energies

MDPI

Article

A Self-Learning Detection Method of Sybil Attack Based on LSTM for Electric Vehicles

Yi-Ying Zhang [1,2], Jing Shang [1,*], Xi Chen [3] and Kun Liang [1]

1 College of Artificial Intelligence, Tianjin University of Science & Technology, Tianjin 300457, China; yiyingzhang@tust.edu.cn (Y.-Y.Z.); liangkun@tust.edu.cn (K.L.)
2 Global Energy Interconnection Research Institute, Beijing 102209, China
3 GEIRI North America; 250 W Tasman Dr., Ste 100, San Jose, CA 95134, USA; xc@ieee.org
* Correspondence: shangjing@mail.tust.edu.cn; Tel.: +86-166-0030-0915

Received: 6 February 2020; Accepted: 12 March 2020; Published: 16 March 2020

Abstract: Electric vehicles (EVs) are the development direction of new energy vehicles in the future. As an important part of the Internet of things (IOT) communication network, the charging pile is also facing severe challenges in information security. At present, most detection methods need a lot of prophetic data and too much human intervention, so they cannot do anything about unknown attacks. In this paper, a self-learning-based attack detection method is proposed, which makes training and prediction a closed-loop system according to a large number of false information packets broadcast to the communication network. Using long short-term memory (LSTM) neural network training to obtain the characteristics of traffic data changes in the time dimension, the unknown malicious behavior characteristics are self-extracted and self-learning, improving the detection efficiency and quality. In this paper, we take the Sybil attack in the car network as an example. The simulation results show that the proposed method can detect the Sybil early attack quickly and accurately.

Keywords: EV; Sybil attack; intrusion detection; self-learning

1. Introduction

With the increasingly serious environment and energy problems, the application and popularization of new energy electric vehicles (EVs) has become a hot topic of global researchers. EV charging pile is one of the energy Internet entrances, carrying the important mission of charging power supply, charging measurement and billing, vehicle charging safety, and charging data interconnection. With the large-scale application of information technology in the charging service network, malicious users intrude into the charging pile of EVs to steal electricity for charging, which has an obvious hidden danger of information security. It is very important to ensure the interconnection between the piles and the safety of direct current (DC) charging. With the rapid development of EVs, the frequency of malicious attacks, the loss caused by them, and the difficulty of defense are greatly increased. Intrusion detection in the environment of super-fast charging piles is facing severe challenges.

In recent years, deep learning has been widely used in the field of network security [1]. Because the method of deep learning can extract better features from data to create a better detection model, and find the correlation between high-dimensional features, it can obtain a higher detection accuracy than the traditional method of machine learning. Traditional intrusion detection system (IDS) framework design tends to divide them into two systems: One for training and the other for prediction [2–6]. The whole process is not very effective because it requires a lot of prophetic data and too much human intervention. On the one hand, the vehicle data in the existing database is not suitable for the real scene, and the model trained with these data is not practical. On the other hand, this kind of model can only be used to detect the known attacks, and cannot do anything to the unknown attacks [7]. Therefore,

it is of great significance to study how to use a deep learning algorithm to identify malicious network attacks. However, it is difficult to use the intrusion detection mechanism that has been applied in the wired network under the environment of wireless and mobile properties and dynamic topology characteristics of an EV network.

This paper proposes an intrusion attack detection method based on self-learning. This method uses an integrated learning framework, based on the intrusion of false information packets about the traffic, and uses the LSTM neural network to obtain the characteristics of the change in the time dimension of the traffic data based on the traditional IDS. The transmission of contextual information forms a closed-loop system for training and prediction. At the same time, it is stored in the knowledge base according to a certain structure and continuously updated to identify diverse attacks and achieve intelligent detection.

2. Related Research Status

Traditionally, according to different data analysis methods, current intrusion detection methods can be divided into two categories: Abnormal intrusion detection and misuse intrusion detection [8–14].

Misuse intrusion detection refers to the collection of known intrusion behavior characteristics and the establishment of a related feature database. During the detection process, the existence of intrusion behaviors is determined by comparing the consistency of related data. The advantage of this method is that the false alarm rate is low, and known attack behaviors can be found, but the detection result depends on the completeness of the signature database, and the signature database must be updated in time. This method has a good detection rate for known attacks but cannot detect new or uncommon intrusions.

Anomaly intrusion detection refers to establishing the normal mode profile of the system in advance. If the real-time detected system deviates from the normal system model and exceeds a certain threshold, an intrusion alarm is issued. The distributed group identity authentication mechanism proposed in [15] uses the association between nodes and uses a key mechanism to authenticate the node's identity. This method detects locally without the intervention of a base station, which is more accurate than traditional detection schemes. However, due to the frequent changes of the car-connected network, the Sybil node detection is costly. Wu and others use the hidden Markov model to infer the Sybil node, find the real identity hidden under the camouflage node, and detect the Sybil node, but the detection cost is large [16]. Ji et al. [17] used the customer network management (CNM) algorithm to divide the target into separate trust groups. By calculating the global trust of the trust group, the trust value of each node in the group is measured, so that vehicles with lower trust values are considered malicious vehicles. The disadvantage of the mechanism is that it cannot prevent vehicles with higher trust values from carrying out sudden attacks [18–20]. Based on the digital signature issued by the roadside facility, Ge [21] proposed a Sybil node detection mechanism based on the driving route of the vehicle and the public key certificate. Some studies have proposed methods to determine Sybil nodes using vehicle motion trajectories [22,23]. The road side unit (RSU) digital signature is obtained during the driving process of the vehicle to determine the vehicle trajectory [24–29]. The advantage of this method is that it does not depend on attack characteristics and finds intrusion behavior based on the detection target, but how to define the normal mode contour of the system is a difficult problem.

To solve the above problems, this article analyzes the advantages and disadvantages of existing misuse intrusion detection and anomalous intrusion detection based on the learning intrusion detection methods of Sybil attacks in the car-connected network, and designs a self-learning intrusion detection method of Sybil attacks in order to eliminate the interference of prior knowledge, the received signal strength indication (RSSI), and the received information of the vehicle are used to detect the Sybil node, and at the same time, it establishes its own database and continuously updates it to achieve the effect of misuse detection. Compared with other detection methods, the proposed method not only can increase the detection rate but can comprehensively detect known and unknown attacks.

