Intelligent and Converged Networks ISSN 2708-6240
2023, 4(4): 313−325 DOI: 10.23919/ICN.2023.0026

CNNs-based end-to-end asymmetric encrypted communication system

Yongli An, Zebing Hu, Haoran Cai, and Zhanlin Ji*

Abstract: In this paper, we propose an asymmetric encrypted end-to-end communication system based on convolutional neural networks to solve the problem of secure transmission in the end-to-end wireless communication system. The system generates a key generator through a convolutional neural network as a bridge. The private and public keys establish a key pair relationship of arbitrary length sequence information. The transmitter and receiver consist of autoencoders based on convolutional neural networks. For data confidentiality requirements, we design the loss function of the end-to-end communication model based on a convolutional neural network. We also design bugs based on different predictions about the information the system eavesdropper has. Simulation results show that the system performs well on additive Gaussian white noise and Rayleigh fading channels. A legitimate party can establish a secure transmission under a designed communication system; an illegal eavesdropper without a key cannot accurately decode it.

Key words: end-to-end communication system; convolutional neural network; asymmetric encryption; loss function; physical layer security

1 Introduction

With the continuous progress of science and technology, wireless communication technology has also experienced rapid development, especially the application of mobile communication technology represented by 5G, which marks an unprecedented change in the field of information dissemination[1, 2]. With the continuous improvement of living standards, people will have higher and higher requirements for wireless communication, which makes the security of wireless communication systems a very challenging task.

The communication system divides the transmitter and receiver into several submodules, each independent of the others and each with a separate objective function. The advantage of this design approach is that each component can be optimized separately, resulting in today's reliable modular communication systems[3]. With the emergence of deep learning concepts, deep neural networks have started to be applied by research workers in wireless communications for physical layer design, including channel estimation[4], signal detection[5], feedback and reconstruction of channel state information[6], channel coding and decoding[7], and end-to-end communication systems, and some results can meet or even surpass the performance of traditional communication algorithms.

Unlike traditional communication systems, deep learning based end-to-end communication goes back to the essence of communication: transferring information from one end to the other. During the design of the end-to-end communication system, each module will no longer be designed and tuned separately. Instead, the communication system is considered as a whole, and the sender and receiver are jointly trained to optimize the system's performance as a whole, which is a new communication system optimization idea different from the modular design[8–13]. In Ref. [14], it was first proposed to use the neural network in deep

• Yongli An, Zebing Hu, Haoran Cai, and Zhanlin Ji are with College of Artificial Intelligence, North China University of Science and Technology, Tangshan 063210, China. E-mail: anyl@ncst.edu.cn; huzebing2021@gmail.com; caihaoran69@gmail.com; zhanlin.ji@gmail.com.
* To whom correspondence should be addressed.
Manuscript received: 2023-04-03; accepted: 2023-07-13

learning to construct an end-to-end communication system. The author can obtain a higher performance limit by training the communication system based on the autoencoder (AE) through end-to-end learning. But for communication systems, it is not enough to guarantee their reliability and effectiveness; if the security of their communication cannot be guaranteed, then the whole communication process may be meaningless[15].

Many researchers and scholars have explored and established appropriate security strategies to ensure the successful operation of communication systems. On the one hand, the physical layer security of communication uses the randomness of the transmission medium to achieve secure transmission and secure authentication during communication, i.e., its security is independent of the computing resources of the illegals[16–18]. Another aspect of the algorithm for secure encryption based on the physical layer is based on the characteristics of the wireless propagation channel or the characteristics of the transceiver. The common denominator of these characteristics is that they have a certain degree of randomness and independence. However, the encryption algorithm requires the emergence of quantum computers with supercomputing power whose security can be guaranteed[19, 20]. Also, the application of security mechanisms for protecting wireless communication systems through combining neural networks and cryptography continues to rise. Reference [21] proposes a symmetric cryptographic design method for neural networks, and the high-performance data encryption method is a new attempt to apply the parallel processing power of neural networks to cryptography. The authors of Ref. [22] demonstrated that neural networks could learn how to perform various forms of encryption and decryption to protect information from other neural networks without the need to prescribe specific encryption algorithms to these neural networks. The authors of Ref. [23] studied the endogenous security of end-to-end learning communication, redesigned the loss function of a deep learning communication model based on autoencoders, and proposed the use of noise-reducing autoencoders for authentication, a new deep learning approach to reconstruct the physical layer security framework for wireless communication. Reference [24] proposes end-to-end learning of a finite-length code for Gaussian eavesdropping channels. Communication security is measured based on the mutual information between messages and the eavesdropper Eve's observations using mutual information neural estimation (MINE). In Ref. [25], authors proposed to mention a symmetric encrypted end-to-end communication system based on deep convolutional generative adversarial networks to solve the security problem of transmission in end-to-end based wireless communication systems. However, it is difficult for key resource management. At the same time, the information transmitted in the communication system, secret documents make up a large part of it. Attacks and theft by illegal users of communications can be of great benefit when the communicator does not take appropriate measures[26, 27].

So far, few studies have paid attention to wireless communication system encryption security based on end-to-end learning. Security is an important performance evaluation index of wireless communication systems. Whether the information transmission of the communication system can get enough security protection is an essential condition for the existence and application of the communication system. The research in this thesis focuses on combining end-to-end communication systems with cryptography to achieve wireless communication security.

In this thesis, we construct a convolutional neural network (CNN)-based key generator, combine the key generator with an AE network based on CNNs, and design a CNNs-based end-to-end asymmetric encrypted communication system (CAE-E2E). The system uses CNNs to complete the entire communication process, and the specific contributions are as follows:

(1) To alleviate the critical dimensionality nuisance, CNNs are used as key generators. The "black box" nature of the neural network is combined with the key pair to create an imaging relationship to improve further the stability and flexibility of the generated key

pair.

