The Hybrid Similar Neighborhood Robust Factorization Machine Model for Can Bus Intrusion Detection in the In-Vehicle Network

Yuchu He, Zhijuan Jia, Mingsheng Hu, Chi Cui, Yage Cheng, and Yanyan Yang

***Abstract*— Controller area network (CAN) is the most commonly used bus technology for In-vehicle network and uses multicast communication without corresponding security measures. Therefore, the message data field is vulnerable to tampering and other attacks. Recent machine learning-based intrusion detection methods for CAN bus messages only use the information contained in the message data field and do not take into account the contribution made by the neighboring information of CAN bus messages. In addition, previous models considered the data domain information of CAN bus messages as separate features and did not consider the unique weight of each feature, as well as the second-order interaction information between features. Therefore, we propose a novel intrusion detection model, The Hybrid Similar Neighborhood Robust Factorization Machine Model (HSNRFM), for detecting anomalies in CAN bus messages to address the shortcomings and problems of the previous models. To be able to incorporate the contribution of similar neighborhood information and learn the unique weight parameters of each feature in the model decision process, as well as additional second-order interaction information between features, the HSNRFM model solves the above problem using a similarity calculation method and a factorization machine model. Comprehensive experimental results are compared on real vehicle datasets. The HSNRFM model has AUC values of 0.9216 and 0.901 and AUPR values of 0.9194 and 0.9018 on two real datasets, respectively. And the results show that our proposed HSNRFM model has excellent detection efficiency for intrusion detection of CAN bus messages.**

***Index Terms*— Intrusion detection model, in-vehicle network, controller area network bus, modern car security, factorization machine.**

Manuscript received 23 May 2021; revised 17 July 2021, 2 August 2021, and 21 August 2021; accepted 27 August 2021. Date of publication 4 October 2021; date of current version 12 September 2022. This work was supported in part by the Natural Science Foundation of Henan Province, China, under Grant 202300410510, in part by the Key Scientific Research Projects of Higher Education of Henan Province under Grant 20A580008, and in part by the Science and Technology Program of Henan Province under Grant 212102210415 and Grant 212102210100. The Associate Editor for this article was S. H. Ahmed. *(Corresponding author: Zhijuan Jia.)*

Yuchu He is with the School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, China, and also with the School of Computer and Information Engineering, Henan University, Kaifeng 475001, China (e-mail: heyuchu@foxmail.com).

Zhijuan Jia, Mingsheng Hu, Chi Cui, Yage Cheng, and Yanyan Yang are with the School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, China (e-mail: jzj523@163.com; 47174051@qq.com; cuichi0713@hotmail.com; 897373693@qq.com; hnysyanyan@163.com).

Digital Object Identifier 10.1109/TITS.2021.3113638

I. Introduction

With the continuous development and application of technologies such as smart driving, intelligent transportation, cloud computing and 5G, automobiles are gradually developing towards network connectivity and intelligence [1]–[3]. CAN (Controller area network) is the most commonly used bus in In-vehicle, which adopts multicast communication without corresponding security measures [4], [5], and the message data field is vulnerable to tampering and other attacks. This attack not only poses potential risks such as privacy leakage and property damage, but more seriously endangers the lives of drivers and other traffic participants [6], [7]. Therefore, intrusion detection techniques for CAN bus messages are of great interest [8], [9].

In recent years machine learning-based intrusion detection methods [1], [10]–[12] for CAN bus messages suffer from data sparsity and do not learn weights that are unique to each feature.

Therefore, we propose a novel intrusion detection model, The Hybrid Similar Neighborhood Robust Factorization Machine Model (HSNRFM), for detecting anomalies in CAN bus messages to address the shortcomings and problems of the previous models. Firstly, in order to enhance the robustness of the information in the original data domain, the HSNRFM model performs a pre-processing operation of dimensionality reduction on the original data using a fully connected network. Then, in order to incorporate the contribution of similar neighborhood information in the model decision process, the HSNRFM model calculates the similarity between the data domains of messages using their binary format. Then the HSNRFM model combines the data domain information of the target message and the data domain information of the neighboring messages that are most similar to the target message to form the final input features. Finally, in order to learn the unique weight parameters for each feature and additional second-order interaction information, the HSNRFM model feeds the features of the above CAN bus messages into the factorization machine model to produce the final prediction value. The value of this prediction value indicates whether the target CAN bus message is an anomaly message.

The main contributions made by this work are as follows.

1) We enhance the overall generalization capability of the model by utilizing a fully connected network to enhance the robustness of the raw data and novel use of data field of similar neighbors for enhancing the feature representation of the target CAN bus messages.
2) We use the factorization machine model, which can take into account the second-order interaction feature information, to predict the final probability of anomalous outcomes, which reduces the lost feature information to some extent and enhances the comprehensiveness of the model.
3) Comprehensive experimental results are compared on a real vehicle dataset, and the results show that our proposed HSNRFM model has excellent detection results for intrusion detection of CAN bus messages, outperforming several classical mainstream models in several evaluation metrics.

The remaining sections of this work are structured as follows. Section II will introduce the intrusion detection techniques about in-vehicle CAN bus messages, as well as the principles, advantages and disadvantages of the related models. Next, in Section III, the HSNRFM model proposed in this work will be introduced, including the implementation details and mathematical equation of the model. Then in Section IV the performance metrics of the HSNRFM model will be tested by relevant experiments, including parametric and comparative experiments. Finally, in Section V, the details of this work and the discussion of future work will be summarized.

II. Related Work

In recent years more and more automotive information security issues [13]–[17] have been continuously missed, and the information security of networked vehicles has received great attention from all walks of life [18]–[20]. Therefore, researchers have proposed a large number of intrusion detection models for CAN bus messages. This part reviews the principle of the relevant work relating to CAN bus message anomaly detection of in-vehicle systems [21], [22]. The following sections describe machine learning-based models and deep learning-based models, respectively.

