IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 27, 2020, accepted April 4, 2020, date of publication April 7, 2020, date of current version April 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2986338

Simulation of Vehicle Network Communication Security Based on Random Geometry and Data Mining

CHAO WANG, RUNZE SONG, AND ZHAOHUI LIU
College of Transportation, Shandong University of Science and Technology, Qingdao 266590, China
Corresponding authors: Zhaohui Liu (zhaohuiliu@sdust.edu.cn)

This work was supported by the Major Project of Natural Science Foundation of China (NSFC) under Grant 91120306/F03.

ABSTRACT Internet of vehicles is a specific application of Internet of things technology in the field of intelligent transportation. The rapid development of 5G communication technology promotes the development of Internet of vehicles. Car for cellular network communication node random distribution and complex multi-source interference and mobile terminal security calculation ability is limited, this article in view of the actual scene, was proposed based on random geometry contains eavesdropper (Eve) honeycomb - V2V heterogeneous physical layer security system model, the introduction of automatic (PB) as artificial floating vehicle noise, the analysis of cellular network users in the system (CU), V2V users (VU) and interference of the eavesdropper, each user letter simulation with dry to noise ratio (SINR) of the cumulative distribution function, and by using the random geometry tools related safety expression deduction, Then, data mining was carried out on the distance between PB and VU receiver, PB transmitting power and other related variables through genetic algorithm, and the value process was visualized to extract valuable information, providing a mathematical analysis framework and theoretical guidance for the future design, deployment and operation of cellular vehicle network. The results show that the proposed system model can significantly improve the security of vehicle-network communication.

INDEX TERMS Internet of vehicles, communication security, random geometry, data mining, simulation analysis, visualization.

I. INTRODUCTION

Along with the development of the 5G mobile communications, honeycomb vehicle network technology become a research focus in recent years in the field of automatic driving, car networking is auto mobile Internet, car and road, car and car, car and people, cars and real-time information networking and connectivity between the two cities, but the opening of the honeycomb - V2V heterogeneous system characteristics, the communication security problem is very serious. The 5G technology has the characteristics of high speed, large bandwidth, low delay, and the transmission power of the 5G base station increases. Therefore, the received power and interference power of each user in the system will also change, and the impact on legitimate users and illegal eavesdroppers will also change. In the process of automatic driving, the transmitting and receiving ends of V2V users transmit information. Due to the openness of V2V communication, V2V users are faced with security risks such as information leakage and data tampering while obtaining convenient information exchange. If the hacker intercepts the information directly in an end-to-end manner during the information transmission process, obtains relevant information, and then manipulates the autopilot vehicle system through the command and control server to make it a ''zombie vehicle''. As a means of conducting crimes such as extortion, and even triggering a series of traffic accidents, the safety of passengers will be greatly threatened. Therefore, it is of great significance to study the communication safety of autonomous driving.

This paper uses random geometry theory to establish a random distribution model that includes 5G base stations(BS),CU,VU,Eve and PB. According to the communication characteristics, we analyze the signals received by the CU, VU, and Eve in the system, and obtain the cumulative distribution function of the SINR of each user through simulation, we derive closed-form expressions of

The associate editor coordinating the review of this manuscript and approving it for publication was Patrick Hung.

security indicators such as V2V communication connection probability, Eve eavesdropping interruption probability, and V2V communication secure transmission probability, and compare the distance between VU transmitting and receiving ends, PB and The influence of factors such as the distance of the VU receiver and the transmission power of the PB on the security of the communication. We obtain the optimal solution of the secure transmission probability is through the genetic algorithm. Finally, simulation analysis shows that the probability of safe transmission of information in the autonomous driving communication process in the PB system is higher, which proves the rationality of this cellular-V2V heterogeneous system model and probability expressions including PB.

II. LITERATURE REVIEW OR RELATED WORK

V2V communication is one of the important applications of end-to-end (D2D) communication in the field of vehicle networking. Lin and Hsu [1] first proposed the concept of direct data exchange between two nodes without passing through the base station, that is, the concept of end-to-end communication. Many researchers began to combine cellular networks with D2D after the concept of end-to-end communication was proposed. Feng *et al.* [2], Gandotra and Jha [3], and Ziyang [13] began research on multiplexing D2D communication cellular resources, but the initial research focused on resource allocation and power control [10], [11]. With the continuous development of wireless communication, due to its own characteristics such as openness, information leakage, data tampering and other threats will occur in the communication process. Therefore, the communication security problem has begun to attract the attention of researchers. At present, the research on physical layer security has become a hot spot. The physical layer security is based on the Shannon theory proposed in 1948. In 1975, Wyner proposed a model for eavesdropping channels. Korjik *et al.* [4] introduced the concept of eavesdropping channel on the basis of this, and studied to prevent eavesdroppers from stealing information from wireless phones. Wei [17] accurately describes the nature of physical layer security. Kachouh *et al.* [5], Lei *et al.* [6], Dhilipkumar *et al.* [22], and Zhang *et al.* [27] focus on the physical layer security and resource allocation of D2D communication. Mukherjee and Fereidoun *et al.* [7], [8], Weijia [14], Han *et al.* [15], Jie [16], and Wei [17] all applied stochastic geometry theory to wireless communication networks, simplifying the system model. In particular, Prasanna *et al.* [9], and Adeogun [12] used stochastic geometry theory to analyze the downlink connection model in heterogeneous cellular networks. Therefore, based on its research results, this paper will continue to study the downlink communication link model of cellular-V2V containing eavesdroppers. Fangfang [18], Aiqing [19], and Sixue [20] are both studying the problem of communication security transmission on heterogeneous systems and downlinks, but the focus is on the cellular users of the system, so that the interference received by the CU is minimized. Later, in the study of Eve eavesdropping, Mangang *et al.* [21] proposed a beacon as a transmitter to provide artificial noise to interfere with Eve's illegal eavesdropping. With the development of 5G technology, end-to-end communication has begun to be applied to vehicle-to-vehicle communication in the Internet of Vehicles [31]. Pengyu [23] established the V2V wireless channel model in intelligent transportation. Shengnan [24], Yu [25] studied, and Fangming [26] the resource allocation and security of V2V communication respectively. Shi *et al.* [32], and Zardosht *et al.* [33] constructed an application-oriented probabilistic model to evaluate the performance of LTE-V in safety-related applications; Shen *et al.* [34], and Kanchanasut *et al.* [35] discussed the channel estimation problem in V2V communication with 5G background with high mobility environment and non-stationary characteristics.

In summary, car networking communication security issues in the field of study is not yet perfect, along with the widely application of data mining technology, this paper honeycomb in cellular-V2V heterogeneous communication security is studied, using stochastic geometry tool V2V communications connection probability was deduced, the interruption of Eve eavesdropping probability and V2V communication transmission probability safety indexes such as the safety of the closed expression, data mining through the genetic algorithm for complex expressions, to extract valuable information for the future of cellular network design and deployment operations provide mathematical analysis frame and theory guidance.

III. CELLULAR-V2V HETEROGENEOUS SYSTEM MODEL

With the popularity of 5G technology, especially the high latency of V2V communication in the field of car networking [36], it is necessary to increase the bandwidth. Therefore, the transmission power of the 5G base station is larger than that of the 4G and the previous base station, which also provides a new method for the base station and the floating vehicle to transmit the interference signal to prevent the illegal behavior of the eavesdropper in the system [37].