3. Sybil Attack

3.1. Sybil Attack Features

A Sybil attack refers to a malicious vehicle that illegally uses multiple identities. By forging multiple false identities and sending multiple pieces of false information through different identities, it disrupts and deceives other nodes in the network to launch direct attacks or prepare for other attacks. In the vehicle-linked communication network, vehicle nodes usually discover new nodes by periodically broadcasting beacon information, as shown in Figure 1 below. Assume that when vehicle P receives a request from vehicle S, the vehicle S has a lower trust value for vehicle P. Therefore, the vehicle P broadcasts multiple false messages (P_1,X_1,Y_1), (P_2,X_2,Y_2), (P_3,X_3,Y_3) to the vehicle S by forging multiple fake vehicles P_1, P_2, P_3, but these messages are all sent by the vehicle P to obtain the trust of the vehicle S, thereby S causes false congestion. Given the invisible nature of wireless communications, it is easy for a malicious vehicle to declare multiple identities without being detected.

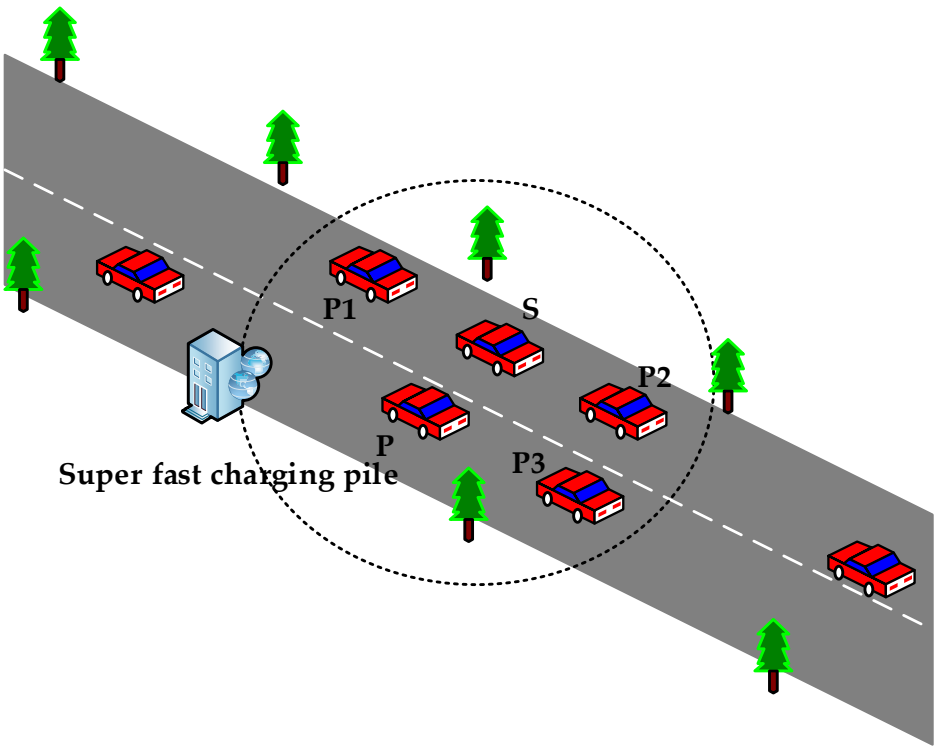

Figure 1. Sybil attack node graph.

There are many types of Sybil attacks: Direct communication, indirect communication, identity falsification, identity theft, simultaneous attacks, and non-simultaneous attacks [30–32]. Malicious vehicles use a few nodes in the car network to control multiple false identities, so as to use these false identities to control or affect a large number of normal nodes in the network.

3.2. Sybil Attack Discovery

Sybil node discovery is the process of detecting false data packets sent by malicious vehicles, and then identifying and isolating the nodes. This article is mainly divided into three steps: Packet detection, Sybil node identification, and node isolation [33–36].

3.2.1. Packet inspection

In the vehicular ad hoc network (VANET) architecture, each vehicle will be equipped with multiple sensing devices, such as the global positioning system (GPS), radar, etc., to obtain the vehicle speed,

position, and direction information. Through the cooperative awareness message (CAM), the vehicle continuously broadcasts its position to the surrounding vehicles in the process of driving, and stores its own vehicle information package and other traffic-related information packages sent by other vehicles in its own knowledge base and keeps updating. In this paper, malicious vehicles can forge multiple identities to send CAM packets through various illegal means to attack. The format of CAM is shown in Figure 2 below.

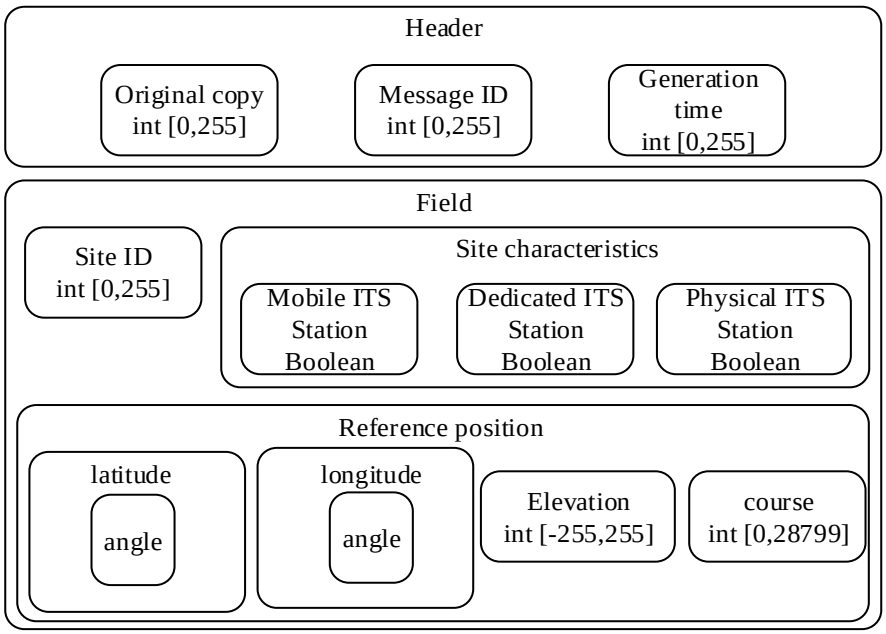

Figure 2. Cooperative awareness message (CAM) data format.