A. Machine Learning-Based Models

Gmiden *et al.* [23] introduced a practical invasion discovery approach for controller area network bus IDS (Intrusion Detection System). Their system is based upon the evaluation of time periods of controller area network message. The main point is to execute an IDS which checks the Controller area network ID of the transmitted information after that computes the moment periods from the most recent one.

Casillo *et al.* [24] presented an embedded invasion discovery method for the vehicle that making use of the capacity of artificial intelligence equations as well as particularly Bayesian networks has the ability to detective feasible cyber invasions on the automobile CAN-Bas.

Seo *et al.* [25] introduced the GIDS (GAN Based Intrusion Detection System), Controller area network bus-based IDS for the car network. They introduced inscribing a great deal of Controller area network bus IDs with basic one-hot-vector, which can enhance the efficiency and also rate of the GIDS. The proposed GIDS makes use of arbitrary phony information in the training procedure rather of the actual assault information. It enables the GIDS method to discover unidentified intrusions with just regular information.

Marchetti and Stabili [26] introduced an innovative invasion discovery method that intends to recognize destructive controller area network bus messages infused by attackers in the controller area network bus of contemporary automobiles. The recommended method recognizes abnormalities in the sequence of messages that stream in the controller area network bus as well as is identified by tiny memory and also computational impacts.

Li *et al.* [27] presented a method to incorporate numerous associated parameters to discover sensing unit information spooning attacks for in-vehicle networks. The presented method makes use of a RF Regression as a forecaster of the proposed approach.

Li *et al.* [28] proposed a novel anomaly detection model for CAN messages, whose main objective is to improve the shortcomings of the traditional random forest model for this task. They applied the optimization algorithm from related literature to the random forest model to make its prediction better on the CAN message anomaly detection task.

B. Deep Learning-Based Models

Hanselmann *et al.* [29] proposed CANet, an innovative deep learning framework that is trained in a without supervision way to identify attacks as well as abnormalities on the controller area network bus. It is the first approach in the literature that works with the ability to servicing messages with various IDs at the same time.

Hossain *et al.* [30] introduced a LSTM-based Invasion Discovery System (IDS) to identify as well as reduce the controller area network bus network invasions. They create their own dataset by obtaining attack-free information from their experimental vehicle as well as by infusing invasions right into the last as well as accumulating the dataset.

Zhou *et al.* [31] presented a method called BTMonitor, to obtain physical inconsistencies of clocks in between various ECUs (Electronic Control Unit). It computes analytical attributes from dimensions on controller area network framework little bit time as finger print.

Chiscop *et al.* [32] proposed an intrusion detection model based on machine learning. The model is mainly concerned with whether or not the message is tampered with, and its main focus is to use a temporal convolutional network to capture the regular behavior patterns of CAN message signals. Thus, malicious message information can be distinguished.

Levy *et al.* [33] proposed a new in-vehicle cybersecurity system. The system consists of two components. The first component uses data augmentation and deep learning techniques to locate physical intrusion situations. The second component uses deep learning to continuously detect device anomalies.

Algorithm 1 Our Proposed Model

Input: The data field of CAN bus message, $Data$

Output: The predicted value of the target CAN bus message i, $\hat{y}_i$

for $i \in$ the CAN bus messages **do**
  Binary formatting of raw hexadecimal data.
    $Data^2 \leftarrow BFC(Data)$
  Enhancing data robustness with fully connected networks.
    $RD \leftarrow f(W^T Data^2 + b)$
  Calculate the similarity between messages using cosine similarity
    Sim = cosine-similarity($Data^2$)
  Combining neighborhood information to generate final input features.
    $RF_i \leftarrow RD_i$
    $RF_j \leftarrow RD_j, j \in N(i)$
    $FIF_i \leftarrow Join(RF_i, RF_j)$
  Predict the probability of data being anomalous.
    Linear regression:$\sum_{k=i} w_i x_i$
    Second order interaction:$\sum_{k=1} \sum_{l=k+1} \hat{w}_{kl} x_k x_l$
    Output: $\hat{y}_i \leftarrow w_0 + \sum_{k=i} w_i x_i + \sum_{k=1} \sum_{l=k+1} \hat{w}_{kl} x_k x_l$
  if $\hat{y}_i > Threshold$:
    $\hat{y}_i \leftarrow 1$
  else:
    $\hat{y}_i \leftarrow 0$
  Return $\hat{y}_i$
end for

Laghrissi *et al.* [34] proposed a novel detection model based on long and short-term memory networks and multiple sources of information. The modified model first performs the work of feature extraction using a dimensionality reduction algorithm, which is subsequently fed into the long- and short-term memory network to derive the final predicted values. The model is enhanced in its generalization ability compared to traditional machine learning models due to the incorporation of multiple deep learning models.

In recent years machine learning-based intrusion detection methods [35]–[38] for CAN bus messages only use the information contained in the message data field and do not take into account the contribution made by the neighboring information of CAN bus messages. In addition, previous models considered the data domain information of CAN bus messages as separate features and did not consider the unique weight of each feature, as well as the second-order interaction information between features [10], [39]–[41]. And the previous models did not consider the impact of the robustness of the original data field information on the model performance [42]–[44].

III. Method

The main idea behind the HSNRFM model proposed in this work is to enhance the robustness of the original data by using a fully connected network, and to enhance the overall generalization capability of the model by novelly using the data field information of similar neighbors for enhancing the feature representation of the target CAN bus message. Moreover, the HSNRFM model uses a factorization machine model that can take into account the second-order interaction information of the features to predict the anomaly probability of the final CAN bus message, which expands the feature information and enhances the comprehensiveness of the model to a certain extent. We will describe in Section III.A how the HSNRFM model enhances the robustness of the original data and combines the data domains of the neighborhood to expand its own feature representation. Subsequently, Section III.B describes how the HSNRFM model incorporates the second-order cross-feature information into the final predicted values. Figure 1 shows the flow chart of the HSNRFM algorithm.