(2) Based on exploring the security of the end-to-end encryption system, the loss function of the end-to-end encryption system based on CNNs is designed to improve further the endogenous safety of the signal transmitted by the transmitter in the system.

(3) The carefully designed CNNs-based end-to-end asymmetric encryption system for the eavesdropping problem in wireless communication systems further optimizes the information encryption key management. Communication system simulation experiments on additive white Gaussian noise channel (AWGN) and Rayleigh channel. Encrypted systems have bit error rate (BER) performance similar to that of traditional communication systems. The proposed CAE-E2E system has superior performance in terms of anti-eavesdropping security compared with the symmetric encrypted end-to-end communication system (SE-E2E) with randomly generated keys.

2 Basic theory

Artificial neural networks (ANN) model the relationship between a set of input information and a collection of output information, using models derived from the human brain's understanding of how stimuli from sensory inputs are responded to. The neuron is the most basic unit of a neural network. In the neural network model, after the input signal $x_1, x_2, ..., x_n$ and parameter b are passed into the neuron, each input signal corresponds to the weight parameter $w_1, w_2, ..., w_n$, and then linearly combined with the model parameters in the neuron, and then output through the activation function (f) to become the next input $h_{w,b}(x)$ of the layer neuron. Different connection methods and different parameter settings of neurons constitute various neural networks. The neuron model is shown in Fig. 1.

With the booming field of information security, data in transit is prone to severe security-level issues such as leakage, tampering, and repudiation. The purpose of information encryption research is to ensure the need for data confidentiality. With the development of deep learning and cryptography, intelligent cryptography will be the future trend of cryptographic

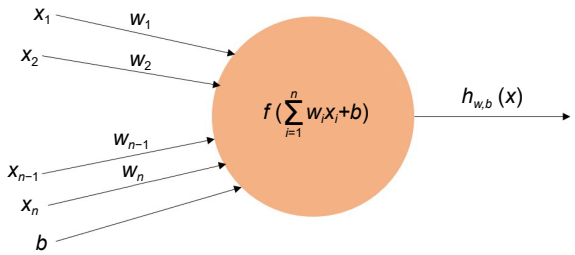


Fig. 1 Neuron model.

communication. Diffie and Hellman[28] first introduced the idea of the public-key cryptosystem, which is mainly used to solve the symmetric cryptosystem key distribution and management problems. The most crucial feature of asymmetric cryptosystems is that the encryption and decryption keys differ. The key in asymmetric encryption consists of a public key and a private key pair, and the two keys in the critical team have a very close relationship (mathematical relationship).

The convolutional neural network is an input-to-output mapping, which can learn many mapping relationships between input and output. The multi-level structure realizes the dimensionality reduction of the data, combining low-level local features into higher-level features. By utilizing convolutional and pooling layers to process the input data, CNNs can learn complex features from the input. These properties are precisely what are needed to generate high-quality key pairs. The security of the key depends on the difficulty of the reverse derivation of the CNNs model. The generation of the seed private key is omitted, and the CNNs are used as the key generator to establish the key pair relationship (private key and public key) of sequence information of any length.

As shown in Fig. 2, the sender encrypts the message with the public key, and the receiver decrypts the ciphertext with the private key. The decryption key must never be made public, and legitimate recipients can only use the private key. During the encryption process, there is no need to distribute the key for decryption to the receiver, thus solving the problem of information public transmission and key distribution. In an asymmetric system, the private key generates the public key according to specific rules, and the mathematically complex problem of reversely deriving

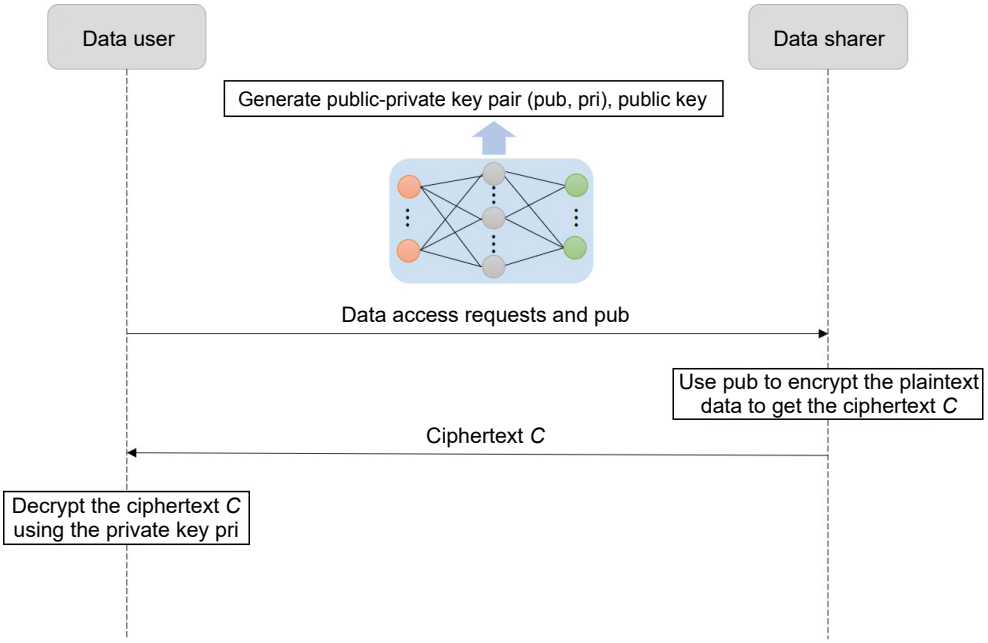


Fig. 2 Asymmetric encryption of data.

the private key from the public key represents the algorithm's security. Generally speaking, deriving the private key from the public key consumes a large amount of computing resources, which is not feasible under the current computing background, thereby ensuring data security.