As shown in the figure above, the header of the CAM data stores the time and number of the data generation, and the basic fields store the ID, movement, and location information of the vehicle. The vehicle ID is the identification number of each vehicle. Vehicles regularly send CAM data packets to vehicles in the communication range by providing basic sensing services in a collaborative intelligent transportation system (ITS) network. According to the broadcasted CAM data packet, vehicle-related information can be extracted, and the vector of the vehicle at a certain time is defined as (ID,t,X_{pose},Y_{pose},Dir,v,a), where ID represents the ID of the vehicle; t represents the time stamp of the node; X_{pose}, Y_{pose}, represents the location of the node; Dir represents the node driving direction; v indicates the speed of the node; and a indicates the acceleration of the vehicle.

Therefore, in the time of $t \in (0, n)$, the driving information of a vehicle can be expressed as:

$$X = \begin{bmatrix} ID_1 & t_1 & X_{pose1} & Y_{pose1} & Dir_1 & v_1 & a_1 \\ ID_1 & t_2 & X_{pose2} & Y_{pose2} & Dir_2 & v_2 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ID_1 & t_n & X_{posen} & Y_{posen} & Dir_n & v_n & a_n \end{bmatrix}. \quad (1)$$

3.2.2. Identification of Sybil Nodes

In the vehicle-connected network architecture, each node can obtain two kinds of information, one is the CAM data from the neighbor node, and the other is the physical measurement value carried by the neighbor node. If the neighbor node is a malicious Sybil node, the position information in the CAM data and its own physical measurement result are very different, and the CAM nodes of different virtual vehicles all originate from the same physical node. Based on the above differences, this article

conducts the discovery of Sybil nodes. Using the wireless communication equipment equipped on the car, the received RSSI can be obtained, that is, RSSI is used as a physical measurement value in the process of determining the Sybil node.

RSSI indicates the signal strength of other vehicles received in the car-connected network. The unit is dBm, and its value decreases as the distance d increases. Assuming the distance between vehicles in vehicle communication is d, the calculated relationship between RSSI and d is:

$$d = 10^{\frac{|RSSI|-A}{10n}}. \tag{2}$$

Among them, the RSSI is a negative value, A represents the signal strength when the transmitting end and the receiving end are 1 m apart, n represents the environmental attenuation factor, and the determination of A and n depends on the environment in which the vehicle is located. The study found that the applicable attenuation models of the car-connected network are:

$$PL(d) = \begin{cases} PL(d_0) + 10n_1 \log_{10}\left(\frac{d}{d_0}\right), d_0 \le d \le d_b \\ PL(d_0) + 10n_1 \log_{10}\left(\frac{d_b}{d_0}\right) 10n_2 \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma, d > d_b \end{cases}, \tag{3}$$

where d_b is the critical distance, and the optimal value is 104 m. The parameters of some variables in the observer line of sight (OLOS) and the line of sight (LOS)are shown in the Table 1.

Table 1. Wireless network attenuation model parameters.

Scenes		n_1	n_2	$PL(d_0)$	X_σ
LOS	Highway	−1.66	−2.88	−66.1	3.95
	Urban area	−1.81	−2.85	−63.9	4.15
OLOS	Highway	−1.66	−3.18	−76.1	6.12
	Urban area	−1.93	−2.74	−72.3	6.67

In order to forge multiple identities to broadcast false information, a malicious vehicle needs to consider that the vehicle is a malicious vehicle if the calculated d does not match the location information in the CAM data packet sent by the neighboring vehicle.

3.2.3. Sybil Nodes Isolated

In order to speed up and isolate the detection of malicious vehicles and improve the detection efficiency of IDS, this paper designed a punishment model to reduce Sybil attacks, which can prevent malicious nodes from continuing to attack other nodes during IDS detection, that is, to record the vehicle's attacks through penalty factors, and make the attacking vehicle have no impact on the vehicle for a period of time. The penalty model for resisting Sybil attacks can be summarized as:

$$R(n) = \begin{cases} I(n) \\ f(x)D(n) \end{cases}, \tag{4}$$

where $I(n)$ refers to the excitation function when the data packet sent by the target vehicle is trusted n, and $D(n)$ is the penalty function of the trust value when the vehicle n attacks, $f(x) > 1$. If the vehicle sends out false data packets, the trust value of the target vehicle will drop rapidly. The greater the number of attacks, the larger the penalty factor, and the faster the target function will be put into the blacklist. The flowchart of Sybil node discovery based on the punishment incentive is shown in Figure 3.

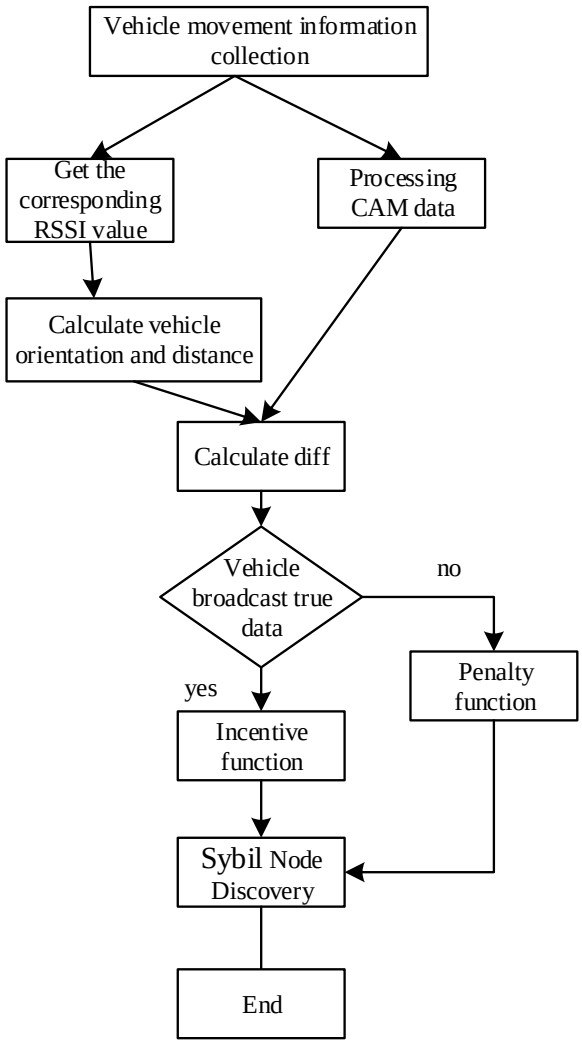

Figure 3. Flow chart of Sybil node discovery based on the punishment incentive.