A. SCENE MODEL

The paper studies the communication security of random cellular-V2V heterogeneous systems in the car network area. Thesystem model includes 5G base station (BS), cellular network user (CU), V2V user (VU), eavesdropper (Eve) and autopilot floating vehicle (PB). All base stations and users are equipped with a single antenna, and the distribution of CU, VU, Eve, and PB satisfies the Poisson point distribution process of stochastic geometric theory. The scenario model of establishing a cellular-V2V heterogeneous system based on this is shown in Figure. 1

In this scenario, all users are located within the coverage area of the base station, and communication between users is completely controlled by the network infrastructure of the operator. The operator is responsible for user identity authentication, access control, connection establishment, resource allocation and security management. V2V communication

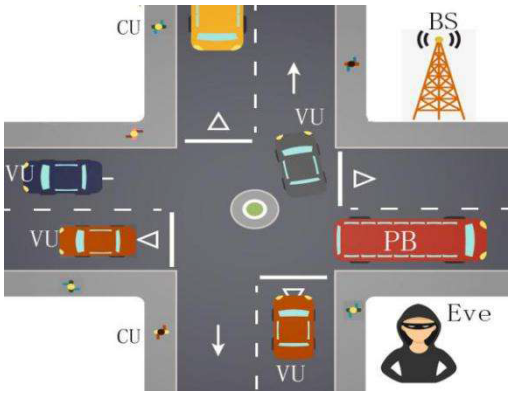

FIGURE 1. Cellular-V2V heterogeneous system scene model.

links share the spectrum resources of normal cellular systems and can be applied to local services, such as local content sharing V2V direct communication is performed between the transmitting and the receiving of the VU, and the CU communication needs to pass through the BS first and then to the receiving end [29]. Eve intercepts the V2V link. The PB provides signals to the legitimate users VU and CU [30]. At the same time, Eve emits artificial noise to affect the quality of the eavesdropping channel [39], thereby improving the communication security of the cellular-V2V heterogeneous system and preventing the V2V communication application from being automatically Information leakage and tampering occurred during the communication of driving vehicles.

B. SIMULATION MODEL

In order to describe the random locations of cellular users, V2V users, eavesdroppers, and autopilot floating vehicles in the cellular-V2V heterogeneous system, we model the system and simulate using the Poisson point process of stochastic geometry theory: All users are nodes randomly distributed in a two-dimensional plane [38], and the position satisfies the Poisson point distribution process. There is a 5G base station with N antennas in the center. The coverage area is a circle with a length of R = 500m. M single antenna users are randomly distributed in the coverage area of the 5G base station, where we have N>M. VUs and autonomous floating vehicles can only be distributed in the lane due to their driving characteristics,and the solid line area indicates that the lane range is 600×1000 m^2. For the convenience of analysis, it is assumed that this system model contains 4 pairs of V2V users and 1 unmanned floating vehicle. The algorithm for establishing the system model is shown in Algorithm 1. The random distribution model of each user in the cellular-V2V heterogeneous system established by the above algorithm is shown in Figure. 2.

With the popularization of the 5G mobile communication technology,which will result in uneven distribution of signal transmission nodes, which is one of the important communication characteristics in the 5G era [40]. In order to better conform to the communication system model in the actual vehicle network,it is necessary to study the system model of

Algorithm 1 System Model Algorithm

1) Generate a random number Z following the N (0,1).
2) Calculate $\mu = \Phi(Z)$, then μ obeys uniform distribution on (0,1)
3) Follow the steps below to calculate the inverse function F_β^{-1} of the poisson distribution function to find m$*$
$*\mathrm{m}_0 = \max([\beta + Z\beta], 0)$
$*$ If $F_\beta(m_0) < \mu$,Then make $\mathrm{m}_0 = 1+\mathrm{m}_0$ until $F_\beta(m_0) > \mu$, and $\mathrm{m}* = \mathrm{m}_0$
$*$ If $F_\beta(m_0) > \mu$,Then make $\mathrm{m}_0 = \mathrm{m}_0 - 1$ until $F_\beta(m_0) < \mu$, and $\mathrm{m}* = \mathrm{m}_0 + 1$
4) Set the 5G base station as the center and the radius r=500m coverage area
5) Finally, determine the random position of the user in the model by
$\mathrm{x(i)}=500+\mathrm{r} \times \mathrm{sqrt}(\mathrm{m}_{11}*) \times \cos(2\pi \times \mathrm{m}_{12}*)$,
$\mathrm{y(i)}=500+\mathrm{r} \times \mathrm{sqrt}(\mathrm{m}_{21}*) \times \cos(2\pi \times \mathrm{m}_{22}*)$
6) End

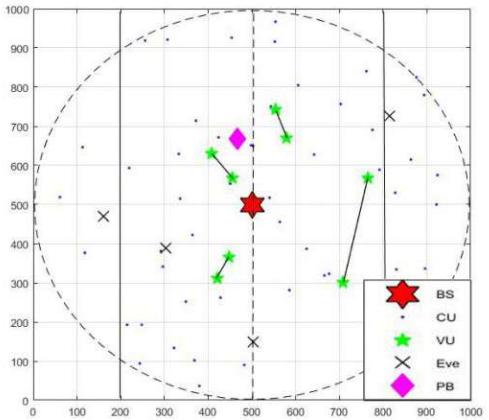

FIGURE 2. User-random distribution model of cellular-V2V heterogeneous system.

the uneven network, and use the stochastic geometry theory and the Poisson point distribution process to carry out modeling and simulation.

C. DOWNLINK COMMUNICATION LINK MODEL

Xu [18] studied the multiplexed uplink of D2D communication embedded in cellular network, and selected CU connection probability and security probability as security metrics. In view of the research goal of the communication safety of autonomous vehicles, the communication priority of the VU is higher than that of the CU, because the CU will not interfere with the VU when the V2V communication multiplexes the downlink resources of the cellular network. Therefore, the downlink is selected as the research model for modeling analysis [28], and the autopilot floating vehicle is introduced as the beacon to improve the safety of the automatic driving. The downlink communication link model of the cellular-V2V heterogeneous system is shown in Figure. 3.

This paper focuses on passive eavesdropping environments. Specifically, eavesdropping nodes in the system

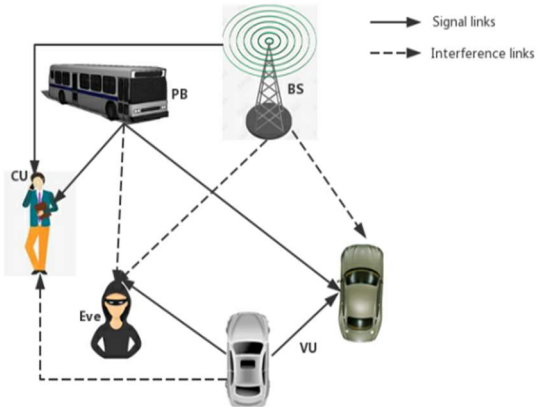

FIGURE 3. Downlink communication link model.

cannot forward collusion with each other, but they can eavesdrop on the downlink communication link of a cellular-V2V heterogeneous system in the entire frequency band, and at the same time the eavesdropping node can eavesdrop and decrypt only one of the links. We generally consider the worst case in the network, that is, the eavesdropping information of the eavesdropping end is determined by the Eve of the largest receiving SINR among all eavesdropping nodes in the system.

A circle with a radius of R=500m centered on a 5G Cellular base station (BS) is selected as a signal coverage area. Considering the case where each user is equipped with a single antenna, the transmission power of the BS to each user is P_{BS}. The location of the CU in this region obeys the Poisson point process of stochastic geometric theory Φc, and the location of VU is marked as Φv. The autopilot floating vehicle in the system model acts as a radio beacon (PB) to transmit signals P_{PB} to all users in the area. Assuming that the information content is known to the legal CU, VU, it can obtain energy from the signal. The illegal Eve receives this unknown signal as an artificial noise, thereby weakening Eve's Signal to Interference and Noise Ratio (SINR) and improving the security of the system. Other relevant variables are defined in Table 1.