3 End-to-end learning confidential communication mechanism

3.1 Asymmetric encrypted communication model

Wireless communication networks mainly use protection mechanisms based on symmetric and asymmetric encryption. An asymmetric encrypted end-to-end communication system based on neural networks is proposed to improve the transmission security of end-to-end communication systems (see Fig. 3).

The model is based on the TensorFlow deep learning framework to build an end-to-end communication system based on CNNs. CNNs are used instead of senders, receivers, and eavesdroppers. The trained key generator is combined with the AE network based on CNNs, and the key is shared with the transmitter and

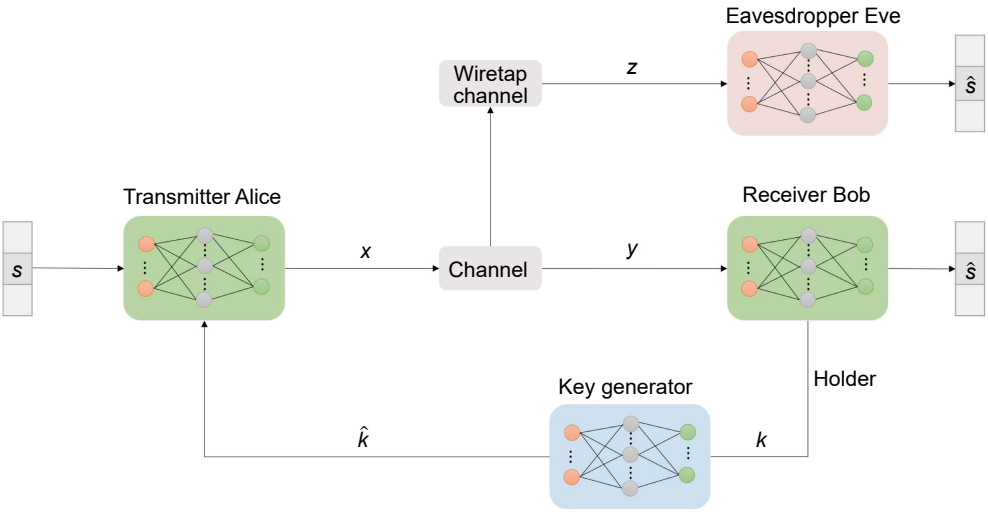


Fig. 3 Asymmetric encrypted communication model.

receiver (the private key holder is the receiver, and the public key is generated by the key generator and sent to the transmitter).

Input the binary code element private key k (omitting the generation of the seed key) to the key generator to generate the public key $\widehat{k}$. The original transmission message s is a randomly generated binary code word. The message s and the public key $\widehat{k}$ pass through the neural network encoder corresponding to the image function $x = F(s,\widehat{k})$ conforming to the transmission condition of the transmit signal x. $x \in \mathbb{R}^n$ occupies n channel time slots. The power normalization layer at the transmitter side imposes a power constraint on x. The transmit signal x passes through the channel described by the conditional probability density function $p(y|x)$. $y \in \mathbb{C}^n$ indicates the received signal. An additive noise layer with a fixed variance $\sigma_1 = (2RE_b/N_0)^{-1}$ represents the channel. The noise is denoted by w, and the received signal is $y = x + w$. The received signal z works in the same way as y. $R = k/n$ indicates the code rate, and E_b/N_0 represents the energy per bit (E_b) ratio to the noise power spectral density (N_0). The receiver connects the received signal y with the private key k and then performs decryption and decoding operations. Optimization is performed by end-to-end reconstruction to minimize the error between the reconstructed information $\widehat{s}$ and the transmitted initial information s.

3.2 Loss function design of the encryption system

The secure transmission of the end-to-end communication system is composed entirely of neural networks, and the parameters in the neural networks are wholly obtained by end-to-end training. This system neural network parameter optimization scheme uses gradient backpropagation to adjust the model's parameters in the negative direction of the gradient. In order to be able to obtain the angles of each parameter in the model, the model's loss function needs to be constructed first, and the upper limit of the model's performance is established by the gradients calculated from the loss function of the model. Therefore, the model can be adapted to learn specific features by adjusting the learning objectives and enabling it to incorporate certain features to give it unique characteristics. The model is implicitly encrypted by using some parts, and the output of the model also includes the elements of model learning; that is, the system itself has specific security. We propose to design the communication system's loss function applicable to this system's secure transmission technique.

The loss function of the end-to-end communication system is mainly composed of two parts, the receiver (Bob), and the eavesdropper (Eve). The specific composition of the system loss function is described in detail next. For Bob, the goal is to restore the code word sent by the sender (Alice) as accurately as possible. For Bob, whose main guarantee is communication reliability, the cross-first loss function of the deep learning classification task is used as Bob's loss function. The specific expressions are as follows:

$$l_{\text{Bob}} = \sum_{i=1}^{n} x_i \log(y_i^m) \tag{1}$$

Note that x is the symbol for Alice to send the message. x_i is the i-th element of x. y_m is the vector output by the neural network model of the signal received by Bob (the output vector of the signal through the main channel). y_i^m is the i-th element of y^m.

For Eve, the goal of implementing secure transmission is to make it as difficult as possible for Eve to recover the original message sent by Alice accurately. A loss function opposite to Bob's can be used as Eve's loss function. However, in terms of the physical meaning represented by Bob's loss function, its purpose is to allow the receiver to maximize the probability of sending the class to which the code word belongs. If Eve only adopts the opposite loss function to Bob as her own, it is equivalent to the fact that for Eve, the probability of sending the class to which the codeword belongs is minimized at the receiving end. Assume an ideal situation where the model can be optimized precisely according to Eve's loss function, the model has probability 0 for all sent signal genera if Eve does not use the class with the highest probability as the class for sending signals as usual. Instead, the type with the lowest chance is used for sending alerts.