In the internet of vehicles, the historical data of vehicle nodes is statistically significant to the discovery of Sybil nodes. In order to forge a false identity, some malicious nodes in the internet of vehicles propagate malicious data packets. When their historical behavior is malicious, their next behavior is malicious with high probability. Therefore, according to the penalty function, the trust value is a subjective prediction of a node's future behavior based on historical data. Therefore, this paper uses the penalty function to judge the probability of node behavior, increase the weight of malicious behavior, and make the trust value quickly converge below the threshold value.

4. Sybil Attack Intrusion Detection Model

In the vehicle-connected network architecture, there are two communication modes for vehicles: Vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure, such as charging pile (V2I) communication, as shown in Figure 4 below. Each vehicle is connected in the vehicle-connected network architecture. Both the fast charging pile and the fast charging pile are regarded as a mobile node. Within a certain communication range (generally a radius of 300 m), the dedicated short range communication (DSRC) transmits its own CAM data packet while inquiring other vehicles about the CAM data packet to obtain a series of road conditions and roads. Traffic information and its road map is shown in Figure 5 below, which improves driving safety, reduces congestion, and improves traffic efficiency.

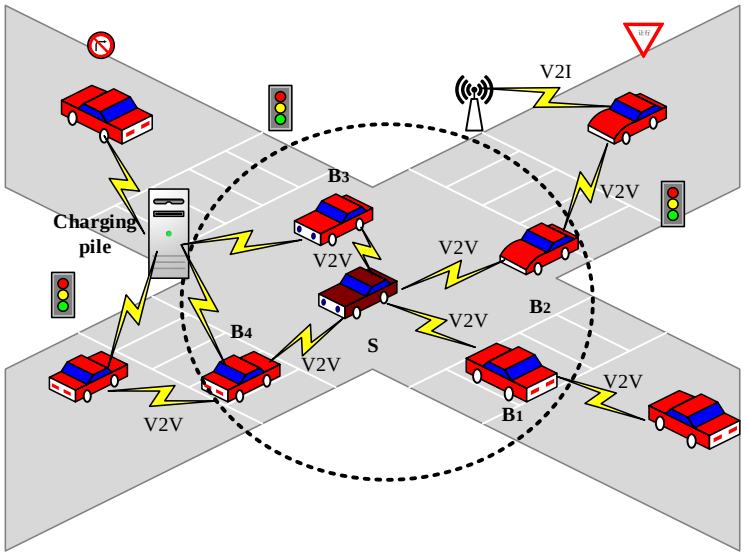

Figure 4. Architecture model of vehicle linkage network.

Figure 5. Live diagram of vehicle linkage network.

4.1. Construct a Self-Learning Sybil Attack Detection Model

Sybil attack detection based on the LSTM neural network algorithm for self-learning technology is the vehicle through the car networking of *ID*, node's timestamp t, vehicle location X_{pose}, Y_{pose}, vehicle driving direction *Dir*, the vehicle's speed v, and vehicle acceleration a and information is obtained, such as the RSSI signal abstraction into the LSTM neural network input layer and output layer neurons. By collecting a large number of CAM data packets, all relevant information in the database is automatically searched; the *ID* of the vehicle is extracted, including key information such as the trust value; a large training data set for neural network training is formed; and finally, this reflects the design requirements and the complex relationship between the results of the neural network can be designed for the use of the intelligent detection system on their own.

LSTM is proposed on the basis of the recurrent neural network (RNN), but when RNN optimizes the back-propagation algorithm, there is a serious problem of gradient disappearance or gradient explosion. Unlike the hidden layer of the RNN, which has only one state, the LSTM adds a state to the hidden layer to store long-term time data, which solves the shortcomings of the gradient of the RNN and can learn long-term dependent information. Therefore, LSTM is more suitable for processing vehicle data in VANET, and is widely used for time series vehicle data anomaly detection and learning.

The basic unit logical architecture of the LSTM is shown in Figure 6 below. At time t, vehicle data x_t is input to the LSTM, and then the state value c_{t-1} and the output value h_{t-1} at time $t-1$ participate in the calculation at time t. Finally, the calculated value at time t is obtained.

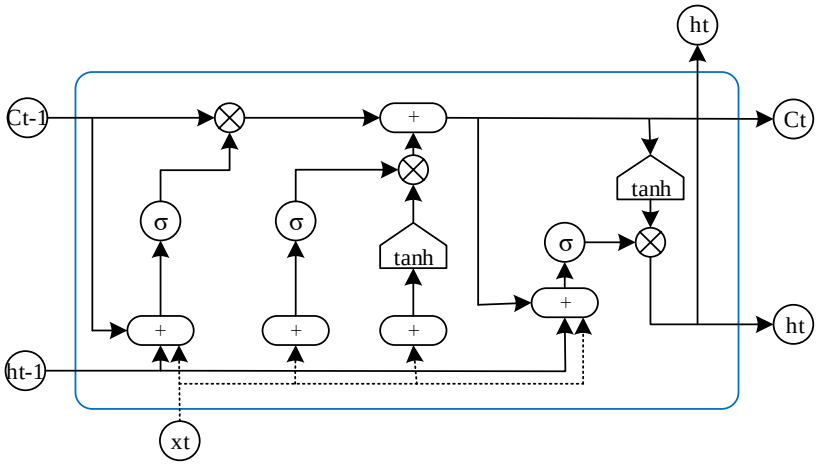

Figure 6. Long short-term memory (LSTM) basic unit logic architecture.

First, the LSTM unit processes the information of the previous memory state through a forget gate to determine the information to be forget from the memory state. The forget gate inputs sum and outputs a value between 0 and 1:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right). \tag{5}$$

Among them, W_f is the weight matrix of forget gate, $[h_{t-1}, x_t]$ means connecting two vectors into a longer vector, b_f is the bias term of forget gate, and σ is the sigmoid function.