Formulas (1)-(3) respectively represent all signal vectors received by the CU, VU receiver and Eve in this cellular-V2V heterogeneous system model are respectively Y_{CU}, $Y_{\mathrm{VU\_RX}}$ and Y_{Eve},

$$Y_{CU} = \sqrt{P_{BS}}g_{BS,CU}x_{BS} + \sqrt{P_{PB}}g_{PB,CU}x_{PB} + \sqrt{P_{VU}}g_{VU,CU}x_{VU} + n_{CU} \quad (1)$$

$$Y_{\mathrm{VU\_RX}} = \sqrt{P_{VU}}g_{VU,VU}x_{VU} + \sqrt{P_{PB}}g_{PB,VU}x_{PB} + \sqrt{P_{BS}}g_{BS,VU}x_{BS} + n_{VU} \quad (2)$$

$$Y_{Eve} = \sqrt{P_{VU}}g_{VU,Eve}x_{VU} + \sqrt{P_{PB}}g_{PB,Eve}x_{PB} + \sqrt{P_{BS}}g_{BS,Eve}x_{BS} + n_{Eve} \quad (3)$$

Among them, x_{BS}, x_{VU} and x_{PB} are the downlink data information vectors transmitted by BS, VU and PB respectively. $g_{\mathrm{i,j}}$ represents the channel gain vector between i and j. For example, $g_{BS,CU}$ represents the channel gain vector of the BS to CU. This paper mainly considers path loss and small-scale fading, namely $g_{i,j} = \varphi_{i,j}d_{i,j}^{-\alpha}$. $\varphi_{i,j}$ determines the fading coefficient of the i to j channel. For example, $g_{BS,CU} = \varphi_{BS,CU}d_{\mathrm{BS,CU}}^{-\alpha}$; n_{i} represents it's own additive white Gaussian noise. Considering the influence of path loss and small-scale fading on the communication security performance of the cellular-V2V system model, the path loss model of the signal is expressed as $d_{i,j}^{-\alpha}$, α is the path loss coefficient; for small-scale fading of the signal, this article assumes that all links are Experiences Rayleigh fading independently.

Then calculate the signal to interference and noise ratio $SINR_{CU}$, $SINR_{VU}$ and $SINR_{\mathrm{Eve}}$ of CU, VU and Eve according to the above parameters.

$$SINR_{CU} = \frac{P_{BS}\mathrm{h}_{BS,CU}}{I_{CU} + N_{CU}} \quad (4)$$

TABLE 1. List of the major variables.

VARIABLE	DEFINTION
Y_{CU} 、 $Y_{\mathrm{VU\_RX}}$ 、 Y_{Eve}	All signal vectors received by the CU, VU receiver and Eve in this cellular-V2V heterogeneous system model
x_{BS} 、 x_{VU} 、 x_{PB}	The downlink data information vectors transmitted by BS, VU and PB
P_{BS} 、 P_{CU} 、 P_{VU} 、 P_{PB}	Transmit power of BS、CU、VU and PB
$g_{\mathrm{i,j}}$	The channel gain vector between i and j
$\varphi_{i,j}$	The fading coefficient of the i to j channel
$d_{i,j}$	Distance between i and j
n_{i}	It's additive white Gaussian noise
I_{CU} 、 I_{VU} 、 I_{Eve}	Indicates the interference power received by the CU、VU and Eve
$\mathrm{h}_{\mathrm{i,j}}$	The channel gain between i and j
N_{CU} 、 N_{VU} 、 N_{Eve}	The noise power of the CU itself、VU itself and Eve itself
$SINR_{\mathrm{i}}$	The signal to interference and noise ratio of i
C_{VU} 、 C_{Eve}	Real-time channel capacity of VU and Eve
R_c 、 R_s 、 R_{e}	Information transmission rate、Safe transfer rate、Safe redundant rate
β_{VU} 、 β_{Eve}	SINR threshold for communication connection
$E_{\phi vu}$	The expectation of all randomly distributed VU communication connection probabilities
$E(d_{\mathrm{i,j}})$	Mean of distances between i and j for all randomly distributed

Among them, the interference I_{CU} indicates the interference power received by the CU, mainly including the interference generated by the PB and the interference generated by the VU transmitter. $h_{BS,CU}$ refers to the channel gain between the BS and the CU, and N_{CU} indicates the noise power of the CU itself.

$$SINR_{VU} = \frac{P_{VU}h_{VU,VU} + P_{PB}h_{PB,VU}}{I_{VU} + N_{VU}} \tag{5}$$

Among them, the interference I_{VU} indicates the interference power received by the VU, mainly the interference generated by the BS to the VU receiver. $h_{VU,VU}$ and $h_{PB,VU}$ represent the channel gain between the VU transmitter and receiver and the channel gain between the PB and VU receivers, respectively. N_{VU} refers to the noise power of the VU itself.

$$SINR_{Eve} = \frac{P_{VU}h_{VU,Eve}}{I_{Eve} + N_{Eve}} \tag{6}$$

Among them interference I_{Eve} indicates the interference power received by Eve, mainly including the interference generated by PB and the interference generated by BS. $h_{VU,Eve}$ indicates the channel gain between the VU transmitter and Eve, and N_{Eve} indicates the noise power of the eavesdropper itself.

For the cellular-V2V heterogeneous communication system applied in the field of automatic driving, inter-vehicle communication has extremely high requirements for low delay due to its own characteristics such as fast moving speed of the vehicle. In particular, shop floor communication involving safety control or early warning requires high real-time performance. Then the secure transmission probability of the selected information is described as a metric for the safety of the autonomous driving communication. In order to ensure the safety of V2V communication in autonomous driving, this paper is based on the Wyner model. Information transmission rate is Rc,secure transmission rate is Rs, and security redundancy rate is $R_e = R_c - R_s$.

A reliable connection of V2V communication can be achieved only when the instantaneous channel capacity C of the receiving user in the downlink communication link is greater than the information transmission rate Rc.

$$C = \log 2(1 + SINR) \tag{7}$$

$$C_{VU} = \log 2(1 + SINR_{VU}) > Rc \tag{8}$$

If the instant channel capacity of Eve is greater than the safety redundancy rate, the communication of the MIMO-V2V system is safely interrupted, thereby ensuring the security of information transmission during the automatic driving process and preventing the eavesdropper from obtaining important information.

$$C_{Eve} = \log 2(1 + SINR_{Eve}) > Re \tag{9}$$

The expression of the safe transmission rate can be obtained from the above formula:

$$Rs = \log 2(1 + SINR_{vu}) - \log 2(1 + SINR_{Eve}) \tag{10}$$

According to the monotonic nature of the log function itself, the security problem of information transmission of V2V communication is transformed into the relationship between SINR and its threshold. By calculating the critical value of SINR,we study the safety performance metrics of cellular-V2V system in autonomous driving. Therefore, in this paper, combined with the changes brought by 5G technology, the cumulative distribution function of SINR of CU, VU and Eve in this cellular-V2V system is obtained by setting the following parameters. Thus, the approximate range of the SINR of CU, VU, and Eve is obtained.

Due to the popularity of 5G technology, especially the high latency of V2V communication in the field of car networking, it is necessary to increase the bandwidth. Therefore, the transmission power of the 5G base station is larger than that of the 4G and the previous base station. According to this new change brought by the 5G base station, the interference suffered by the CUuser and the VU user is minimized. Assume that the base station transmits power to each user. P_{BS} = 53dbm, CU transmit power P_{CU} = 14dbm, The transmit power of the VU transmitter is P_{VU} = 17dbm. The power of the unmanned floating car is P_{PB} = 33dbm. The distribution of each user's position obeys the Poisson point process, which assumes that the maximum distance between the receiving end and the transmitting end of the V2V is 40m, the minimum distance is 1m, and the path loss coefficient is $\alpha = 4$. The system bandwidth is 10 MHz, and we obtain the SINR cumulative distribution function graphs of CU, VU, and Eve by simulation, as shown in Figure. 4.

By setting the above parameters for simulation, we obtain the SINR cumulative distribution function of CU, VU and Eve. Therefore, the specific value distribution of each user's SINR in the downlink model of this cellular-V2V heterogeneous system is known. The comparison can prove that the model is reasonable.

IV. ANALYSIS OF V2V COMMUNICATION SAFETY

In the cellular-V2V heterogeneous system, when the VUs communicate with each other, the resources of the cellular network link are multiplexed. According to the established downlink communication model, the VU is not interfered by the CU. Therefore, this paper selects the downlink communication link as the research object. In the process of automatic driving communication, it is necessary to ensure that the interference received by the VU is as small as possible, and to achieve reliable connection of V2V communication, that is, a minimum threshold value should be set for the SINR to be constrained. According to formulas (7)-(10) and related definitions, the expressions of V2V communication connection probability, combined with the random geometry theory, we get the eavesdropping interruption probability and secure transmission probability of V2V communication.