A. Improving Data Robustness and Expanding Features With Neighborhoods

Previous machine learning-based intrusion detection methods for CAN bus messages only use the information contained in the data field of the message and do not take into account the contribution made by the neighboring information of the CAN bus message. And previous models did not consider the impact of the robustness of the raw data domain information on the model performance. The data field in the original CAN bus message is partially encoded in hexadecimal, and to increase the dimensionality of this information, we convert it to binary encoding using Equation (1).

$$Data^2 = BFC(Data) \tag{1}$$

where $Data$ is the original data field information, BFC represents the binary format conversion, $Data^2$ is the converted binary encoding format data field information.

Firstly, in order to be able to enhance the robustness of the information in the original data domain, the HSNRFM model performs a pre-processing operation on the original data using a fully connected network. The preprocessing operation is shown in Equation (2).

$$RD = f(W^T Data^2 + b) \tag{2}$$

where W is the weight parameter in the fully connected network, b is the bias parameter, f is the activation function, and RD stands for Robust Data.

Subsequently, in order to be able to incorporate the contribution of similar neighborhood information in the model decision process, the HSNRFM model uses the binary format $Data^2$ of the data domain between messages to calculate the similarity between messages. The similarity calculation equation uses the cosine similarity, which is shown in Equation (3).

$$Sim = cosine - similarity(Data^2) \tag{3}$$

where $cosine-similarity$ is the cosine similarity equation in the Sklearn library, Sim is the similarity matrix between messages, and each row stores the similarity information between this message and other messages. The cosine similarity is used in this work because it is the most widely used when comparing similar information between two vectors.

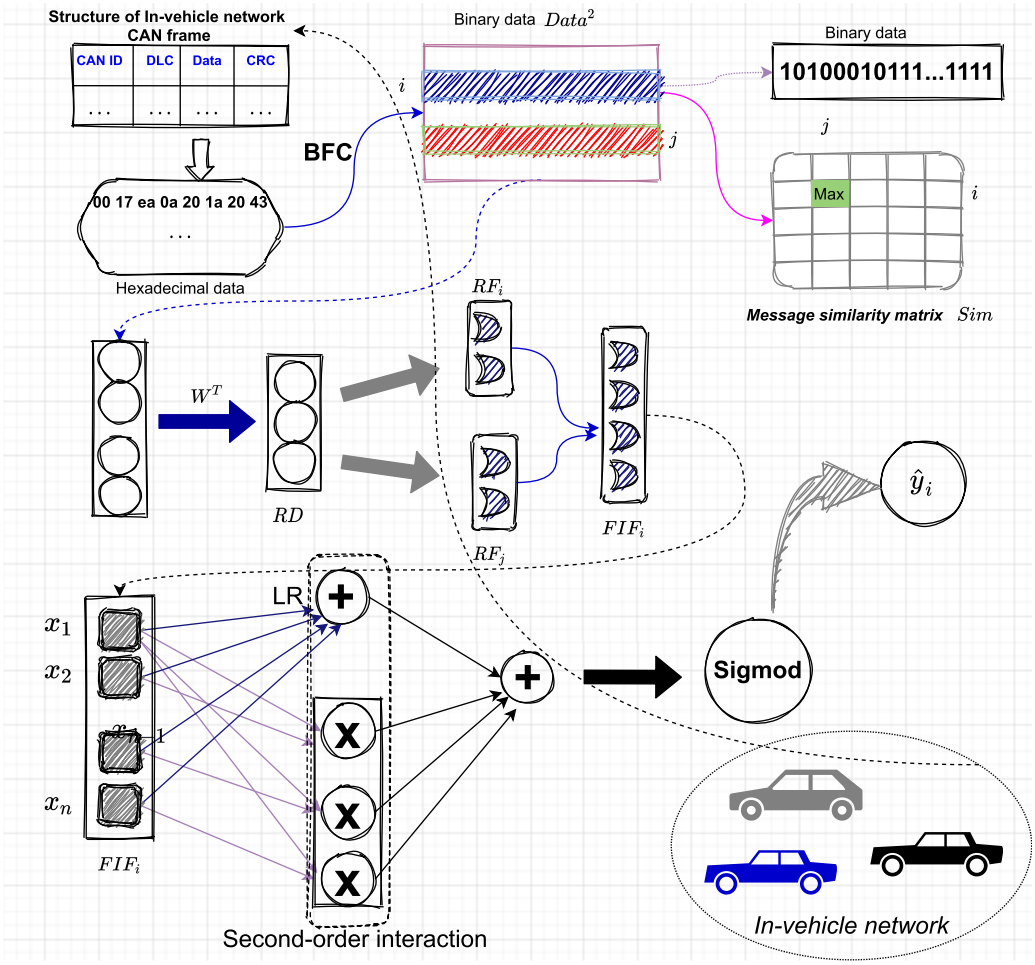


Fig. 1. The algorithm structure of the HSNRFM model.

The HSNRFM model then combines the data field information of the target message and the data field information of the neighboring messages that are most similar to the target message to compose the final input features. The composition method adopts the Equation (4) splicing method, and this operation can maximize the dimensionality of the message features and strengthen the expression capability of the features.

$$\begin{aligned} RF_i &= RD_i \\ RF_j &= RD_j, j \in N(i) \\ FIF_i &= Join(RF_i, RF_j) = [RF_i, RF_j] \end{aligned} \tag{4}$$

where the neighbor j is the most similar to the message i. RF_i and RF_j are the i and jth lines of RD, respectively. FIF_i is the final input feature of message i.