Next, decide what information is stored in memory. This consists of two parts. On the one hand, the sigmoid activation function is used to determine which information to update, and the output is i_t. On the other hand, the *tanh* activation function is used to update the candidate vector, and the output is $\widetilde{C}_t$.

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \tag{6}$$

$$\widetilde{C}_t = tanh(W_c \cdot [h_{t-1}, x_t] + b_c), \tag{7}$$

where W_i, W_c are the weight matrix of the input gate, b_i, b_c are the bias terms of the input gate, the *tanh* function is the activation function, and the formula is expressed as:

$$tanhx = \frac{sinhx}{coshx} = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{8}$$

Finally, which hidden state information to output is decided. First, the output gate is used to determine what to output, then the activation function is used to process the memory state, and finally the output gate is used to control the memory state that needs to be output:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \tag{9}$$

$$h_t = o_t \times tanh(C_t), \tag{10}$$

where W_o is the weight matrix of output gate, b_o is the bias term of output gate, h (t) is the hidden state of the output. The cell state C_t consists of two parts, the first part is the product of C_{t-1} and the forgetting gate output f_t, and the second part is the product of i_t and $\widetilde{C}_t$ of the input gate, that is:

$$C_t = C_{t-1} * f_t + i_t * \widetilde{C}_t \tag{11}$$

The logic structure of the basic unit in LSTM is shown in Figure 6. After the vehicle receives the beacon message, it first standardizes the data, unifies the data to facilitate the calculation of gradients, and accelerates convergence. Before testing, training is performed with a small part of the classic data set. When the accuracy reaches 95% or more, the test is started. Each batch of training data needs to be randomly selected to achieve a different combination of training data in each batch.

4.2. Sybil Attack Detection Process Based on Self-Learning

We can assume that the vehicle nodes are in N states, and in each state, the vehicle can operate normally or maliciously. It is assumed that the current vehicle receives CAM data packets from a specific vehicle multiple time; the corresponding RSSI value set is:

$$\text{RSSI} = [rssi_1, rssi_2, \cdots rssi_n]. \tag{12}$$

The location information of the vehicle in the CAM data packet is:

$$U = [u_1, u_2, \cdots u_n]. \tag{13}$$

The difference between the physical measurement RSSI and CAM data packets can be expressed as:

$$diff = f(\text{RSSI}, U). \tag{14}$$

The intrusion detection system is an active security protection system. It analyzes vehicle data, vehicle flow data, and other characteristics to determine whether the vehicle is normal or contains potential danger. Intrusion detection systems can generally be divided into three modules: A data acquisition module, an intrusion detection module, and a response processing module. This article mainly analyzes the value of $diff$ to determine whether the vehicle is a malicious vehicle. The processing flow of its intrusion detection method is shown in Figure 7.

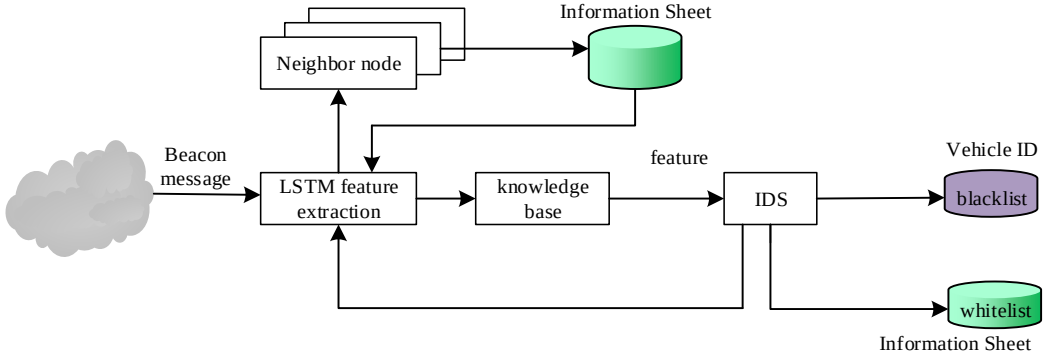

Figure 7. Self-learning-based intrusion detection model.

As shown in Figure 7 above, once a beacon message broadcast by a vehicle in a VANET from a neighbor vehicle, the LSTM module is used to form a feature vector to filter the beacon message broadcast by the neighbor vehicle. If the feature vector has historical data in its knowledge base, it will directly call the black and white list of vehicles to make a judgment. If the extracted feature vector is not in the historical data, IDS needs to be used to determine whether there is an attack on the beacon

message. The detection of the Sybil node in Figure 3 is the core of the IDS, which tries to detect the occurrence of a Sybil attack. If the IDS judges that there is no deviation in the message, it will accept the vehicle to add the vehicle *ID* to the white list. If an attack is detected, the vehicle will be regarded as an attack vehicle, and the feature vector and related data will be updated into the knowledge base.

In order to train the self-learning IDS proposed in this paper, first of all, the training process should be carried out without malicious vehicles, so that the system can detect the biased VANET messages according to the normal model. The vehicle's measured distance and physical distance are comprehensively considered. Through the feature extraction of the LSTM neural network and the continuous updating of the knowledge base, a white list (the *ID* of the vehicle with a higher trust value is stored) and a black list (the *ID* of the vehicle with a lower trust value is stored) is created. Using the vehicle blacklist and whitelist, the detection system can quickly evaluate credible vehicles, and continuously update the knowledge base based on the scores of the detection system and the learning of the LSTM neural network itself.

Since the trust value of each vehicle changes dynamically, but the recently entered trust value is more credible than the historically entered trust value, it is necessary to introduce a weight parameter, a time forgetting factor μ, when updating the trust value; the update formula is:

$$R = \mu \times R_{new} + (1 - \mu) \times R_{old}, \tag{15}$$

where R_{new} is the trust value recently entered by a certain vehicle. R_{old} is the trust value entered in the vehicle history., and $\mu > 0.5$.