Then Eve can fully recover all the signals sent, and the system's security will no longer exist. For this, we redesign the loss function of the eavesdropper, the first part of the Eve loss function:

$$l_{\text{Eve}}^{1} = -\sum_{i=1}^{n} x_i \log(z_i^m) \tag{2}$$

Note that z^m is the vector output by the neural network model of the receiving end of the signal received by Eve (the output vector of the signal passing through the main channel and the eavesdropping channel). z_i^m is the i-th element of z^m.

It is imperative to improve the loss function of Eve further, as only Eq. (2) is used as the loss function of Eve, which may lead to failure in achieving secure transmission of the system in some cases. Reference [29] shows that the method comprises a transmitter, a channel, and a receiver to the Shannon information theory. The transmitter generates the message sent, the channel modifies the message somehow, and the receiver tries to infer which message is sent. According to the analysis of Shannon information theory, the greater the information entropy of the probability vector output by the eavesdropper Eve receiver, the higher the security transmission of the system. We increase the randomness of information by improving Eve's loss function to achieve more secure communication transmission.

l_{Eve}^{2} in Eq. (3) denotes the variance of the output probability vector, and the conflict can be used to describe the distribution of the data somewhat. The smaller the clash, the tighter the data distribution and the more likely the data will converge. l_{Eve}^{3} in Eq. (4) represents the polar deviation of the output probability vector. The opposite variation means the distance between the maximum and minimum values in the data, which can reflect the overall distribution interval of the data. When the extreme difference is minor, the data are more tightly distributed. In the end-to-end communication model, minimizing several variables mentioned above is the essence of constraining the entropy value of Eve's output probability vector so that Eve gets less effective information in recovering the message sent by Alice.

$$l_{\text{Eve}}^{2} = \sum_{i=1}^{n} (z_i^m - u)^2, u = \frac{1}{n}\sum_{i=1}^{n} z_i^m \tag{3}$$

$$l_{\text{Eve}}^{3} = \max(z_i^m) - \min(z_i^m) \tag{4}$$

The analysis yields a loss function based on the secure transmission model of the end-to-end communication system. Still, to obtain the final optimized model, the corresponding model training method needs to be set to make the model achieve the expected results. The loss function of the system model can be divided into two main parts: l_{Bob} and l_{Eve}. After constructing the system model and the system loss function, the training and optimization of the model begin. For the composition of the model's loss function, it is easy to think of two training methods: unified training and iterative training. Unified training means combining l_{Bob} and l_{Eve} into the system's loss function to optimize the entire system's parameters. Iterative training means using l_{Bob} and l_{Eve} as two loss functions. First, use l_{Bob} as the system loss function for training optimization, then l_{Eve} as the system loss function to perform several optimization steps, and iteratively proceed until the system finally converges. For the training method of iterative training, different hyperparameters are tried to be adjusted in the experiment, and ultimately a more desirable result cannot be achieved. Therefore, in this paper, uniform training of the model training is used, i.e., the final loss function of the model is

$$l_{\text{Eve}} = l_{\text{Eve}}^{1} + l_{\text{Eve}}^{2} + l_{\text{Eve}}^{3} \tag{5}$$

$$\text{loss} = l_{\text{Bob}} + l_{\text{Eve}} \tag{6}$$

4 End-to-end learning of the performance of secure communication mechanisms

4.1 System architecture

The essence of the convolutional neural network is a multi-layer perceptron, and its advantage lies in local connection and weight sharing. According to Ref. [30], it is proposed that hidden layers play a crucial role in the performance of neural networks. The model is built by exploring the effect of the number of layers on the model's performance. It is understood that increasing

the number of hidden layers in a neural network can reduce network errors and improve accuracy. Still, it also makes the network model more complex, thus increasing the network training time and the possibility of overfitting. Based on the simulation experiment results, an end-to-end asymmetric encryption neural network is built in Table 1.

4.2 Communication system index evaluation

The asymmetric encrypted end-to-end communication system is extended to perform performance analysis under the AWGN and Rayleigh channels. After constructing the overall network model and loss function, the model's training can be started. The training and testing of the models are done separately. First, the system model is trained, and its network parameters are saved. The data is tested by loading the parameters retained during training.

The training process of the neural network minimizes the loss function by continuously adjusting the size of the weights, which eventually makes the network highly accurate. We expect the asymmetric encryption end-to-end system to use computer numerical computation through a deep learning optimizer to obtain the network parameters that minimize the designed loss function. The goal of choosing the most appropriate optimizer is not to get the highest accuracy but to minimize the training required by the neural network to achieve a given accuracy. We discuss the optimizers of the loss function applicable to the design of this system, comparing the standard optimizers, Adam, BGD, AdaGrad, and RMSprop, under different channels. Loss is the penalty for poor prediction. Loss is a numerical value that indicates the accuracy of the model prediction for a single sample. If the model's prediction is entirely accurate, the loss will be zero; otherwise, the loss will be significant. In this regard, the models trained by different optimizers are drawn based on the loss curves. Therefore the loss curve draws the model trained by different optimizers.

As shown in Fig. 4, when using Adam and RMSprop as optimizers in the AWGN and Raleigh channels, they converge at similar speeds, and the loss value always stays around 0. BGD and AdaGrad do not converge after the epoch reaches 1000, and the two optimizers under the Raleigh channel are close to the same. With

Table 1 CNNs model parameters.