B. Generating Predictions Using Factorization Machine Models

Previous models only considered each byte of the data field information of the CAN bus message as a separate feature in the output of the final predicted value, and did not consider the unique weight of each feature, and the second-order interaction information between features.

Therefore, in order to be able to learn the weight parameters unique to each feature, as well as additional feature information from second-order interactions, the HSNRFM model inputs the final input features of message i into the factorization machine model, and the operation of generating prediction values is shown in Equation (5). The generated predicted values contain two parts, the first part of Equation (5) is the predicted value derived from linear regression, and the second part of Equation (5) is the information derived from the second-order feature interactions.

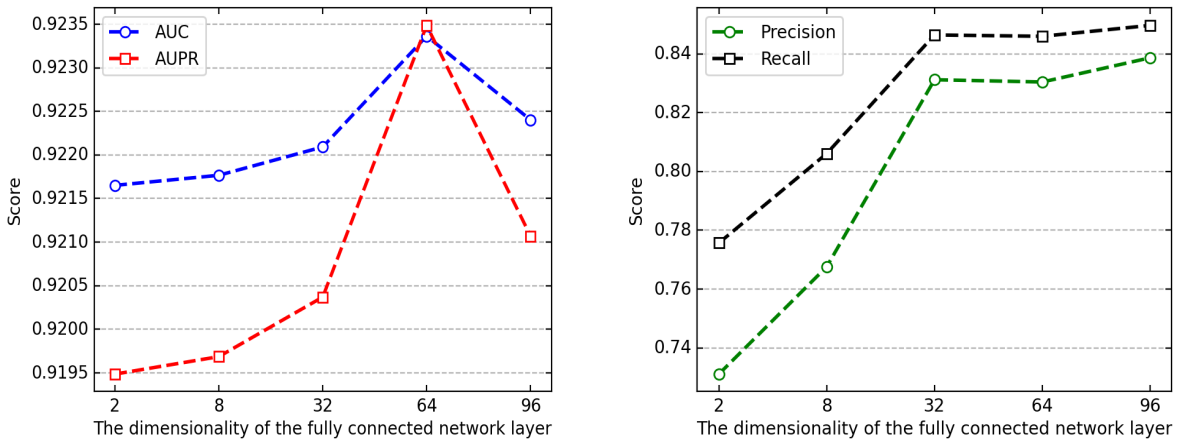
$$\hat{y}_i = w_0 + \sum_{k=i} w_i x_i + \alpha \sum_{k=1} \sum_{l=k+1} \hat{w}_{kl} x_k x_l \tag{5}$$

where $\hat{y}_i$ is the final prediction value derived from the HSNRFM model. The value of this prediction value indicates the probability of whether this target CAN bus message is an anomaly message. $\sum_{k=i} w_i x_i$ is the predicted value derived from linear regression. $\sum_{l=k+1} \hat{w}_{kl} x_k x_l$ is the information derived from the second-order feature interactions.

Algorithm 1 shows the pseudo-code of the HSNRFM algorithm proposed in this work.

IV. Experiment and Discussion

In this section, we describe the data set situation in the experiments, evaluate the setup and show the performance of the HSNRFM model. In addition, we implemented the HSNRFM model using the PyTorch library in the Python



(a) AUC-AUPR (b) Precision-Recall

Fig. 2. The experimental results of HSNRFM model with different dimension of fully connected network under *DataA*.

language and simulated the related experiments in a CPU (Central Processing Unit) environment.

A. Dataset and Pre-Processing Operations

This work uses a realistic dataset named OTIDS from the literature [45], the data of this data set is the vehicle CAN bus data collected under normal operation, and the messages with more serious missing or duplicated data are removed by data pre-processing. In addition, since the original data of CAN data messages are normal data and there is no abnormal message data, this work uses the method of random perturbation to generate abnormal data, i.e., by randomly changing a byte of information in the data field of CAN bus messages to generate abnormal message data.

The timestamp in the dataset represents the time the message was received, the ID is the recipient of the message, and the final hexadecimal data represents the specific content of the message.

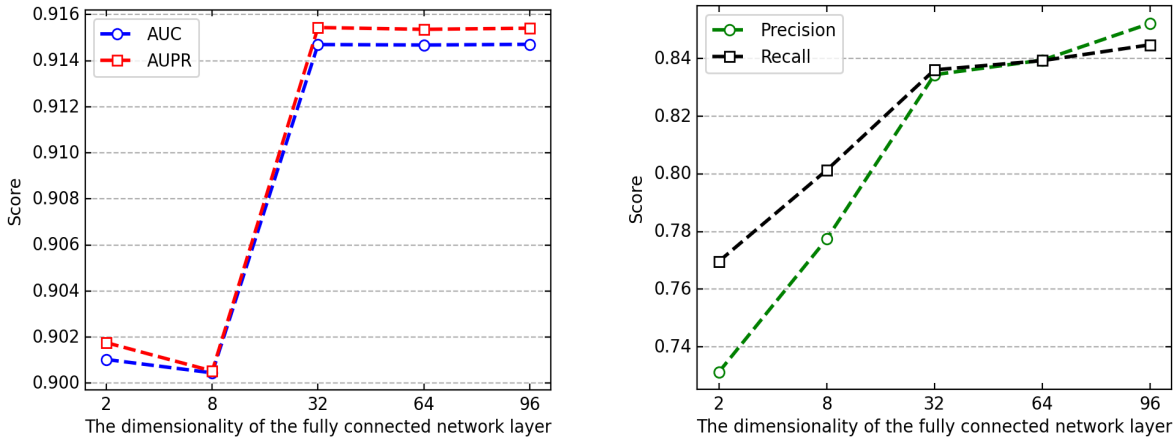
In this work, samples with CAN IDs 0545 and 0316 are sampled as experimental data sets, where all samples with ID 0545 are used as *DataA*, and all samples with ID 0316 are used as *DataB*. These two datasets are used to evaluate the performance of the HSNRFM model. In addition, the results of the experiments are evaluated using four metrics: AUC (Area Under ROC Curve), AUPR (Area Under Precision-Recall Curve), Precision, and Recall. Precision is how many of the positive samples predicted by the model are true positive samples; Recall is how many of the true positive samples are inferred by the model. AUPR is the area under the Accuracy-Recall curve. AUC is the area under the ROC curve. The larger the value of all the above metrics, the better the generalization performance of the model. 70% of all samples were used as the training set for training the model and 30% of the samples were used as the test set for evaluating the results of the model.