5. Simulation Experiment of the Intrusion Detection Mechanism Based on Self-Learning

5.1. Experimental Environment and Evaluation Criteria

In this simulation experiment, we analyzed and evaluated the performance of the self-learning intrusion detection mechanism. Before the experiment started, it was run in an attack-free environment, and data was collected in the absence of an attack in order to distinguish it from later Sybil attacks. Then, an intrusion detection experiment was performed on a 1-km highway. At the same time, charging piles were installed on the highway. In our simulation, the attack flow and normal flow occurred randomly. The normal flow and the attack flow lasted for 2 min each time, and the number of vehicles changed. The experiment was carried out through the Urban Traffic Simulation Tool (SUMO) and Network Simulator version 2 (NS2). Among them, SUMO is currently the most-used road simulation package. It can simulate urban road networks. It is an object-oriented, time-discrete network simulation tool. The interface can also present many perfect low-level protocols. NS2 is a kind of object-oriented network simulator. We used it to simulate the vehicle network easily. The experimental simulation parameters are shown in Table 2.

Table 2. Experimental parameters.

Parameter	Parameter Value
Vehicle speed	10–30 m/s
MAC protocol	802.11 p
Sending frequency	1 Hz
Communication range	200 m
Simulation time	1000 s

5.2. Data Preprocessing

The vehicle will inevitably be affected by other electromagnetic waves during driving, which makes the collected vehicle data abnormal, such as RSSI, wavelength, transmission rate, etc. By calculating the range of the attribute data in the vehicle data (range = maximum − minimum), it

was found that some of the data were extremely different, so the attribute data of the vehicle was standardized to avoid the huge impact of abnormal data on the distance calculation.

The normalized formula is as follows:

$$y_i = \frac{x_i - \overline{x}}{s}, \overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2}. \quad (16)$$

Among them, x_i represents raw data that has not been processed, y_i represents the data after normalization, and n represents the number of data.

6. Experimental Results and Analysis

In order to verify the effectiveness of the model designed in this paper, two evaluation criteria, the detection rate and false detection rate, were used. The detection rate is the ratio of the number of malicious vehicle nodes successfully detected to the number of malicious vehicle nodes in the network. The proportion of normal vehicle nodes that are misdetected are referred to as malicious vehicle nodes. At the same time, in order to improve the accuracy of the mechanism, the experiment performed multiple simulations to find the average value.

6.1. Analysis of Simulation Experiment Results

Figure 8 shows the changes in the trust values of the two normal and malicious nodes selected. With the detection of the vehicle during the simulation time, the trust value of the normal vehicle is continuously rising. At 1000 s, the trust value is about 0.96. Assuming the threshold is 0.5, the vehicle is a trusted vehicle. At 1000 s, the trust value of a vehicle is about 0.1, which is far below the credibility threshold. The vehicle is a malicious vehicle. It can be seen that the detection model can detect malicious vehicles with a trust value below a threshold.

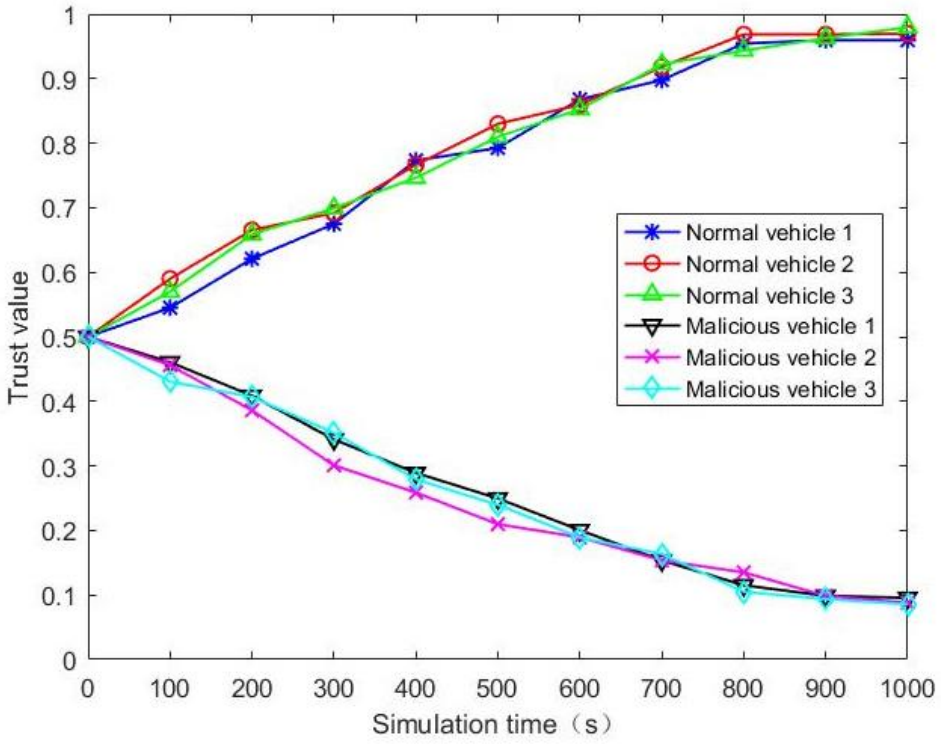

Figure 8. Vehicle simulation experiment trust value results.

6.2. Performance Analysis

As shown in Figure 9, if the electric vehicle charging pile is also regarded as a vehicle node, as the number of vehicle nodes increases, the detection rate of Sybil attacks also increases, and the false detection rate will continue to decrease. This is because when the number of vehicle nodes is small and the learning attack feature time is short, the nodes are sparsely distributed and the Sybil attack detection is not accurate. With the increase of the learning time, the detection rate of Sybil attacks eventually remained at about 95%, and the false detection rate remained at about 5%.