A. COMMUNICATION CONNECTION PROBABILITY

According to the derivation of formulas (7)-(10), combined with the monotonic characteristics of the log function,

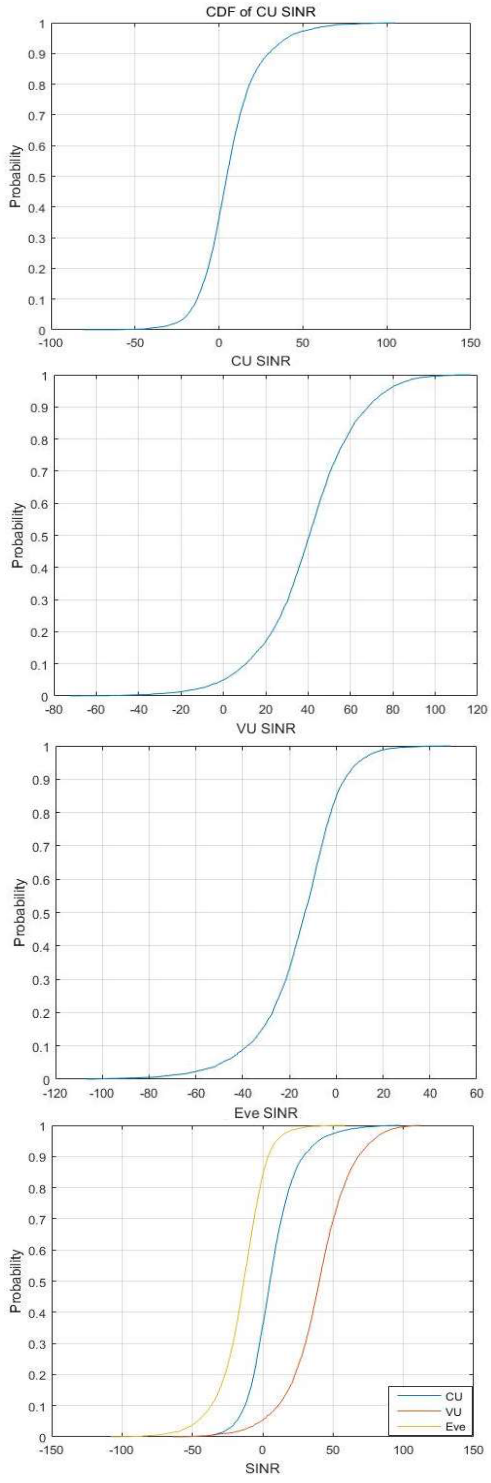

FIGURE 4. SINR cumulative distribution function and comparison chart for each use.

thesuccessful connection condition $SINR_{VU} > \beta_{VU}$ of the V2V user can be obtained. Among them, βVU represents SINR threshold for communication connections between V2V users. If $SINR_{VU} < \beta_{VU}$, then the V2V link cannot be successfully connected. The derivation process of the closed-form expression of the communication connection probability of the V2V user is as follows:

$$\begin{aligned} &P_{con}^{vu}(\beta_{VU}) \\ &\quad = 1 - E_{\phi vu}[P(\varphi \le \frac{(I_{VU} + N_{VU})\beta_{VU}}{P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha}})] \\ &\quad = e^{-[(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} N_{VU}]} \\ &\qquad \times E_{I\mathrm{vu}}(e^{-[(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} I_{\mathrm{vu}}]}) \end{aligned} \tag{11}$$

Among them, $E_{\phi vu}$ represents the expectation of all randomly distributed VU communication connection probabilities within the system model, g obeys the Rayleigh distribution hypothesis, and is derived from the characteristics of the Rayleigh channel. The power fading coefficient φ obeys an exponential distribution with a parameter of 1, to simplify the calculation. Suppose $\varphi_{VU,VU}$ and $\varphi_{VU,PB}$ are the same constant and marketed as φ. Then, get the solution to $E_{I\mathrm{vu}}(e^{-[(PVUd_{VU,VU}^{-\alpha} + PPBd_{VU,PB}^{-\alpha})^{-1} \beta VUI\mathrm{vu}]})$. According to the above hypothesis $\varphi_{\mathrm{BS,VU}}$ obeys the exponential distribution with a parameter of 1, you can get the following expression:

$$\begin{aligned} &E_{I\mathrm{vu}}(e^{-[(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} I_{\mathrm{vu}}]}) \\ &= \frac{1}{1 - [-(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} P_{BS} d_{BS,VU}^{-\alpha}]} \\ &= E_{d_{BS,VU}}(\frac{1}{1 + \kappa d_{BS,VU}^{-\alpha}}) \end{aligned} \tag{12}$$

In which, $\kappa = (P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} P_{BS}$ Here, according to

the derivation in Lee *et al.* [10], the following approximation is obtained:

$$E_{d_{BS,VU}}(\frac{1}{1 + \kappa d_{BS,VU}^{-\alpha}}) \simeq (1 + \frac{\kappa^{2/\alpha}}{[E(d_{BS,VU})]^2})^{-1}$$

Among them, $E(d_{BS,VU}) = 2\mathrm{R}/3$. Put the above formula $E(d_{BS,VU}) = 2\mathrm{R}/3$ into $P_{con}^{vu}(\beta VU)$ to get the closed expression of the final V2V user communication connection probability:

$$\begin{aligned} &P_{con}^{vu}(\beta_{VU}) \\ &\quad = (1 + \frac{[(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} P_{BS}]^{2/\alpha}}{[E(d_{BS,VU})]^2})^{-1} \\ &\qquad \times e^{-[(P_{VU} d_{VU,VU}^{-\alpha} + P_{PB} d_{VU,PB}^{-\alpha})^{-1} \beta_{VU} N_{VU}]} \end{aligned} \tag{13}$$

B. EAVESDROPPING PROBABILITY

Under the premise of ensuring normal connection between V2V users, let us study the outage probability of Eves on V2V link eavesdropping. Assume that all Eve in this system can eavesdrop on the VU. If there is Eve's SINR for V2V link eavesdropping is greater than the threshold β_{Eve}. Then, the V2V user communication interruption causes the eavesdropping to be interrupted, thereby ensuring the security of information transmission. Therefore, we take the Eve with the largest SINR for discussion and obtain the following

expression based on the deduced results.

$$P_{Int}^{vu}(\beta_{Eve}) = P(SINR_{Eve} > \beta_{Eve}) = e^{-(P_{VU}^{-1} d_{VU,Eve}^{\alpha} N_{Eve} \beta_{Eve})} E_{I_{Eve}}[e^{-(P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve} I_{Eve})}] \quad (14)$$

Among them, the interference $IEve$ refers to the interference power received by Eve, mainly including the interference generated by PB and the interference generated by BS configured with multiple antennas, which is:

$$I_{Eve} = I_{Eve,BS} + I_{Eve,BS} = P_{BS} d_{BS,Eve}^{-\alpha} g_{BS,Eve} + P_{PB} d_{PB,Eve}^{-\alpha} g_{PB,Eve}$$

Then, continue the deduction of $E_{I_{Eve}}$:

$$\begin{aligned} & E_{I_{Eve}}[e^{-(P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta Eve I Eve)}] \\ &= E_{d_{BS,Eve}}\left(\frac{1}{1 + P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve} P_{BS} d_{BS,Eve}^{-\alpha}}\right) \\ &\quad \times E_{d_{PB,Eve}}\left(\frac{1}{1 + P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve} P_{PB} d_{PB,Eve}^{-\alpha}}\right) \\ &= \left[1 + \frac{(P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve} P_{BS})^{\alpha/2}}{[E(d_{BS,Eve})]^2}\right]^{-1} \\ &\quad \times \left[1 + \frac{(P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve} P_{PB})^{\alpha/2}}{[E(d_{PB,Eve})]^2}\right]^{-1} \end{aligned} \quad (15)$$

Among them, $E(d_{BS,Eve}) = 2R/3$, $E(d_{PB,Eve}) = 128R/45\pi$, and set $\mu = P_{VU}^{-1} d_{VU,Eve}^{\alpha} \beta_{Eve}$.

