next, we use the derived ASC expressions to set up the data sets and design the BP prediction model.

4. Secrecy Performance Prediction Method

4.1. Data Sets. $T_i = (X_i, y_i)$. $X_i$ is given as:

$$X_i = (x_{i1}, x_{i2}, \ldots, x_{i5}).$$  \tag{17}

$X_i$ includes 5 indicators, which are $W_{SR}$, $W_{RD}$, $W_{RE}$, $K$, and $\gamma$. The ASC performance is the output $y_i$. By using (13), it can obtain the corresponding $y_i$.

4.2. Network Structure. Figure 2 shows the BP structure [24].

4.3. Metrics. Two metrics are MSE and AE. For PP testing data, they are given as:

$$MSE = \frac{\sum_{c=1}^{PP} (d^2 - y^2)^2}{PP},$$  \tag{18}

$$AE = |d^2 - y^2|. \tag{19}$$

Table 1: Simulation parameters.

| Parameter | Value |
|-----------|-------|
| $m$       | 1, 2, 3 |
| $K$       | 0.4   |
| $W_{SR}$  | 5 dB  |
| $W_{RE}$  | 5 dB  |

Figure 4: Prediction of BP.

Figure 5: AE of BP.

Figure 6: Prediction of ELM.

Figure 7: AE of ELM.
Figure 8: Prediction of SVM.

Figure 9: AE of SVM.

Figure 10: Prediction of GR.
5. Simulation Analysis

Here, $E = 1$, and $\mu = \frac{W_{RD}}{W_{RE}}$ (in decibels).

For different channels, we evaluate the ASC performance with $\bar{y} = 10$ dB in Figure 3. The parameters are given in Table 1. The following observations can be made: (1) increasing $\mu$ improves the ASC performance; (2) the 2-Rayleigh model can obtain the best ASC performance among the three channels.

In Figures 4–13, we consider SVM, ELM, GR, and RBF [25] methods to compare with the BP network. Table 2 gives the simulation parameters. The MSE and AE of BP are 0.000232889 and 0.04324, which are the lowest MSE and AE in the five methods. This is because BP has the ability to adapt to the time-varying characteristics and enhance the global stability. It has more computing power than other four methods and can be used to solve the rapid optimization problem.

6. Conclusion

An AF relaying scheme was used to improve the ASC performance of medical IoT communication networks in this paper. The ASC expressions were derived. Furthermore, we proposed an intelligent prediction algorithm based on the BP network. The simulation results show that (1) as the $\mu$ increases, the system’s ASC performance becomes better and (2) compared with SVM, ELM, GR, and RBF methods, the proposed BP algorithm can obtain a better MSE and AE.

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

References

[1] R. Cao, Z. Tang, C. Liu, and B. Veeravalli, "A scalable multicloud storage architecture for cloud-supported medical Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1641–1654, 2020.
[2] 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.

[3] D. Meng, X. Wang, M. Huang, L. Wan, and B. Zhang, “Robust weighted subspace fitting for DOA estimation via block sparse recovery,” *IEEE Communications Letters*, vol. 24, no. 3, pp. 563–567, 2020.

[4] X. Wang, L. Wan, M. Huang, C. Shen, Z. Han, and T. Zhu, “Low-complexity channel estimation for circular and non-circular signals in virtual MIMO vehicle communication systems,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 3916–3928, 2020.

[5] X. Wang, M. Huang, and L. Wan, “Joint 2D-DOD and 2D-DOA estimation for coprime EMVS-MIMO radar,” *Circuits, Systems and Signal Processing*, vol. 40, no. 6, pp. 2950–2966, 2021.

[6] C. W. Chen, “Internet of video Things: next-generation IoT with visual sensors,” *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6676–6685, 2020.

[7] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, “A secure IoT-based modern healthcare system with fault-tolerant decision making process,” *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 3, pp. 862–873, 2021.

[8] 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.

[9] M. Torabi and D. Haccoun, “Impact of antenna correlation on the physical layer security of cooperative relaying with OSTBC system,” *IET Communications*, vol. 14, no. 19, pp. 3472–3479, 2020.

[10] S. Park and H. Son, “Near-Perfect code scrambling with limited key information for wiretap channels,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13410–13423, 2020.

[11] W. Yang, X. Zhao, and J. He, “Physical layer security and energy efficiency driven resource optimisation for cognitive relay networks,” *IET Communications*, vol. 14, no. 17, pp. 2953–2961, 2020.

[12] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, “Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13005–13017, 2020.

[13] X. Lu, W. Yang, X. Guan, and Y. Cai, “DCE-based secure transmission for massive MIMO relay system Against active eavesdropper,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13045–13059, 2020.

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

[16] X. J. Peng, “A spheres-based support vector machine for pattern classification,” *Neural Computing & Applications*, vol. 31, no. 1, pp. 379–396, 2019.

[17] T. Wu, W. L. Xue, H. Z. Wang et al., “Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1892–1904, 2021.

[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 and Applications*, vol. 33, no. 9, pp. 3891–3900, 2021.