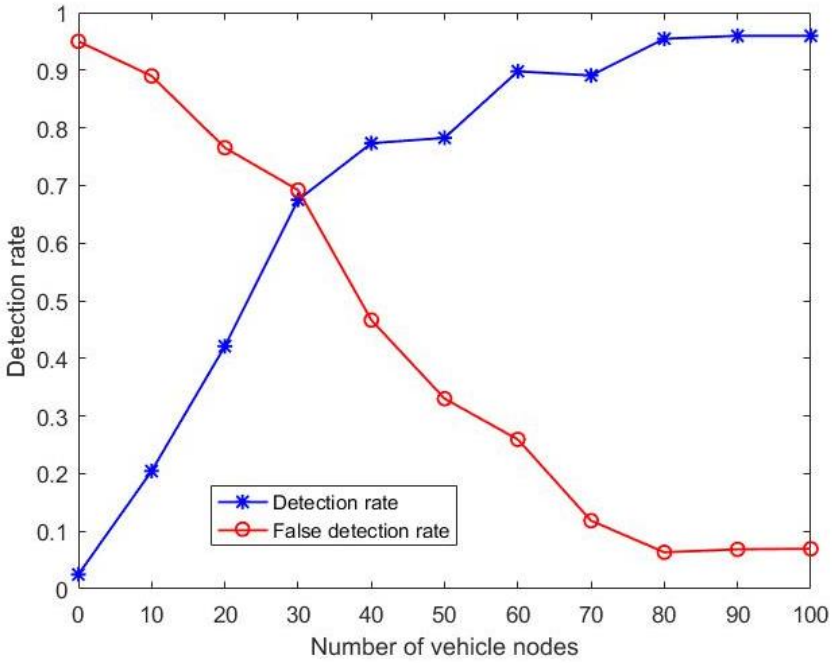

Figure 9. Simulation results of system detection rate and false detection rate.

In order to further prove the effectiveness of the self-learning scheme in this paper, by setting the same normal flow and attack flow attack flow, the self-learning scheme method in this paper was compared with the method that does not use the self-learning scheme in [16]. As can be seen from Figure 10, in the case of using the self-learning scheme in this paper and the case without the self-learning scheme, the detection rate of both models decreases when the number of malicious nodes increases, but when the detection time is greater than 300 s, the detection rate using the experimental scheme is significantly higher than the detection rate without using the experimental scheme and the detection rate is steadily tending to 96%, while the detection rate without using the self-learning scheme is relatively stable under a short time. However, when the time reaches after 120 s, the detection rate is not stable. It can be seen that the self-learning scheme used in this paper has obvious efficiency and applicability compared with the non-self-learning scheme.

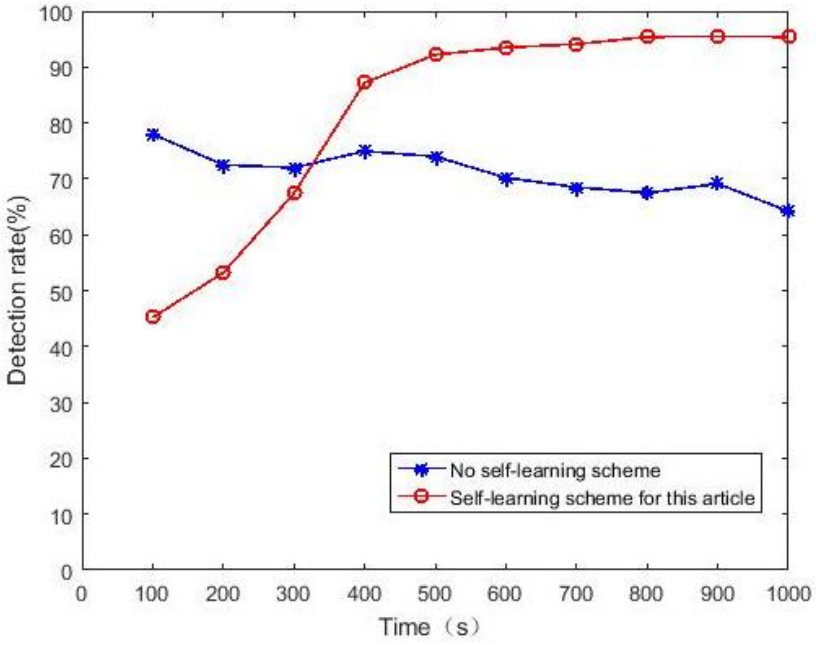

Figure 10. Comparison of different experimental protocols and detection rates.

7. Conclusions

After investigating at the problem of information security between EVs and charging piles, the self-learning-based intrusion detection mechanism constructed in this paper can prevent various Sybil attacks. Compared with the existing methods, the proposed solution effectively ensures the integrity of the message and protects the privacy of the EV. By establishing a reputation threshold and a trust threshold for each node broadcast message, malicious nodes are effectively identified. At the same time, the scheme establishes a self-learning Sybil attack detection structure, and adapts to the high-dimensional highly dynamic topology of the vehicle network with lightweight ideas. This scheme has a high detection rate and a low false detection rate for malicious nodes whether they come from forged or legal identities.

In the simulation experiments, the performance of the self-learning detection model in this paper was evaluated from the results of simulating trust values and the detection rate of malicious nodes. The experimental results show that this self-learning detection model can quickly detect a variety of malicious nodes, and the detection rate of malicious nodes is also high. Compared with the existing detection models, the detection model proposed in this paper is suitable for the vehicle-to-vehicle communication environment. The self-learning model accelerates the detection speed of malicious nodes compared with the traditional model. At the same time, it can detect not only the known attack types in the database but also the unknown attack types. In summary, this solution can be applied to the on-board system of electric vehicles, ensuring the information security requirements of the communication system between EVs and charging piles, and laying the foundation for the development of new energy vehicles.