The closed expression of the probability of Eve eavesdropping is obtained by substituting the above formula into the original form:

$$P_{Int}^{vu}(\beta Eve) = \left[1 + \left(\frac{3}{2R}\right)^2 (\mu P_{BS})^{2/\alpha}\right]^{-1} \times \left[1 + \left(\frac{45\pi}{128R}\right)^2 (\mu P_{PB})^{2/\alpha}\right]^{-1} e^{-(\mu N Eve)} \quad (16)$$

C. SECURE TRANSMISSION PROBABILITY

The closed expression of VU communication connection probability and Eve eavesdropping probability is obtained above. When Eve's SINR for V2V link eavesdropping is less than the threshold β_{Eve}, the V2V link communication does not interrupt, that is, the information transmission is reliable. Therefore, the probability at this time is defined as the probability of safety without interruption, that is, $P_{\text{sec}}^{vu}(\beta Eve) = 1 - P_{Int}^{vu}(\beta Eve)$. Then, according to the definition of the secure transmission probability of the end-to-end communication link in [18], and Combined with the downlink communication link model of the cellular-V2V heterogeneous system in this paper, the expression of the secure transmission probability P_{tsp}^{vu} of the V2V link in the vehicle networking scenario is obtained.

$$P_{tsp}^{vu} = P_{con}^{vu}(\beta VU)[1 - P_{Int}^{vu}(\beta Eve)] \quad (17)$$

TABLE 2. Simulation parameter.

Simulation Parameter	Value
Community radius/m	500
5G base station's transmit power /dBm	53
Cellular user transmit power /dBm	14
V2V transmitter's transmit power /dBm	17
Transmitting power of autonomous floating vehicles /dBm	33
Road loss coefficient	4
System bandwidth /MHZ	10

V. ANALYSIS OF V2V COMMUNICATION SAFETY

Extracted from the complex expression and access to large amounts of data into useful information for the deployment of the operation to provide theoretical guidance for car networking communication and analysis, this section through the genetic algorithm, is derived from the nonlinear closed dig up the implicit in the expression, the relationship between potential value to decision, patterns and trends, and used the knowledge and rules based cellular network simulation model, seek security in the transmission probability and the optimal solution of this kind of nonlinear problem, and through the experiment to prove the rationality of the algorithm and adaptive.

According to the derived expressions (13)-(17), the distance between the VU transmitter and receiver, the distance between the PB and VU receivers, and the PB transmit power are related to the safety of the autonomous communication. The VU connection probability, eavesdropping outage probability and safe transmission probability are simulated in the downlink communication link model of the cellular-V2V heterogeneous system. The safety transmission probability of V2V communication in this system before and after the introduction of the autopilot floating vehicle is compared, and the rationality of the probability expression derived based on the cellular-V2V downlink system model is verified.

In the simulation process, the downlink communication link of the cellular-V2V heterogeneous system includes 5G base station, CU, VU, Eve, and PB. We assume that the minimum distance between users is 1m, and the maximum distance that VU users can communicate is 40m. In order to simplify the calculation, any pair of V2V communication in the cell is independent of each other and does not interfere with each other, its position distribution obeys Poisson point process. The specific simulation parameters are shown in Table 2.

When V2V user distances $d_{VU,VU}$ are 10m, 20m, 30m and 40m, the variation of the V2V user communication connection probability with the SINR threshold is shown in Figure 5. It can be seen from the figure that the probability of V2V user communication connection decreases with the

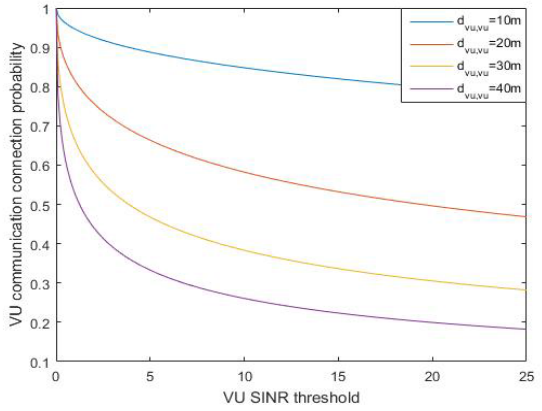

FIGURE 5. Influence of VU distance on its communication connection probability.

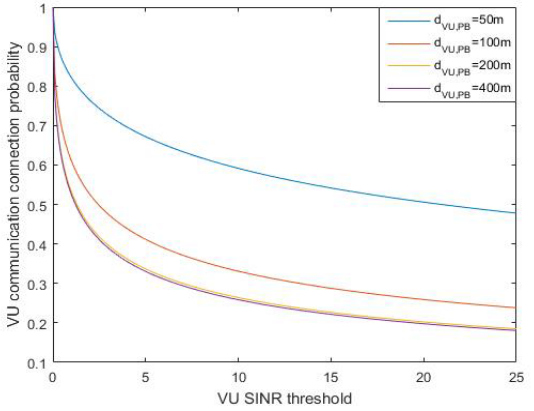

FIGURE 6. Influence of VU and PB distance on VU communication connection probability.

increase of $d_{VU,VU}$. When the V2V transmitter and receiver are close together, the communication connection probability is extremely high and does not change much with the SINR threshold. As the distance between the two increases, the connection probability decreases rapidly with the increase of the SINR threshold.

When the distance between the VU receiving end and the unmanned floating vehicle is $d_{VU,PB}$, 50m, 100m, 200m, and 400m, the V2V user communication connection probability varies with the SINR threshold as shown in Figure 6. It can be seen from the figure that the probability of V2V user communication connection decreases with the increase of $d_{PB,VU}$. And when the distance between VU and PB exceeds 200m, the communication connection probability is less affected by this factor. The distance between VU and PB has a significant influence on the probability of VU communication connection. Next, assuming that the distance between VU and PB is 250m, we simulate the influence of the probability of PB transmission on the probability of V2V user communication connection.

Assume that the distance between V2V users is always at a maximum of 40m. When the transmitting power of the self-driving floating vehicle as the beacon PB is 33dbm, 43dbm, 53dbm, 63dbm, respectively, the V2V user communication

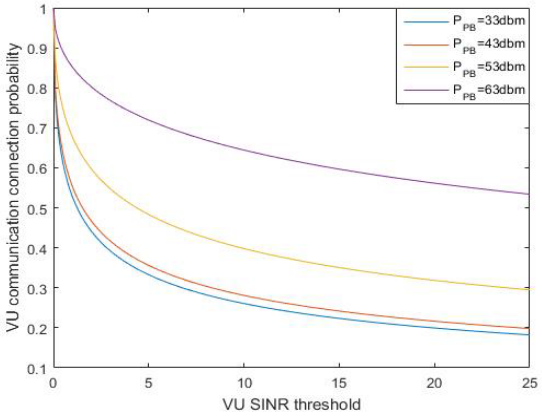

FIGURE 7. Influence of PB transmit power on VU communication connection probability.

connection probability changes with the SINR threshold as shown in Figure 7. It can be seen from the figure that the greater the transmission power of the autonomous floating vehicle as a beacon, the higher the V2V user communication connection probability. When the transmission power is reduced to about 40 dbm, the connection probability is less affected by this factor, and the actual system needs to be considered in combination with energy consumption and resource allocation.

The communication connection probability of V2V users is simulated from the distance between the transmitting and receiving ends of the VU, the distance between the PB and the VU receiving end, and the PB transmitting power. The results are reasonable. This provides a new way to improve the safety of communication for autonomous driving.

Next, from Eve's simulation analysis of the eavesdropping outage probability of V2V communication, that is, when Eve'sSINR exceeds the threshold, V2V communication is interrupted to ensure that information is not eavesdropped. At this time, the state of V2V is defined as an unsafe state. The following is simulated from the distance between VU and Eve and the power of the PB of the self-driving floating vehicle, and the change of the probability of eavesdropping with the threshold is discussed.

