Hindawi
Scientific Programming
Volume 2023, Article ID 9896847, 1 page
https://doi.org/10.1155/2023/9896847

Retraction

Retracted: Security and Privacy Protection of Car Networking Consistent Algorithm Based on Smart Multi-Sensor

Scientific Programming

Received 1 August 2023; Accepted 1 August 2023; Published 2 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Niu, "Security and Privacy Protection of Car Networking Consistent Algorithm Based on Smart Multi-Sensor," *Scientific Programming*, vol. 2022, Article ID 1160021, 9 pages, 2022.

Hindawi
Scientific Programming
Volume 2022, Article ID 1160021, 9 pages
https://doi.org/10.1155/2022/1160021

Research Article

Security and Privacy Protection of Car Networking Consistent Algorithm Based on Smart Multi-Sensor

Zuoling Niu

School of Zhongxing Communication, Xi'an Traffic Engineering Institute, Xi'an 710300, Shaanxi, China

Correspondence should be addressed to Zuoling Niu; niuzuoling@xjy.edu.cn

Received 16 June 2022; Revised 27 July 2022; Accepted 9 August 2022; Published 31 August 2022

Academic Editor: M. A. Rashid Sarkar

With the rapid development of the Internet and wireless communications, smart multi-sensor networks are gradually being used in various fields, and the Internet of vehicles technology combined with smart multi-sensor network came into being. However, although the Internet of vehicles technology has greatly facilitated people's travel in traffic, its problems in security and privacy protection have also been amplified and became a major threat to the Internet of vehicles technology. Consistency algorithms are an important solution to the trust problem and are a prominent representative of distributed algorithms. In order to solve the problem of security and privacy protection of smart multi-sensors in car networking technology, in this paper, consistent algorithm and group signature verification technology are used to study the security and privacy protection performance of the Internet of vehicles in a connected random network composed of 300 nodes through artificially synthesized simulation data. Using the method in this paper, collect and analyze the experimental data of the number of messages, verification delay, traffic load, and message loss rate of randomly generated vehicles within 200 seconds and evaluate the performance of privacy protection in the maximum consistent algorithm; the results show that the verification delay will increase with the increase of the number of messages, and the more traffic load, the higher the message loss and verification delay, and the maximum consistent algorithm has good privacy protection performance. In terms of data, the RSU-based auxiliary scheme consumes 25.59% of the communication of the KPI-based signature scheme and 25.64% of the swarm scheme.

1. Introduction

1.1. Background Meaning. In the era of Internet informatization, advances in wireless communication technology, mobile cloud computing, automobiles, and smart terminal technologies are driving the evolution of vehicle self-organizing networks to the Internet of vehicles paradigm [1]. In recent years, the Internet of vehicles has become one of the most active research fields in the network and intelligent transportation system. As an open fusion network, the Internet of vehicles plays an important role in solving various driving and traffic problems through advanced information and communication technologies [2]. However, although the Internet of vehicles technology has improved the safety on the road and greatly facilitated people, it is more vulnerable to security and privacy threats due to the huge scale of the Internet of vehicles network, open wireless channels, and predictable movement trajectories. Intruders may steal drivers' private information through open wireless channels, and track drivers according to the car's moving trajectory, the Internet of vehicles technology is also prone to information leakage. Information security and privacy protection issues will become a major concern for connected car technology.

1.2. Related Work. With the development of wireless networks, smart multi-sensor networks are used in many fields, and the Internet of vehicles technology is one of them. Many scholars have conducted related research on the security and privacy protection issues in smart multi-sensor networks and Internet of vehicles technologies. Xu studied the relationship between the Internet of vehicles and big data in the vehicle environment, mainly studying how the Internet of vehicles supports the transmission, storage, and calculation of big data, and benefits from the performance of the Internet of vehicles [3, 4]. Chen proposed an innovative

paradigm called the Vehicle Cognitive Internet (CIoV). Unlike existing work that focuses on communication technology, CIoV improves transportation by mining effective information from physical and network data spaces. Security and network security [5]. Kang et al. studied the location privacy issues and defense measures in the cloud-enabled Internet of vehicles, first proposed two unexplored VM mapping attacks, and then designed a VM identifier replacement scheme and a pseudonym change synchronization scheme to protect location privacy [6]. Zongpu et al. proposed two novel methods to improve source location privacy security protection and node energy utilization in smart multi-sensor networks [7]. Memon introduces a novel query privacy algorithm for continuous query of location-based services, which is called the hidden algorithm of authentication speed dynamic transmission mode [8]. Memon and Arain proposed a novel dynamic route privacy protection scheme for continuous query services in road networks [9]. Zhang et al. proposed an authentication asymmetric group key agreement based on attribute encryption (ABE-AAGKA), which combines the advantages of attribute encryption and identity authentication, and uses attribute encryption and authentication technology to ensure the security and protection of the group key agreement personal privacy [10]. Muthusenthil and Murugavalli proposed the privacy protection of the cluster-based geographic routing protocol in MANET [11]. Zhao et al. proposed an effective VANET revocable group signature scheme based on the Chinese remainder theorem and Schnorr signature algorithm, which can achieve privacy protection by using blind certificates [12]. The above experts and scholars have analyzed the security and privacy protection issues in telematics technology from several perspectives, but they have not proposed a proven method.