B. Hyperparametric Experiments

The purpose of the first experiment set in this section is to observe the performance of the HSNRFM model under fully connected networks of different dimensions, which is used to verify whether enhancing the input data robustness can contribute to the generalizability of the model proposed in this work. The purpose of the second experiment set up in this section is to observe whether the second-order interaction information among the input features can enhance the performance of the model. The experimental data set and evaluation metrics are referred to Section IV.A.

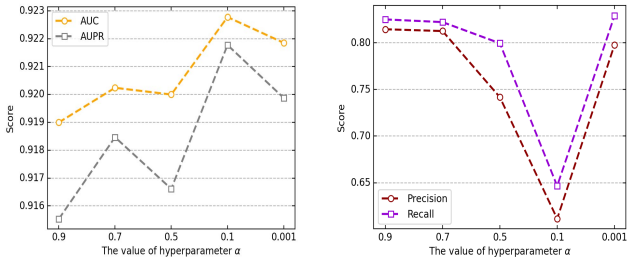
1) Dimensionality of the Fully Connected Network Layer: The fully connected network referred to in this section is a neural network used to enhance the robustness of the input data, and the size of its dimensionality not only controls the number of features of the final input data, but also determines the strength of the robustness of the input data to a certain extent. Figure 2 and Figure 3 show the performance of the HSNRFM model proposed in this work with fully connected networks of different dimensions. The horizontal coordinates of Figure 2 and Figure 3 are the values of the fully connected network dimensions, and the values vary in the range of [2, 8, 32, 64, 96], and their vertical coordinates are the specific values of AUC, AUPR, Precision and Recall, respectively.

The two subplots of Figure 2 show the performance of the HSNRFM model on dataset A. It can be observed that the AUC and AUPR achieve the maximum value when the dimension value is 64, while the AUC and AUPR values of the HSNRFM model decline when the feature dimension of the fully connected network is greater than 64 or less than 64. In contrast, the model achieves better performance under Precision and Recall metrics when the dimensionality is 32 and 96. The two subplots in Figure 3 show the performance of the HSNRFM model on dataset B. Under the AUC and AUPR metrics, the performance of the model tends to be flat when the dimensionality is 32. There is a slight improvement in performance when the dimension is greater than 32. And under the Precision and Recall metrics, the performance of the model enhances with increasing dimensionality. The reason for this phenomenon is that the complexity and fitting power of the model grow as the dimensionality increases under the AUC and AUPR metrics, which will make the model more and more effective in prediction. However, when the



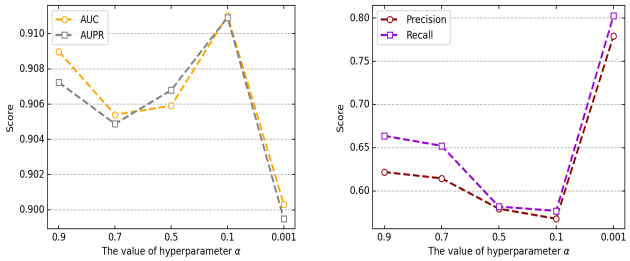
(a) AUC-AUPR (b) Precision-Recall

Fig. 3. The experimental results of HSNRFM model with different dimension of fully connected network under $DataB$.



(a) AUC-AUPR (b) Precision-Recall

Fig. 4. The experimental results of HSNRFM model with different value of hyperparameter α under $DataA$.



(a) AUC-AUPR (b) Precision-Recall

Fig. 5. The experimental results of HSNRFM model with different value of hyperparameter α under $DataB$.

dimensionality exceeds a certain threshold, the model learns the noise in the data, which leads to the appearance of an overfitting phenomenon, and thus the prediction effect of the model decreases.

The above experimental results illustrate that the appropriate dimensionality of the fully connected network on a given dataset can enhance the robustness of the input data and thus improve the performance of the model.

2) The Value of Hyperparameter α: The hyperparameter of this part is α in Equation (5), which controls the weight of the second-order interaction information among the input features in the final prediction value. Figure 4 and Figure 5 show the performance of the HSNRFM model proposed in this work with different values of the hyperparameter α. The horizontal coordinates of Figure 4 and Figure 5 are the values of hyperparameters α with values varying in the range of $[0.9, 0.7, 0.5, 0.1, 0.001]$, and their vertical coordinates are the specific values of AUC, AUPR, Precision and Recall, respectively.