Type of layer		Kernel size/annotation	Activation function
Key generator	Conv1D	5	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	None
Transmitter	Conv1D	5	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Normalization	Power normalization	None
Receiver	Conv1D	5	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	Relu
	Conv1D	3	Sigmoid

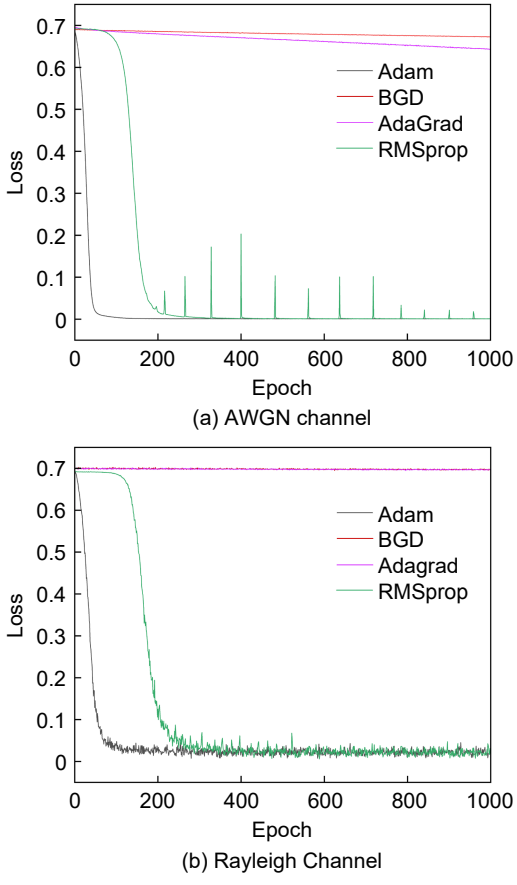


Fig. 4 Model loss for different optimizers.

gradient sparsification in model training, Adam has a more stable performance effect than RMSprop in terms of the overall magnitude of the loss curve and minimizes the loss function more quickly. Therefore, Adam is chosen as the optimizer for training this neural network.

Before training the asymmetric encryption end-to-end model, we set the hyperparameters of the neural network as in Table 2. The next question that needs to be discussed is whether the ideal model can be obtained when training its end-to-end communication system with other consistent training parameters.

As shown in Fig. 5, the loss function converges faster as the number of training iterations for different channel communication systems increases. The loss curve gradually smoothes out, with fluctuations but remains stable overall. The neural network can correctly receive the features of the signal and decode it correctly. The designed end-to-end communication encryption system based on CNNs has good generalization ability.

Table 2 Model training hyperparameters.

Parameter	Value	
	AWGN	Raleigh
Learning rate	1×10^{-4}	
Optimizer	Adam	
Block size	160	
Number of epochs	3500	6000

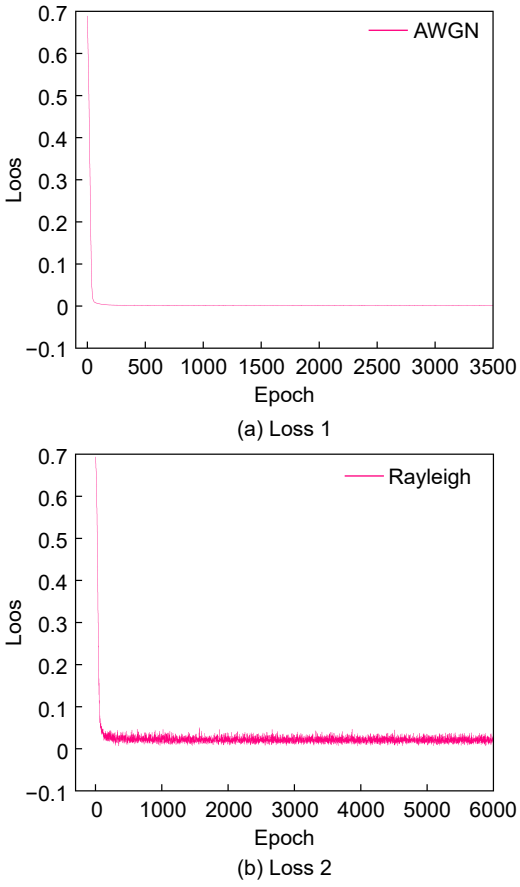


Fig. 5 System performance evaluation.

4.3 System BER performance simulation

In this paper, block error rate (BLER) is used as a metric to measure the performance of asymmetric encrypted end-to-end communication systems to analyze the performance of the communication system. The BLER is the probability that the output of the receiver is not equal to the sent message, which can be expressed as

$$\mathrm{BLER} = \frac{1}{M}\sum_{s} \mathrm{pr}(\hat{s} \neq s) \tag{7}$$

Note that M is the number of test data, and pr indicates the accuracy rate of the transmitted signal to the received signal. In deep learning-based communication systems, BLER and BER are the same and are uniformly referred to as BER in the following.

To simulate the communication system performance, we all choose the signal-to-noise ratio (SNR) that can be considered normalized. The purpose of communication is to transmit valid information. Given the channel conditions, we always want to spend the least amount of energy per bit on average, regardless of the modulation method and the error correction code used by the system. So we always choose BER for simulation and comparison.

As shown in Fig. 6, the horizontal axis of the plot is the different signal-to-noise ratios E_b/N_0 in dB, and the vertical axis is the BER. The parameter R in a CNNs-based end-to-end communication system is the message transmission rate, $R=k/n$. There are two reasons for setting the signal-to-noise ratio to a numerical value: first, if the signal-to-noise ratio is set too high, the generalization ability of the network will be limited, causing the variance of the neural network to be too high; second, if the signal-to-noise ratio is set too low, the influence of noise on the input signal will