As the SINR threshold of Eve increases, the probability of eavesdropping interruption will decrease, as shown in Figure 8. As the SINR threshold of Eve increases, the probability of eavesdropping interruption will decrease. For example, when the signal transmitted by the PB is larger, the interference signal received by Eve as an illegal user is larger. Therefore, the probability that a V2V user can maintain normal communication is greater, the probability of eavesdropping is small, and the probability of eavesdropping is smaller. As shown in Figure 8.

When the distance between Eve and VU is closer, the path loss of the signal is smaller. Therefore, the higher the probability of eavesdropping, the more realistic the actual situation of the car network communication system is. At this time,

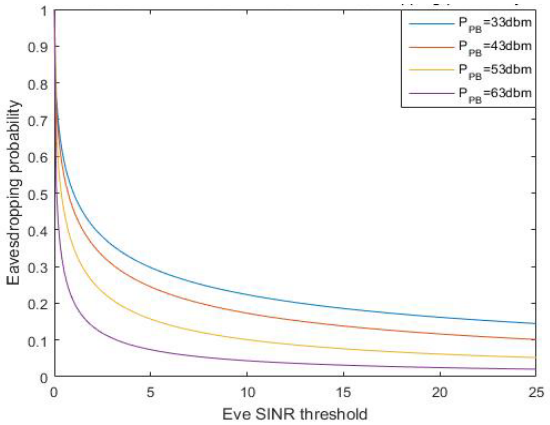

FIGURE 8. Influence of PB transmit power on eve eavesdropping outage probability.

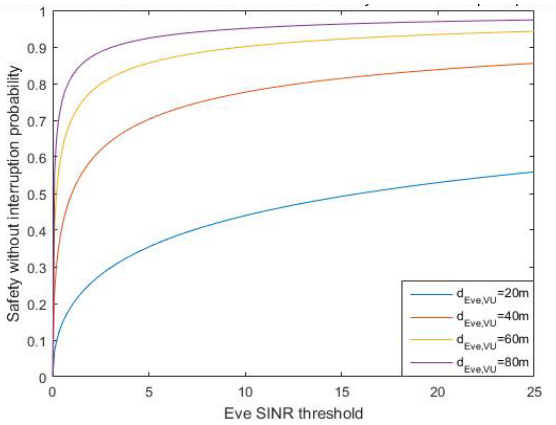

FIGURE 10. Influence of Eve and VU distance on the probability of uninterrupted safety.

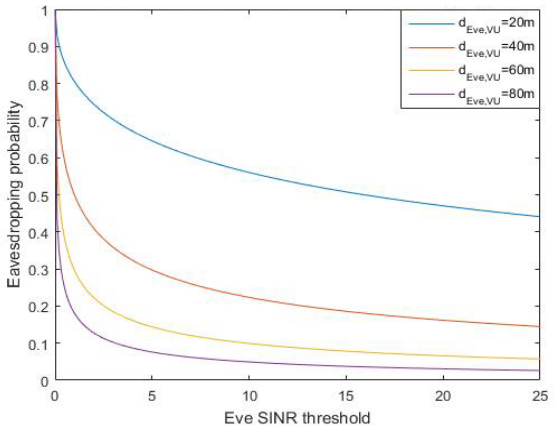

FIGURE 9. Influence of Eve and VU distance on the probability of Eve eavesdropping.

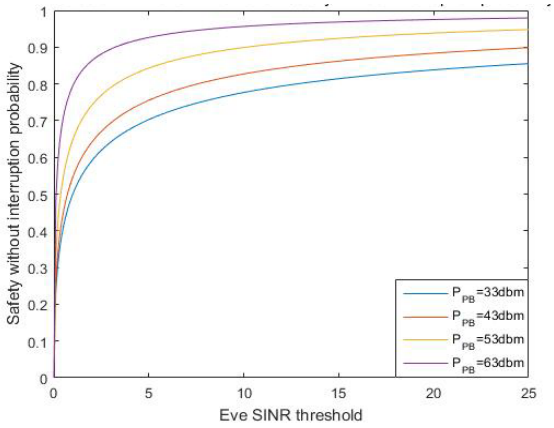

FIGURE 11. Influence of PB transmit power on safety uninterrupted probability.

the information between the V2V users cannot be transmitted securely, and normal communication cannot be established, so the probability of eavesdropping interruption is higher. And the probability of eavesdropping is gradually reduced as the distance between Eve and VU increases, as shown in Figure 9.

When Eve taps the V2V link, the SINR is less than the threshold value $\beta_{E\mathrm{ve}}$, the V2V link communication does not interrupt, that is, the information transmission is reliable, so the probability at this time is defined as the security uninterrupted probability, that is, $P_{\mathrm{sec}}^{vu}(\beta Eve) = 1 - P_{Int}^{vu}(\beta Eve)$. The simulation is carried out from two aspects of the distance between VU and Eve and the power of PB of unmanned floating vehicle, and discusses the change of safety uninterrupted probability with threshold.

The closer the distance between the legitimate VU and the illegal Eve user in the cellular-V2V heterogeneous system, the higherthe probability of eavesdropping and the worse the reliability of information transmission between V2V users. Therefore, the probability of uninterrupted security is lower. As the distance between VU and Eve increases, the probability of uninterrupted security presents an increasing trend, as shown in Figure 10.

At this time, $d_{VU,E\mathrm{ve}} = 40\mathrm{m}$. When the transmission power of the autopilot floating vehicle PB in this cellular-V2V heterogeneous system is larger, the interference power to Eve is increased, and Eve's eavesdropping ability is worse. Therefore, the probability of uninterrupted security is higher, and the trend of increasing is presented, as shown in Figure 11.

Then, according to the definition and expression of $P_{con}^{vu}(\beta VU)$ and $P_{Int}^{vu}(\beta Eve)$ as well as the relationships with each parameter system, changes of P_{tsp}^{vu} can be obtained through comprehensive analysis. The data mining technology based on genetic algorithm is used to find the optimal solution of the safe transmission probability. The information transmission security problem of V2V communication is simulated, and the objective function is:

$$P_{tsp}^{vu} = P_{con}^{vu}(\beta VU)[1 - P_{Int}^{vu}(\beta Eve)],$$

$P_{con}^{vu}(\beta VU)$ and $P_{Int}^{vu}(\beta Eve)$ is shown in formulas (13) and (15).

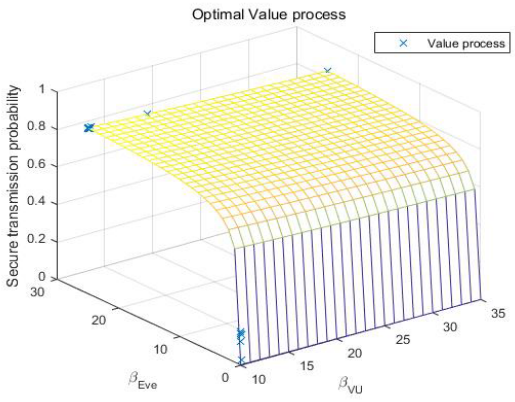

FIGURE 12. Data mining value process.

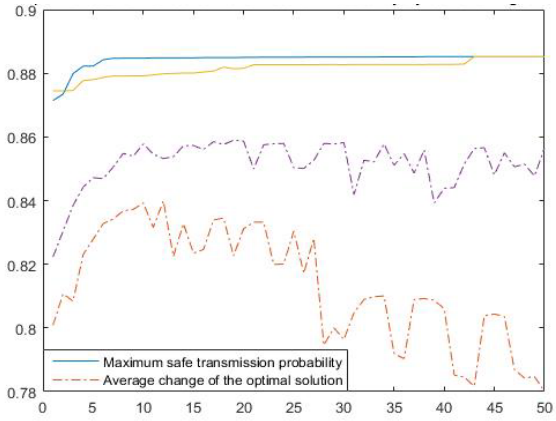

FIGURE 13. Simulation process of safe transmission probability's optimal solution.

The benefit matrix is randomly generated, and the maximum number of iterations is set to 50, the number of individuals is 40, and the generation gap is set to 0.9. The objective function, the closed expression of the safe transmission probability, is set as the fitness function. The independent variable is the threshold β_{VU} and β_{Eve}. The distance between the transmitting end and the receiving end of the VU is average, that is:

$$d_{VU,VU} = 20m, \quad d_{VU,PB} = 50m.$$

The other parameters are unchanged, and the optimal solution is obtained by the operation of algorithm selection, crossover, mutation, etc. The value of the safe transmission probability is shown in Figure. 12.