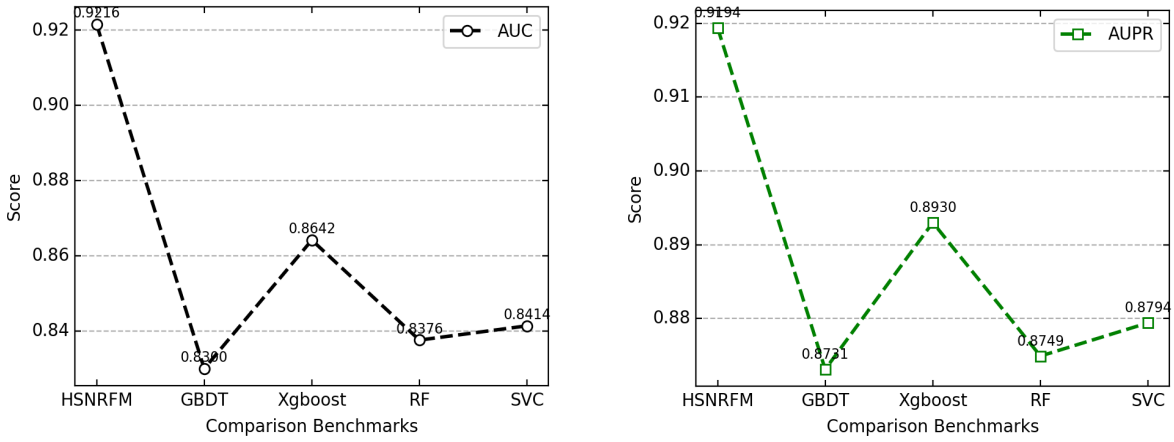
The two subplots in Figure 4 show the performance of the HSNRFM model on dataset A. The two subplots in Figure 5 show the performance of the HSNRFM model on dataset B. It can be observed that the performance of the HSNRFM model under both AUC and AUPR metrics is optimal when the value of parameter α is taken as 0.1. In contrast, the opposite pattern appears under the Precision and Recall metrics, where the values of both Precision and Recall are minimum when the value of the hyperparameter is 0.1.

The above experimental results illustrate that a certain proportion of second-order association information between features can improve the performance of the HSNRFM model under AUC and AUPR metrics, however, it decreases the performance of the HSNRFM model under Precision and Recall metrics. The reason for the above situation is that the second-order interaction information among features does not satisfy all evaluation metrics, and different evaluation metrics have their own focus and limitations. Therefore, different proportions of second-order interaction information between features need to be selected for different scenarios.

C. Benchmark Comparison

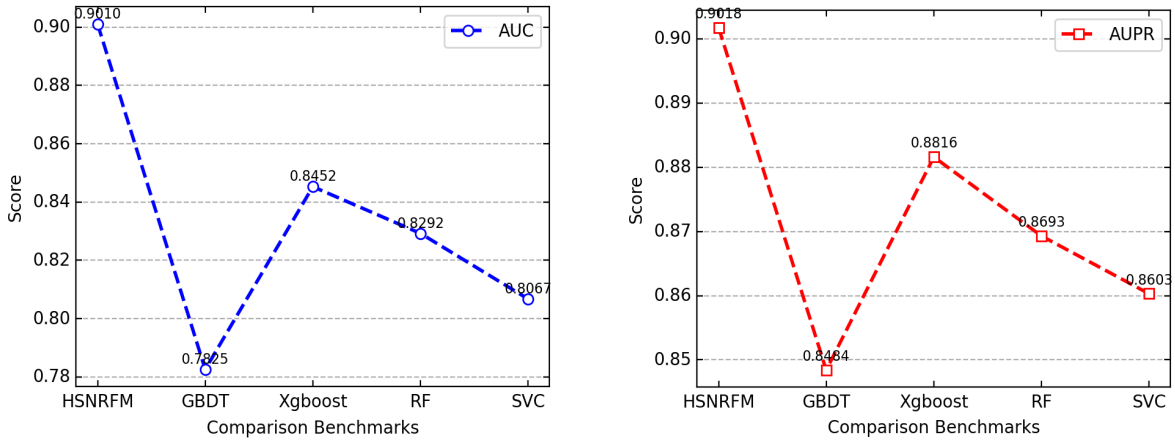
In this section, in order to verify the effectiveness of the HSNRFM model proposed in this work in practical application scenarios, we compare its experimental results with four classical intrusion detection algorithms, which are the following models.

1) GBDT: The Gradient boosting Decision Tree algorithm is a composite algorithm that iteratively trains a series of



(a) AUC (b) AUPR

Fig. 6. The comparison of HSNRFM model with other benchmarks under *DataA*.



(a) AUC (b) AUPR

Fig. 7. The comparison of HSNRFM model with other benchmarks under *DataB*.

decision trees, where each decision tree is fitted with the negative gradient value of the loss function based on the currently trained decision trees, and then these decision trees are used to make a joint decision to obtain the final result.

2) XGBoost: The basic idea of the XGBoost algorithm is similar to that of GBDT, which continuously performs feature splitting to grow a tree, learning one tree per round, in fact, fitting the residuals between the predicted and actual values of the previous round model. And it is efficient to make many improvements in related algorithms and engineering.
3) RF: Random forest model is an integrated learning method for classification, which builds multiple decision trees at training time and outputs as the mean of all decision trees as the final prediction.
4) SVC: SVC (Support Vector Classification) is a classification version of the SVM (Support Vector Machines) algorithm, which is a parametric machine learning model with a better theoretical foundation.

Figures 6 and 7 show the experimental results of the HSNRFM model with four comparative benchmark models on datasets A and B, respectively, with the evaluation metrics of AUC and AUPR. It is evident that the HSNRFM model proposed in this work achieves the first place in both datasets in terms of AUC and AUPR values. The AUC value on dataset A is 0.9216 and the second place is only 0.8642, and the AUPR value is 0.9194 and the second place is only 0.893. The AUC value on dataset B is 0.901 and the second place is only 0. 8452, and the AUPR value is 0.9018 and the second place is only 0.8816. Figures 8 and 9 show the flow of the loss values for a particular experiment.