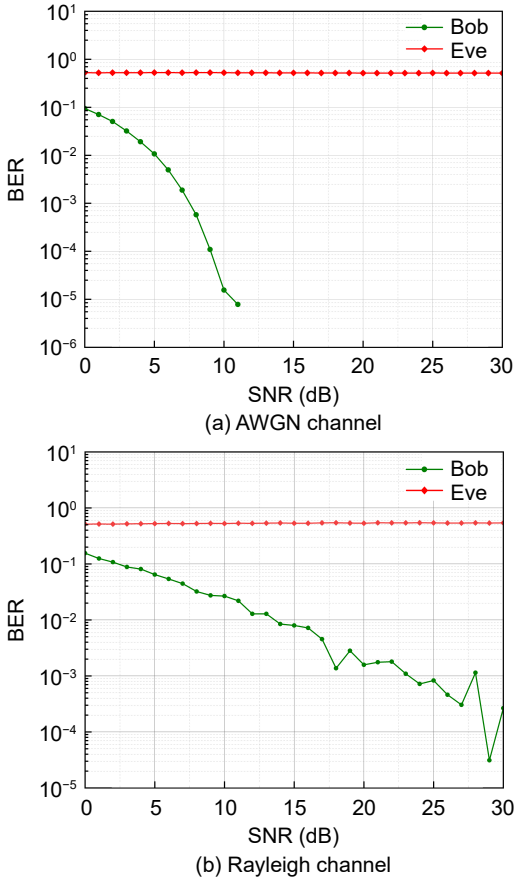


Fig. 6 BER of Bob and Eve under different channels.

be too significant, which will limit the learning ability of the neural network for signal characteristics and the decoding process, resulting in excessive deviation of the network. For performance analysis, the end-to-end encryption system is extended to the AWGN and Raleigh channels at a communication rate of R=1/2. The main channel SNR used in this training process is 10 dB for the AWGN channel and 15 dB for the Rayleigh channel. In order to provide Eve with a better eavesdropping environment, the signal-to-noise ratio of the eavesdropping channel is fixed at 20 dB. It is assumed that Eve has sufficient priori information about the received symbolic information, i.e., she knows the structure of the neural network based on the end-to-end communication system. Eve uses a trained and independent decoder for decoding. Bob and Eve are tested at an SNR of 0–30 dB.

The simulation results satisfy that the larger the signal-to-noise ratio is, the smaller the legitimate receiver BER is. The eavesdropper maintains a BER above 50% for different signal-to-noise ratios. It can be shown that the final trained communication system can better learn the features of the main channel and encrypt them implicitly into the decoder.

4.4 Communication system anti-eavesdropping security evaluation

Two models, Wiretap Channel I and Wiretap Channel II, were proposed by Wyner in Ref. [31]. The first type of eavesdropping channel describes a communication system that is eavesdropped on by an eavesdropper through a so-called eavesdropping channel, where the content received by the eavesdropper receives more severe noise contamination compared to the receiver. The second type of eavesdropping channel is in a noiseless channel. The eavesdropper can intercept a section of n-length information from the transmitted code word for analysis. The eavesdropper can only select a fixed-length area for eavesdropping, but the eavesdropper can arbitrarily determine n positions to eavesdrop. This is verified for the security of this end-to-end cryptosystem eavesdropping model I. In practice of the eavesdropping channel model, most eavesdroppers have poorer channel quality than the primary channel, resulting in different signals being received. The essence of our proposed solution for secure transmission lies in that the current communication system can work under the main channel. In contrast, 10 dB, 15 dB, 25 dB, and 30 dB noise addition on the eavesdropping channel can also carry out secure transmission. As shown in Fig. 7, the simulation results show that the BER of Eve does not change significantly as the signal-to-noise ratio of the eavesdropping channel increases, and the communication encryption system can maintain a certain level of security when operating in the main channel.

As powerful machine learning algorithms, neural networks have proved their importance as state-of-the-art experimental comparisons[32, 33]. In communication, neural networks are widely used to implement end-to-end communication systems and have achieved the best performance in some tasks. Simply showing the BLER of an autoencoder is not enough to explain its

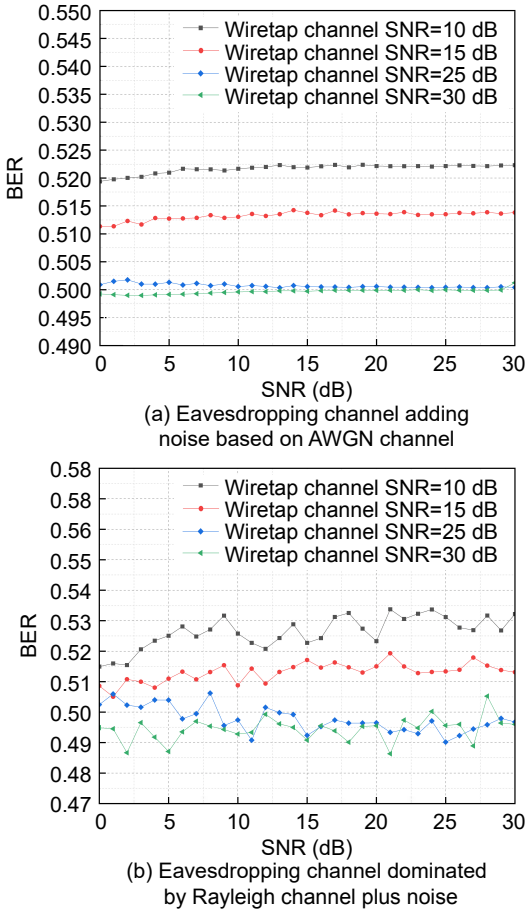


Fig. 7 Eve's BER under eavesdropping channel plus noise.

performance. We further discuss the advantages of the CAE-E2E system. Therefore, we compare the system with the communication rate of $R=k/n=1$ with the traditional modulation method binary phase-shift keying (BPSK) under the condition of AWGN channel. As shown in Fig. 8, the simulation results show that our designed end-to-end asymmetric encryption may also yield joint coding and modulation gains, which can be derived as an advantage of deep learning applied to encryption in communication systems.