Author Contributions: All authors contributed to the writing and revisions; Resources, Y.-Y.Z.; Performed research and wrote the paper, J.S.; Refined the ideas and interpreted the results, X.C.; Validation, K.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Project of State Grid Corporation of China, grant number 5418-201958524A-0-0-00.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rata, M.; Rata, G.; Filote, C.; Raboaca, M.S.; Graur, A.; Afanasov, C.; Felseghi, A.-R. The ElectricalVehicle Simulator for Charging Station in Mode 3 of IEC 61851-1 Standard. *Energies* **2020**, *13*, 176. [CrossRef]
2. Chou, Y.; Chang, X.M.; Chou, Q.; Peng, C.; Su, S.T. Anomaly detection method of stream data based on LSTM and sliding window. *Comput. Appl.* **2019**. [CrossRef]
3. Hussain, A.; Bui, V.-H.; Baek, J.-W.; Kim, H.-M. Stationary Energy Storage System for Fast EV Charging Stations: Optimality Analysis and Results Validation. *Energies* **2020**, *13*, 230. [CrossRef]
4. Kim, D.-J.; Ryu, K.-S.; Ko, H.-S.; Kim, B. Optimal Operation Strategy of ESS for EV Charging Infrastructure for Voltage Stabilization in a Secondary Feeder of a Distribution System. *Energies* **2020**, *13*, 179. [CrossRef]
5. Gao, X.; Ma, Y.X.; Tang, X.B.; Lu, X.R. Research on Self-learning and Automatic Design of Optical Fiber Loop in Smart Substation Based on Matlab Neural Network Algorithm. *Power Syst. Prot. Control* **2019**, *22*, 159–167.
6. Chen, Y.H.; Zhou, D.; Zheng, W.B. Data transmission device of charging pile based on WiFi. *Meas. Test. Technol.* **2019**, *11*, 1–3.
7. Javed, M.A.; Zeadally, S.; Hamid, Z. Trust-based security adaptation mechanism for Vehicular Sensor Networks. *Comput. Netw.* **2018**, *137*, 27–36. [CrossRef]
8. Xia, F.; Li, C.Y.; Chen, D.X.; Tang, J. A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 305–314.
9. Lim, K.; Manivannan, D. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Veh. Commun.* **2016**, *4*, 30–37. [CrossRef]
10. Zhang, Y.Z.; Ye, X.Q. Sybil detection based on periodic ultra-wideband distance information in WSN. *Telecommun. Sci. Mag.* **2016**, *8*, 110–117.
11. Hu, R.H.; Dong, X.M.; Wang, D.L. Research on Node Replication Attack and Sybil Attack Defense Mechanism in Wireless Sensor Networks, Computer Aided Verification. *J. Electr.* **2015**, *8*, 743–752.
12. Trifa, Z.; Khemakhem, M. Sybil Nodes as a Mitigation Strategy against Sybil Attack. *Procedia Comput. Sci.* **2014**, *32*, 1135–1140. [CrossRef]
13. Grover, J.; Laxmi, V.; Gaur, M.S. Sybil attack detection in VANET using neighbouring vehicles. *Int. J. Secur. Netw.* **2014**, *9*, 222–233. [CrossRef]
14. Olariu, S.; Kha-Lil, I.; Abuelela, M. Taking VANET to the clouds. *Int. J. Pervasive Comput. Commun.* **2011**, *7*, 7–21. [CrossRef]
15. Huang, L. Design and implementation of sensor network based on distributed group identity authentication. *Comput. Eng.* **2007**, *10*, 161–163.
16. Wu, D.P.; Si, S.S.; Yan, J.J.; Wang, R.Y. Detection mechanism of social network Sybil nodes based on behavior characteristic analysis. *J. Electr. Inf. Technol.* **2017**, *9*, 2089–2096.
17. Ji, W. Research on Several Key Issues of Reputation Mechanism in Peer-to-Peer Environment. Master's Thesis, University of Science and Technology of China, Hefei, China, 11 March 2009.
18. Zhang, H.; Zhang, J.B.; Zhang, T. Research on an Incentive Model Against Sybil Attack. *Comput. Technol. Dev.* **2012**, *12*, 164–186.
19. Shareh, M.B.; Navidi, H.; Javadi, H.H.S.; HosseinZadeh, M. Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model. *Inf. Sci.* **2019**, *470*, 94–108. [CrossRef]
20. Ma, H.; Liang, Y.; Ji, S.; Li, D. A trust/distrust-based reputation attack defense strategy and stability analysis. *Comput. Res. Dev.* **2018**, *12*, 2685–2702.
21. Ge, J.Y. Sybil node detection based on routes and certificates in VANET. *Commun. Technol.* **2012**, *11*, 40–43.
22. Fang, H.; Guo, G.; Zhang, J. Multi-faceted trust and distrust prediction for recommender systems. *Support Syst.* **2015**, *71*, 37–47. [CrossRef]
23. Gai, K.; Choo, K.K.R.; Qiu, M.; Zhu, L. Privacy-Preserving Content-Oriented Wireless Communication in Internet-of-Things. *IEEE Internet Things J.* **2018**, *5*, 3059–3067. [CrossRef]
24. Chen, Y.; Ye, Q.; Li, M.Z. Research on Identity-based Encryption Algorithms in Wireless Sensor Networks. *Comput. Appl. Softw.* **2015**, *12*, 302–309.
25. Tan, L.; Lian, Y.F.; Chen, K. Method for identifying malicious users in social networks based on composite classification model. *Comput. Appl. Softw.* **2015**, *12*, 1–17.
26. Wang, X.; Liu, L.; Su, J.S. RLM: A general model for trust representation and aggregation. *IEEE Trans. Serv. Comput.* **2010**, *5*, 131–143. [CrossRef]

27. Rodrigues, R.; Druschel, P. Peer-to-peer systems. *Commun. ACM* **2010**, *53*, 72–82. [CrossRef]
28. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
29. Wu, D.P.; Zhang, P.N. Node service ability aware packet forwarding mechanism in intermittently connected wireless networks. *IEEE Wirel. Commun.* **2016**, *15*, 8169–8181. [CrossRef]
30. Yu, X.; Liu, L.; Wu, Y. Optimal routing among WSN clusters based on ring search. *Telecommun. Sci.* **2015**, *2*, 109–118.
31. De Fuentes, J.M.; González-Manzano, L.; González-Tablas, A.I.; Blasco, J. Jorge Security Models in Vehicular Ad-hoc Networks: A Survey. *IETE Tech. Rev.* **2014**, *31*, 47–64. [CrossRef]
32. Riccardo, P. S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia. *Comput. Netw.* **2016**, *94*, 205–218.
33. Chu, G.F.; Chen, Q.; Zhang, L. Analysis and comparison of P2P network simulator. *Comput. Technol. Dev.* **2011**, *11*, 66–69.
34. Chen, H.Q.; Wang, H.; Wang, H.K. Node localization method for detecting Sybil attack in wireless sensor network. *Telecommun. Eng.* **2011**, *9*, 87–91.
35. Cao, X.; Kou, W.; Du, X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Inf. Sci.* **2010**, *180*, 2895–2903. [CrossRef]
36. Ren, X.L.; Jiang, C. Sybil attack detection scheme based on hierarchical grid. *Comput. Eng.* **2010**, *11*, 159–163.