According to the above experimental results, the performance of the HSNRFM model is substantially ahead of the remaining four benchmark models, which verifies the effectiveness of the HSNRFM model and shows that it can detect potential abnormal messages in a realistic scenario in time to protect the safety of vehicles and users. In addition, the HSNRFM model substantially outperforms the rest of the algorithms for all three metrics and two independent data sets,

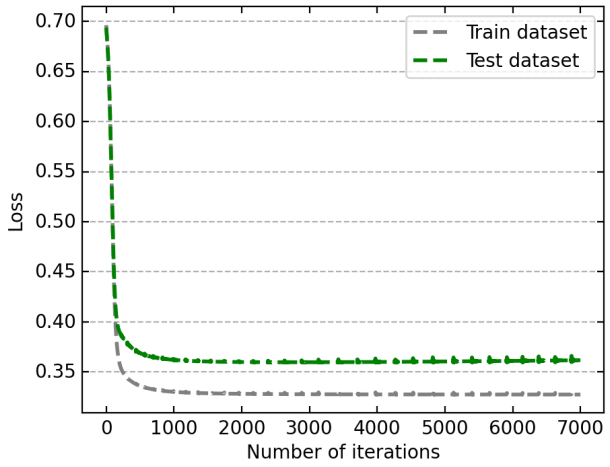


Fig. 8. The loss of the model in the training and test sets under *DataA*.

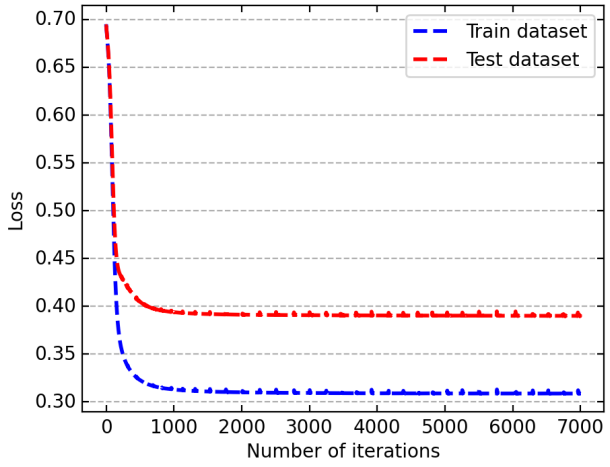


Fig. 9. The loss of the model in the training and test sets under *DataB*.

which also indicates the existence of some validity of the improved method in this work.

V. Conclusion

In this work, we enhance the overall generalization capability of the model by utilizing a fully connected network to enhance the robustness of the raw data and novel use of data field of similar neighbors for enhancing the feature representation of the target CAN bus messages. In addition, we use the factorization machine model, which can take into account the second-order interaction feature information, to predict the final probability of anomalous outcomes, which reduces the lost feature information to some extent and enhances the comprehensiveness of the model. And comprehensive experimental results are compared on a real vehicle dataset, and the results show that our proposed HSNRFM model has excellent detection results for intrusion detection of CAN bus messages, outperforming several classical machine learning models in several evaluation metrics. However, there are still some limitations of the HSNRFM model, how to be compatible with higher-order feature interaction information, and how to handle larger in-vehicle message data are the focus of our future research.

References

[1] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Secur.)*, San Francisco, CA, USA, vol. 4, 2011, pp. 447–462.

[2] B. I. Kwak, J. Woo, and H. K. Kim, "Know your master: Driver profiling-based anti-theft method," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 211–218.

[3] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proc. Workshop Embedded Secur. Cars*, 2004, pp. 1–13.

[4] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[5] D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: Vehicle virus," in *Proc. IASTED Int. Conf. Commun. Syst. Netw. (AsiaCSN)*, 2008, pp. 66–72.

[6] T. Hoppe, S. Kiltz, and J. Dittmann, "Automotive it-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Berlin, Germany: Springer, 2009, pp. 145–158.

[7] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable: A story of telematic failures," in *Proc. 9th USENIX Workshop Offensive Technol. (WOOT)*, 2015, pp. 1–9.

[8] A. Van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth—A simple, backward compatible broadcast authentication protocol for CAN bus," in *Proc. Workshop Lightweight Cryptogr. (ECRYPT)*, vol. 2011, 2011, p. 20.

[9] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. Int. Conf. Cyber Secur.*, Dec. 2012, pp. 1–7.

[10] X. Sun, B. Yan, X. Zhang, and C. Rong, "An integrated intrusion detection model of cluster-based wireless sensor network," *PLoS ONE*, vol. 10, no. 10, Oct. 2015, Art. no. e0139513.

[11] P. Tyagi and D. Dembla, "Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2014, pp. 2084–2090.

[12] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2014.

[13] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone, and A. Santone, "CAN-bus attack detection with deep learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5081–5090, Aug. 2021.

[14] J. Gao and H. Tembine, "Distributed mean-field-type filters for traffic networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 507–521 Feb. 2018.

[15] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and T. Reddy, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021.

[16] J. Gao and H. Tembine, "Empathy and berge equilibria in the forwarding dilemma in relay-enabled networks," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Nov. 2017, pp. 1–8.

[17] S. Agrawal *et al.*, "Federated learning for intrusion detection system: Concepts, challenges and future directions," 2021, *arXiv:2106.09527*. [Online]. Available: http://arxiv.org/abs/2106.09527

[18] M. Muter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 1110–1115.

[19] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Proc. 6th Int. Conf. Inf. Assurance Secur.*, Aug. 2010, pp. 92–98.

[20] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2016, pp. 63–68.

[21] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2008, pp. 220–225.

[22] A. Boudguiga, W. Klaudel, A. Boulanger, and P. Chiron, "A simple intrusion detection method for controller area network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–7.

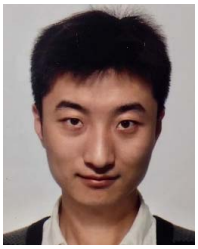
[23] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *Proc. 17th Int. Conf. Sci. Techn. Autom. Control Comput. Eng. (STA)*, Dec. 2016, pp. 176–180.