We find that the value of the optimal solution for finding the safe transmission probability is mostly concentrated in the upper left corner of the function surface graph, and the SINR cumulative distribution function of VU and Eve from the simulation experiment is shown in Figure 4. According to the above experimental results, we select the appropriate value range of SINR threshold, the value range of β_{VU} is 10-35 db, and the value range of β_{Eve} is 0-25 db. Then, according to the setting of the above parameters, we perform simulation experiments to observe the optimal solution of the objective function., that is, the maximum value of the safe transmission probability and the change of the average value of the optimal solution in each iteration. Through many experiments, the results show that the algorithm has good convergence for solving the maximum value of the safe transmission probability, and the optimization efficiency is high, and the number of iterations is small, which is suitable for solving this problem. Figure 13 shows two independent data mining simulation experiments. We can clearly find that although the average of each of the safe transmission probability solutions differs greatly in the two experiments, the final convergence results are consistent, that is, the maximum value of the obtained safety transmission probability is consistent.

Return the maximum value according to the simulation experiment and output the two independent variable thresholds β_{VU} and β_{Eve} when the maximum probability of safe transmission is output. Assuming that the system parameters are unchanged, the threshold value obtained by making the above-mentioned secure transmission probability to the maximum value is taken, that is, $\beta VU = 10$db, $\beta Eve = 25$db. The distance between the transmitting end and the receiving end of the VU is average, that is, $d_{VU,VU} = 20m$. Considering the communication connection probability and safety non-disruption probability of V2V users, the variation of safe transmission probability of V2V link with PB transmitting power is simulated

First, the probability of information transmission in the process of automatic driving communication increases with the increase of the transmitting power of the self-driving floating car PB. The greater the PB transmit power, the greater the probability of safe transmission, and as the distance between VU and PB decreases, the probability of safe transmission increases. Particularly, when $d_{VU,PB} < 50m$, the changes of safe transmission probability $d_{VU,PB}$ are relatively obviously. This is in line with the situation in the actual system, when the distance is similar, the path loss of the received signal is small. Therefore, the received signal is large, the SINR is increased, and the channel capacity is also increased, so the probability of being greater than the threshold is increased. Therefore, the probability of safe transmission increases with the decrease of $d_{VU,PB}$, as shown in Figure 14.

In order to prevent the leakage of information when the V2V communication of the self-driving vehicle is weakened,Eve's eavesdropping ability is weakened, and the communication safety of the autonomous driving is improved. On the basis of the cellular-V2V heterogeneous system model, an autopilot floating vehicle is introduced as a beacon to transmit signals. The following is a comparison of the safe transmission probability of a cellular-V2V heterogeneous system before and after the introduction of an autonomous floating vehicle. Figure 15 shows the comparison of the context of the safe transmission probability of introducing autonomously driven floating vehicle as a PB. Suppose $P_{PB} = 53$dbm at this time, The introduction of automatic

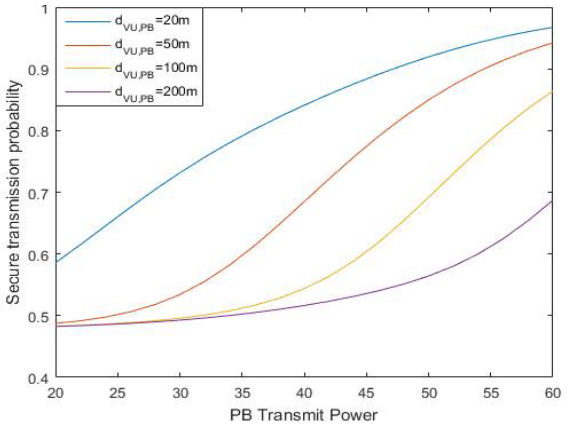

FIGURE 14. Simulation analysis diagram of safe transmission probability.

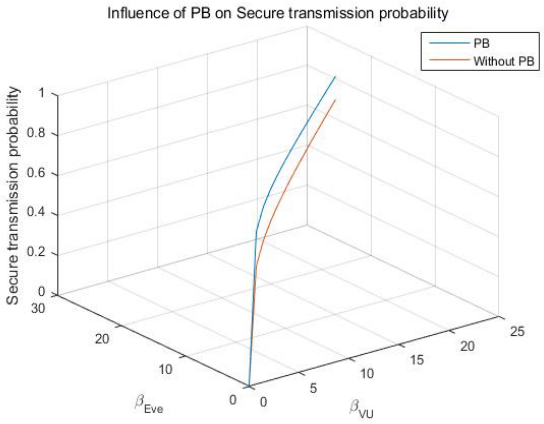

FIGURE 15. Comparison of the relationship between the probability of safe transmission before and after the introduction of PB.

driving floating vehicle as PB system, legitimate users know the information content, the signal can be used as a receiving signal, but illegal users do not know the information content, the signal can be used as a kind of artificial noise, reduce its eavesdropping ability, so as to ensure the safe transmission of information in the process of automatic driving communication. It can be seen from the experimental results that the information security transmission probability of the automatic driving communication process in the PB-introduced system is higher, which proves the rationality of the system model and the simulation experiment.

VI. CONCLUSION

The existence of the Internet of vehicles makes people's travel more intelligent. Mining the value behind the large amount of data stored in the Internet of vehicles and analyzing it effectively is the basis of intelligent application, and it is also one of the methods to improve the security performance of cellular -V2V communication. In the context of 5G technology, this paper establishes a cellular-V2V heterogeneous system model including 5G base station, CU, VU, Eve and PB by using random geometry theory. We introduce the automatic driving floating vehicle as PB, and use the transmitted signal as an artificial noise. The legitimate user knows that the information content will not be interfered by decoding. The eavesdropper receives the unknown signal and becomes artificial noise and is disturbed. We obtained the cumulative distribution functions of the SINR of CU, VU, and Eve through simulations, thereby proving that this cellular-V2V system model has certain rationality. We also conduct theoretical research and simulation experiments on safety indicators such as V2V communication connection probability, Eve eavesdropping interruption probability and V2V communication security transmission probability; and comprehensively considered communication connection probability and eavesdropping interruption probability to conduct simulation experiments and experiments on secure transmission probability. The result accords with the situation in the actual communication system. Since the probability of safe transmission is a multivariate nonlinear expression, we mine the data by genetic algorithm, obtain the optimal solution of the safe transmission probability, and extract valuable information to provide a decision-making scheme for the research of communication safety of autonomous driving; Finally, the simulation analysis shows that the information transmission safety probability of the automatic driving communication process in the PB-introduced system is higher. This proves the rationality of the cellular-V2V heterogeneous system model and simulation experiment including the self-driving floating vehicle, and provides research ideas and methods for further improving the safety of autonomous driving communication and preventing security problems such as information leakage and data tampering. The research in this paper has not considered the interference between different VU. In the actual Internet of Vehicles, V2V communication exists between multiple vehicles, and mutual interference cannot be ignored. The next research work will focus on solving such problems.

REFERENCES

[1] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proc. INFOCOM 19th Annu. Joint Conf. IEEE Comput. Commun. Societies*, Mar. 2000, pp. 1273–1282.

[2] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, S. Li, and G. Feng, "Device-to-device communications in cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 49–55, Apr. 2014.

[3] P. Gandotra and R. K. Jha, "Device-to-Device communication in cellular networks: A survey," *J. Netw. Comput. Appl.*, vol. 71, pp. 99–117, Aug. 2016.

[4] V. Korjik, V. Yakovlev, and I. Babkov, "The wire-tap channel concept against eavesdropping of indoor radio telephone," in *Proc. 8th Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 1997, pp. 477–479.

[5] A. Kachouh, H. Chour, Y. Nasser, and H. Artail, "Ergodic capacity analysis and transmission power optimization in D2D underlaying cellular communication," *Phys. Commun.*, vol. 34, pp. 144–156, Jun. 2019.