On this basis, we further system anti-eavesdropping security performance evaluation. We do not use as above independent training eavesdropping decoder. Suppose Bob chooses to disclose his decoder structure. In that case, Eve has access to the same decoder structure as Bob, and the eavesdropping decoder is also the decoder corresponding to Alice's encoder. Under current conditions, the difference between Bob and Eve is that the signals they receive experience different

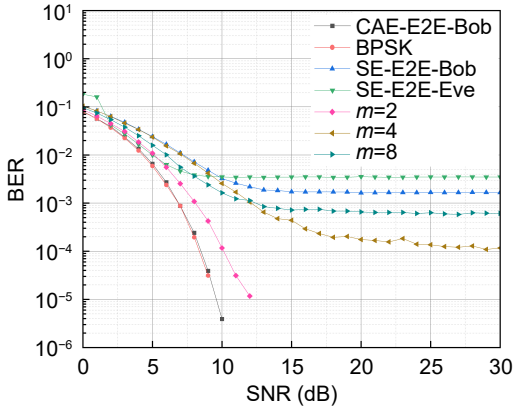


Fig. 8 Comparison of CAE-SE-E2E system, SE-E2E system, and BPSK modulation system.

channel losses. Bob holds the private key required for encrypted communication, while Eve does not have this privilege. These factors cause Bob and Eve to receive slightly different signals, causing their understanding of the transmitted information to differ. We compare the CAE-E2E system to a random key symmetric encryption end-to-end communication system (SE-E2E) with the same neural network structure.

The key generator converts the private key into the corresponding public key according to specific rules, and the length of the public key depends on the encryption algorithm used and the length of the private key. Assuming that the value of m represents different private key lengths, the initial length of the private key in the designed communication encryption system is $m=1$. The public key's length increases with the private key's length. In this case, we hope the CAE-E2E system has excellent encryption strength for secure communication. Simulation experiments show that we can effectively limit Eve's eavesdropping by changing the length of the private key, and Bob's received signal is not affected by the change in the length of the private key. The CAE-E2E system is substantially better than the SE-E2E system in terms of communication performance and security against eavesdropping.

5 Conclusion

In this paper, we propose an end-to-end asymmetric encrypted communication system based on CNNs, starting from the current security issues in designing an

end-to-end communication system with encryption key management.

We propose to use CNNs as key generators to generate high-quality key pairs, and CAE-E2E systems communicate with data asymmetric encryption. The designed key generator generates the key pair, the public key is shared with the sender for the encrypted transmission of the message, and the receiver decrypts the message as the private key holder. Based on this, the loss function of the secure transmission model for end-to-end communication is redesigned to improve further the intrinsic security and optimization of the end-to-end communication system. Experiments are simulated on the AWGN and Rayleigh channels to analyze the effect of training parameters of various aspects of the loss curve on the system's performance. The eavesdropper is designed according to different predictions of the information held by the eavesdropper, all measured in terms of BER. Firstly, in eavesdroppers with the same neural network structure, the BER of the eavesdropper for the test noise-added eavesdropping channel is maintained at about 0.5. Secondly, the eavesdropper obtains the decoder structure eavesdropping test of the legitimate person. The eavesdropper can only decode accurately by mastering the private key, which has better security performance than the SE-E2E communication system. The experimental results show that the eavesdropper in the CAE-E2E system has an impossible distance to the maximum bit error rate required for reliable communication.

In future research, the performance of the communication system in the AWGN channel and Rayleigh channel is investigated in this paper, with a future focus on migrating the proposed secure transmission scheme to more communication scenarios

Acknowledgment

This work was supported by the National Key Research and Development Program of China (No. 2017YFE0135700), the High Level Talent Support Project of Hebei Province (No. A201903011), the Natural Science Foundation of Hebei Province (No. F2018209358), the Tsinghua Precision Medicine Foundation (No. 2022TS003), the Telecommunications Research Centre (TRC) of University of Limerick, Ireland, the Science and Education for Smart Growth Operational Program (2014–2020) (No. BG05M2OP001-1.001-0003), co-financed by the European Union through the European Structural and Investment funds.

References

[1] K. Kaur, S. Kumar, and A. Baliyan, 5G: A new era of wireless communication, *Int. J. Inf. Technol.*, vol. 12, no. 2, pp. 619–624, 2020.

[2] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, Wireless communication technologies for IoT in 5G: Vision, applications, and challenges, *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–12, 2022.

[3] Z. Qin, H. Ye, G. Y. Li, and B. H. F. Juang, Deep learning in physical layer communications, *IEEE Wirel. Commun.*, vol. 26, no. 2, pp. 93–99, 2019.

[4] Q. Hu, F. Gao, H. Zhang, S. Jin, and G. Y. Li, Deep learning for channel estimation: Interpretation, performance, and comparison, *IEEE Trans. Wirel. Commun.*, vol. 20, no. 4, pp. 2398–2412, 2020.

[5] W. Zhang, M. Feng, M. Krunz, and A. Hossein Yazdani Abyaneh, Signal detection and classification in shared spectrum: A deep learning approach, in *Proc. IEEE INFOCOM 2021 - IEEE Conf. Computer Communications*, Vancouver, Canada, 2021, pp. 1–10.

[6] H. Ye, L. Liang, and G. Y. Li, Circular convolutional auto-encoder for channel coding, in *Proc. 2019 IEEE 20th Int. Workshop on Signal Processing Advances in Wireless Communications* (*SPAWC*), Cannes, France, 2019, pp. 1–5.

[7] A. V. Makkuva, X. Liu, M. V. Jamali, H. Mahdavifar, S. Oh, and P. Viswanath, KO codes: Inventing nonlinear encoding and decoding for reliable wireless communication via deep-learning, arXiv preprint arXiv: 2108.12920, 2021.

[8] S. Cammerer, F. A. Aoudia, S. Dörner, M. Stark, J. Hoydis, and S. ten Brink, Trainable communication systems: Concepts and prototype, *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5489–5503, 2020.

[9] H. Ye, L. Liang, G. Y. Li, and B. H. Juang, Deep learning-based end-to-end wireless communication systems with conditional GANs as unknown channels, *IEEE Trans. Wirel*, *Commun.*, vol. 19, no. 5, pp. 3133–3143, 2020.