[24] M. Casillo, S. Coppola, M. D. Santo, F. Pascale, and E. Santonicola, "Embedded intrusion detection system for detecting attacks over CAN-BUS," in *Proc. 4th Int. Conf. Syst. Rel. Saf. (ICSRS)*, Nov. 2019, pp. 136–141.
[25] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2018, pp. 1–6.
[26] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1577–1583.
[27] H. Li, L. Zhao, M. Juliato, S. Ahmed, M. R. Sastry, and L. L. Yang, "POSTER: Intrusion detection system for in-vehicle networks using sensor correlation and integration," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 2531–2533.
[28] Y. Li, F. Li, and J. Song, "The research of random forest intrusion detection model based on optimization in internet of vehicles," *J. Phys., Conf. Ser.*, vol. 1757, no. 1, Jan. 2021, Art. no. 012149.
[29] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," *IEEE Access*, vol. 8, pp. 58194–58205, 2020.
[30] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," *IEEE Access*, vol. 8, pp. 185489–185502, 2020.
[31] J. Zhou, P. Joshi, H. Zeng, and R. Li, "Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network," *ACM Trans. Embedded Comput. Syst.*, vol. 18, no. 6, pp. 1–23, Jan. 2020.
[32] I. Chiscop, A. Gazdag, J. Bosman, and G. Biczók, "Detecting message modification attacks on the CAN bus with temporal convolutional networks," 2021, *arXiv:2106.08692*. [Online]. Available: http://arxiv.org/abs/2106.08692
[33] E. Levy, A. Shabtai, B. Groza, P.-S. Murvay, and Y. Elovici, "CAN-LOC: Spoofing detection and physical intrusion localization on an in-vehicle CAN bus based on deep features of voltage signals," 2021, *arXiv:2106.07895*. [Online]. Available: http://arxiv.org/abs/2106.07895
[34] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *J. Big Data*, vol. 8, no. 1, pp. 1–16, Dec. 2021.
[35] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.
[36] W.-H. Chen, S.-H. Hsu, and H.-P. Shen, "Application of SVM and ANN for intrusion detection," *Comput. Oper. Res.*, vol. 32, no. 10, pp. 2617–2634, 2005.
[37] J. Wu, D. Peng, Z. Li, L. Zhao, and H. Ling, "Network intrusion detection based on a general regression neural network optimized by an improved artificial immune algorithm," *PLoS ONE*, vol. 10, no. 3, Mar. 2015, Art. no. e0120976.
[38] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, 2009.
[39] A. J. Deepa and V. Kavitha, "A comprehensive survey on approaches to intrusion detection system," *Procedia Eng.*, vol. 38, pp. 2063–2069, Jan. 2012.
[40] C. Patsakis, K. Dellios, and M. Bouroche, "Towards a distributed secure in-vehicle communication architecture for modern vehicles," *Comput. Secur.*, vol. 40, pp. 60–74, Feb. 2014.
[41] T.-J. Park, C.-S. Han, and S.-H. Lee, "Development of the electronic control unit for the rack-actuating steer-by-wire using the hardware-in-the-loop simulation system," *Mechatronics*, vol. 15, no. 8, pp. 899–918, Oct. 2005.
[42] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1624–1639, Dec. 2011.
[43] Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles, "HIDE: A hierarchical network intrusion detection system using statistical preprocessing and neural network classification," in *Proc. IEEE Workshop Inf. Assurance Secur.*, vol. 85, Jun. 2001, p. 90.
[44] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, Jul. 2009.
[45] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2017, pp. 57–5709.

Yuchu He was born in Pingdingshan, Henan, China, in 1985. He received the B.S. degree from Henan Normal University in 2009, the master's degree from Sichuan University in 2012, and the Ph.D. degree from Chongqing University in 2018. He has been a Post-Doctoral Researcher with Zhengzhou Normal University and Henan University. His current research interests include intelligent transportation systems and machine learning.

Zhijuan Jia was born in Zhengzhou, Henan, China, in 1973. She received the B.S. degree in computer applied technology from PLA Information Engineering University, Zhengzhou, in 1993, and the M.S. degree in educational technology from Beijing Normal University, Beijing, China, in 2006. Since 1993, she has worked at Zhengzhou Normal University, where she is currently a Professor. She was a Visiting Scholar with the University of Wollongong Australia in 2017. She has published more than 30 papers and one monograph. Her research interests include information security and trusted computing. She is an Awarder of the National Science Fund of China and the Academic Leader of Henan Science and Technology Department.

Mingsheng Hu was born in Zhengzhou, Henan, China, in 1973. He received the B.S. degree in computer software from Central China Normal University in 1997, the M.S. degree in software engineering from PLA Information Engineering University in 2005, and the Ph.D. degree in control engineering from Huazhong University of Science and Technology in 2007. Since 1997, he has worked at Zhengzhou Normal University, where he is currently a Professor. He has published more than 20 papers and one monograph. His research interests include information security and complex networks. He is an Awarder of the National Science Fund of China.



Chi Cui was born in Zhengzhou, Henan, China, in 1987. He received the B.S. degree in software engineering from the University of Macau, Macau, in 2010, and the M.S. degree in information technology from The Hong Kong University of Science and Technology in 2011. He is currently a Lecturer at Zhengzhou Normal University. His research interests include information security, robotics, and the Internet of Things.

Yage Cheng was born in Zhengzhou, Henan, China, in 1987. She received the B.S. degree in mathematics and applied mathematics from Anyang Normal University in 2012 and the M.S. degree in applied mathematics from Minzu University of China in 2015. She is currently a Lecturer with Zhengzhou Normal University. Her research interests include information security, cryptography, and the Internet of Things.

Yanyan Yang was born in Luoyang, Henan, China, in 1986. She received the B.S. and M.S. degrees in computer from Zhengzhou University, China, in 2010 and 2013, respectively. She is currently a Lecturer with Zhengzhou Normal University. Her research interests include information security and data mining.