[6] J. Lei, H. Chen, and F. Zhao, "Stochastic geometry analysis of downlink spectral and energy efficiency in ultradense heterogeneous cellular networks," *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Apr. 2018.

[7] S. Mukherjee, "Downlink SINR distribution in a heterogeneous cellular wireless network with biased cell association," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6780–6786.

[8] F. H. Panahi and T. Ohtsuki, "Stochastic geometry modeling and analysis of cognitive heterogeneous cellular networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 141, Dec. 2015.

[9] P. Madhusudhanan, J. G. Restrepo, Y. Liu, and T. X. Brown, "Analysis of Downlink Connectivity Models in a Heterogeneous Cellular Network via Stochastic Geometry," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3895–3907, Jun. 2016.
[10] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1–13, Jan. 2015.
[11] J.-M. Liang, P.-Y. Chang, J.-J. Chen, C.-F. Huang, and Y.-C. Tseng, "Energy-efficient DRX scheduling for D2D communication in 5G network," *J. Netw. Comput. Appl.*, vol. 116, pp. 53–64, Aug. 2018.
[12] R. O. Adeogun, "A novel game theoretic method for efficient downlink resource allocation in dual band 5G heterogeneous network," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 119–141, Jul. 2018.
[13] L. Ziyang, *Research on Cognitive-Based Cellular and D2D Hybrid Networks*. Beijing, China: Beijing Univ. Posts and Telecommunications, 2013.
[14] X. Weijia, *Research on Physical Layer Security Technology of Dense Heterogeneous Cellular Networks Under Non-Ideal Conditions*. Zhengzhou, China: Strategic Support Force Information Engineering Univ., 2018.
[15] W. M. Han, Y. Huang, and L. Mei, "Research on virtual cellular manufacturing scheduling based on the scale-free random network model," *Appl. Mech. Mater.*, vol. 532, pp. 241–248, Feb. 2014.
[16] C. Jie, *Application of Random Geometry Theory in Cellular Networks*. Nanjing, China: Nanjing Univ. Posts and Telecommunications, 2016.
[17] Z. Wei, *Performance Analysis of Heterogeneous Networks Based on Random Geometry*. Beijing, China: Beijing Univ. Posts and Telecommunications, 2017.
[18] X. Fangfang, *Research on Physical Layer Security Transmission Technology in D2D Communication System*. Xi'an, China: Xidian Univ., 2018.
[19] Z. Aiqing, *Research on Key Technologies of Data Security Transmission in D2D Communication*. Nanjing, China: Nanjing Univ. Posts and Telecommunications, 2016.
[20] S. Sixue, *Research on D2D Communication Security Transmission Technology Based on Physical Layer Secure Communication Theory*. Beijing, China: Beijing Jiaotong Univ., 2018.
[21] Z. Mangang, J. Xiangdong, and Z. Meng, "Research on energy efficiency of hybrid network based on massive MIMO and D2D technology," *Signal Process.*, vol. 2017, vol. 33, no. 01, pp. 53–61.
[22] S. Dhilipkumar, C. Arunachalaperumal, and K. Thanigaivelu, "A comparative study of resource allocation schemes for D2D networks underlay cellular networks," *Wireless Pers. Commun.*, vol. 106, no. 3, pp. 1075–1087, Jun. 2019.
[23] L. Pengyu, *Vehicle-To-Vehicle Broadband Wireless Channel Modeling in Intelligent Transportation System*. Beijing, China: Beijing Jiaotong Univ., 2014.
[24] L. Shengnan, *Research on Resource Allocation Scheme in V2V Communication*. Beijing, China: Beijing University of Posts and Telecommunications, 2018.
[25] S. Yu, "V2V secure communication based on LTE D2D discovery process," *Commun. World*, vol. 22, pp. 30–31, Nov. 2017.
[26] S. Fangming, *Research on Security of Unmanned Communication Protocol Based on VANET*. Nanjing, China: Nanjing Univ. Posts and Telecommunications, 2017.
[27] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2319–2324.
[28] P. Madhusudhanan, J. G. Restrepo, Y. Liu, and T. X. Brown, "Downlink coverage analysis in a heterogeneous cellular network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 4170–4175.
[29] S. H. Rhee and X. Lei, "Hidden terminal aware clustering for large-scale D2D networks," *Wireless Pers. Commun.*, vol. 107, no. 3, pp. 1367–1381, Aug. 2019.
[30] R. Ghallab, A. A. Sakr, M. Shokair, and A. A. El-Azm, "Electronic relay performance in the inband device-to-device (D2D) communication system," *Telecommun. Syst.*, vol. 72, no. 1, pp. 29–39, Sep. 2019.
[31] P. JiaZheng, S. YiXin, Z. DanHong, Q. Yue, and L. ZhiWen, "Velocity forecasts using a combined deep learning model in hybrid electric vehicles with V2V and V2I communication," *Sci. China Technol. Sci.*, vol. 63, pp. 55–64, Mar. 2019.
[32] M. Shi, Y. Zhang, D. Yao, and C. Lu, "Application-oriented performance comparison of 802.11p and LTE-V in a V2V Communication System," *Tsinghua Sci. Technol.*, vol. 24, no. 2, pp. 123–133, 2019.
[33] B. Zardosht, S. S. Beauchemin, and M. A. Bauer, "A predictive accident-duration based decision-making module for rerouting in environments with V2 V communication," *J. Traffic Transp. Eng. (English Ed.)*, vol. 4, no. 6, pp. 535–544, Dec. 2017.
[34] X. Shen, Y. Liao, X. Dai, M. Zhao, K. Liu, and D. Wang, "Joint channel estimation and decoding design for 5G-enabled V2V channel," *China Commun.*, vol. 15, no. 7, pp. 39–46, Jul. 2018.
[35] K. Kanchanasut, S. Boonsiripant, A. Tunpan, H. K. Kim, and M. Ekpanyapong, "Internet of cars through commodity V2 V and V2X mobile routers: Applications for developing countries," *KSCE J. Civil Eng.*, vol. 19, no. 6, pp. 1897–1904, Sep. 2015.
[36] M. R. Jabbarpour, A. Marefat, A. Jalooli, R. M. Noor, R. H. Khokhar, and J. Lloret, "Performance analysis of V2 V dynamic anchor position-based routing protocols," *Wireless Netw.*, vol. 21, no. 3, pp. 911–929, Apr. 2015.
[37] C. Huang, B. Zhai, A. Tang, and X. Wang, "Virtual mesh networking for achieving multi-hop D2D communications in 5G networks," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101936.
[38] O. Hayat, R. Ngah, and Y. Zahedi, "In-band device to device (D2D) communication and device discovery: A survey," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 451–472, Feb. 2019.
[39] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.
[40] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

CHAO WANG was born in Changchun, Jilin, China, in 1974. He received the master's and Ph.D. degrees from Jilin University. He is working with the School of Transportation, Shandong University of Science and Technology. His research interests are mainly in modern urban transportation system planning, emergency rescue, the Internet of Things, data mining, and traffic safety technologies. He has won the first prize of the Municipal Science and Technology Progress Award, the Outstanding Instructor of scientific and technological innovation, and the first prize of the Postdoctoral Academic Forum of Control Science and Engineering.

RUNZE SONG was born in Qingdao, Shandong, China, in 1997. He received the bachelor's degree from the Shandong University of Technology, China. He is currently with the College of Transportation, Shandong University of Science and Technology. His research interests include intelligent vehicle and 5G networks.

ZHAOHUI LIU was born in Changchun, Jilin, China, in 1972. She received the master's and Ph.D. degrees from Jilin University. She was with the National Key Laboratory of Automotive Simulation and Control, China, and the University of Toronto, Canada, in the field of intelligent coordination and safety control of human-vehicle-environment systems. She is currently working with the College of Transportation, Shandong University of Science and Technology. She is the Leader of the Institute of Traffic Behavior and Traffic Safety. She has published more than 50 academic articles, published three academic works, and has more than 20 patents. Her research interests are mainly in traffic safety technology, the Internet of Things, the environmental perception, positioning, and driving control technology for unmanned vehicles.