[10] F. Ait Aoudia and J. Hoydis, End-to-end learning for OFDM: From neural receivers to pilotless communication, *IEEE Trans. Wirel. Commun.*, vol. 21, no. 2, pp. 1049–1063, 2022.

[11] H. Ye, G. Y. Li, and B. H. Juang, Deep learning based

end-to-end wireless communication systems without pilots, *IEEE Trans. Cogn. Commun. Netw*, vol. 7, no. 3, pp. 702–714, 2021.

[12] H. Jiang, S. Bi, L. Dai, H. Wang, and J. Zhang, Residual-aided end-to-end learning of communication system without known channel, *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 631–641, 2022.

[13] Y. An, S. Wang, L. Zhao, Z. Ji, and I. Ganchev, A learning-based end-to-end wireless communication system utilizing a deep neural network channel module, *IEEE Access*, vol. 11, pp. 17441–17453, 2023.

[14] T. O'Shea and J. Hoydis, An introduction to deep learning for the physical layer, *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, 2017.

[15] A. Burg, A. Chattopadhyay, and K. -Y. Lam, Wireless communication and security issues for cyber-physical systems and the internet-of-things, *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, 2017.

[16] N. Goergen, T. C. Clancy, and T. R. Newman, Physical layer authentication watermarks through synthetic channel emulation, in *Proc. 2010 IEEE Symp. on New Frontiers in Dynamic Spectrum* (*DySPAN*), Singapore, 2010, pp. 1–7.

[17] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks, *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, 2013.

[18] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X. Shen, An LDPC code based physical layer message authentication scheme with prefect security, *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, 2018.

[19] T. Dean and A. Goldsmith, Physical-layer cryptography through massive MIMO, in *Proc. 2013 IEEE Information Theory Workshop* (*ITW*), Seville, Spain, 2013, pp. 1–5.

[20] W. Li, D. McLernon, K. K. Wong, S. Wang, J. Lei, and S. Ali Raza Zaidi, Asymmetric physical layer encryption for wireless communications, *IEEE Access*, vol. 7, pp. 46959–46967, 2019.

[21] M. Arvandi, S. Wu, A. Sadeghian, W. W. Melek, and I. Woungang, Symmetric cipher design using recurrent neural networks, in *Proc. 2006 IEEE Int. Joint Conf. Neural Network Proceedings, Vancouver*, Canada, 2006, pp. 2039–2046.

[22] M. Abadi and D. G. Andersen, Learning to protect communications with adversarial neural cryptography, arXiv preprint arXiv: 1610.06918, 2016.

[23] Z. Sun, H. Wu, C. Zhao, and G. Yue, End-to-end learning of secure wireless communications: Confidential transmission and authentication, *IEEE Wirel. Commun.*, vol. 27, no. 5, pp. 88–95, 2020.

[24] A. Nooraiepour and S. R. Aghdam, Learning end-to-end codes for the BPSK-constrained Gaussian wiretap channel, *Phys. Commun.*, vol. 46, p. 101282, 2021.

[25] Y. An, M. Wang, L. Chen, and Z. Ji, DCGAN-based symmetric encryption end-to-end communication systems, *AEU Int. J. Electron. Commun.*, vol. 154, p. 154297, 2022.

[26] Z. Li, R. Yates, and W. Trappe, Secrecy capacity of independent parallel channels, in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Boston, MA, USA: Springer, 2009, pp. 1–18.

[27] H. Suo, J. Wan, C. Zou, and J. Liu, Security in the Internet of Things: A review, in *Proc. 2012 Int. Conf. Computer Science and Electronics Engineering*, Hangzhou, China, 2012, pp. 648–651.

[28] W. Diffie and M. E. Hellman, New directions in cryptography, in *Democratizing cryptography*: *The work of Whitfield Diffie and Martin Hellman*, R. Slayton, Ed. New York, NY, USA: ACM, 2022. pp. 365–390.

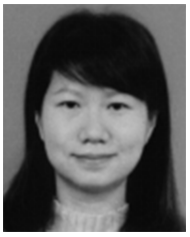
[29] C. E. Shannon, A mathematical theory of communication, *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[30] M. Uzair and N. Jamil, Effects of hidden layers on the efficiency of neural networks, in *Proc. 2020 IEEE 23rd Int. Multitopic Conf.* (*INMIC*), Bahawalpur, Pakistan, 2021, pp. 1–6.

[31] A. D. Wyner, The wire-tap channel, *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[32] C. F. R. Chen, Q. Fan, and R. Panda, CrossViT: Cross-attention multi-scale vision transformer for image classification, in *Proc. 2021 IEEE/CVF Int. Conf. Computer Vision* (*ICCV*), Montreal, Canada, 2022, pp. 347–356.

[33] G. Menghani, Efficient deep learning: A survey on making deep learning models smaller, faster, and better, *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–37, 2023.



Yongli An received the PhD degree in information science from Beijing Jiaotong University, China, in 2015. She is a professor at the North China University of Science and Technology, China. Her current research interests include wireless communication security technology, signal processing in communication, and large-scale MIMO technology.

Zebing Hu is currently pursuing the master degree with College of Artificial Intelligence, North China University of Science and Technology, China. His main research interest is the application of deep learning in wireless communication.

Zhanlin Ji received the MEng degree from Dublin City University, Ireland in 2006, and the PhD degree from the University of Limerick, Ireland in 2010. He is currently a professor with the North China University of Science and Technology, China, and a researcher with the Telecommunications Research Centre (TRC), University of Limerick, Ireland. He has authored/coauthored 70 research articles in refereed journals and conference papers. His research interests include UCWW, the Internet of Things (IoT), cloud computing, big data management, and data mining.

Haoran Cai is currently pursuing the master degree with College of Artificial Intelligence, North China University of Science and Technology, China. His main research interest is the application of deep learning in wireless communication.