1.3. Innovation of This Article. This paper uses group signature scheme, PKI signature scheme and RUS assisted three different verification methods to study the relationship between the number of messages, verification delay, message loss rate, and traffic load. The experiment uses a certificate signature format based on pairing technology. Before the vehicle communicates with other entities, it must pass signature and anonymous certificate verification to prove the accuracy of the message. The certificate and message can be verified by batch verification. The performance of privacy protection in the maximum consistent algorithm is studied. The algorithm can provide higher system reliability, scalability, and flexibility due to its distributed control architecture [13, 14], and when the global topology information is unknown, node privacy can be well protected.

2. Smart Multi-Sensor-Based Car Networking Consistent Algorithm Security and Privacy Protection Method

2.1. Smart Multi-Sensor Network. The concept of the Internet of Things has been in front of us. It means that every object in the Internet infrastructure is interconnected to a global dynamic expansion network. Sensors and smart objects are the main participants in the traditional computing devices of the Internet of Things. Sensors are a key part of the Internet of Things, so are the smart multi-sensor networks [15].

Intelligence and miniature are the future trends for sensors, in which case smart sensors have been created. Smart sensors are intelligent devices that integrate sensors, actuators, and electronic circuits. In other words, smart sensors are devices that integrate multiple sensing elements and microprocessors with monitoring and processing functions. The implementation of intelligent sensor systems was developed on the basis of sensor technology, computer technology, signal processing, network control, and other technologies that develops with these technologies, but is not a simple synthesis of these technologies. Neither the microprocessor nor the network technology is a simple synthesis of the original general technologies. With the combined support of many technologies, high accuracy, resolution and reliability have become the main hallmarks of intelligent sensors.

Smart multi-sensor Networks are self-organizing and consist of a large number of small, low-cost, low-power nodes that communicate via wireless or wired communication. This can detect, monitor and collect environmental information in real time in the target area, and send it to the end user after editing. With the development of wireless communication technology, smart multi-sensor networks have become one of the most powerful technologies that can be used in various applications, such as military surveillance, environmental surveillance, industrial control, and medical surveillance [16]. Due to the high density of nodes, human control factors and environmental factors generated by the robustness of the network introduce errors and redundancy in the information collected by the smart multi-sensor network, which consumes a lot of resources and energy in the process of network communication. Due to the limited power, bandwidth, storage capacity, and data processing capabilities of sensor nodes, reducing data redundancy, improving accuracy, reducing power consumption, and extending its life cycle is applicable to all smart multi-sensor networks. Smart multi-sensor network applications, especially those used in harsh environments (such as Earthquake relief), are susceptible to large-scale damage, usually causing multiple collocated sensors to fail simultaneously and dividing the network into disjoint partitions [17, 18].

Emerging technologies such as the Internet of Things, smart applications, smart grids, and machine-to-machine networks have stimulated the deployment of autonomous, self-configuring large-scale smart multi-sensor networks (WSN) [19], which are generally used for collection, processing, and transmission in the area The object information. Its characteristics are as follows: (1) distributed autonomy. WSN adopts distributed control, simple and flexible management and networking. Nodes can be automatically adjusted and placed to form a network without relying on fixed basic communication functions. (2) Large scale and strong durability. The smart multi-sensor network has tens of thousands of nodes, and the large detection area avoids blind

spots and reduces the influence of factors such as energy constraints and human environmental interference. (3) Scalability. WSN responds effectively to new hubs and can be quickly integrated into global work. (4) Dynamic topology. As a dynamic network, the network topology will change while the network is running, such as switching nodes, switching between operating mode and shutdown mode, and adding new nodes. (5) Application related. According to the physical information involved in the environmental change program, smart multi-sensor networks can be implemented on various hardware node platforms, systems, and network protocols. (6) Spatial location addressing. WSN does not consider the data source, only the space to which the data belongs, and spatial processing can be used. (7) Node capacity is limited. The sensor nodes are powered by small batteries and have limited power. (8) The communication range is restricted, and the communication capacity is restricted. The communication radius of a node is usually tens of meters, and its communication range is limited.

2.2. Internet of Vehicles. The Internet of vehicles, that is, the Vehicle Internet System (VANET) is derived from the Internet of Things and is an intelligent transportation network composed of on-board information modules, road units, and information management platforms. The Internet of vehicles is based on the Internet of Things, using radio frequency identification technology, wireless communication technology, etc., to build a powerful Internet system for the Internet of Things, providing an information exchange platform that can perform real-time interconnection of any object in the transmission system, and can perform any object automatic identification and mutual exchange of information. The vehicle Internet system uses RFID, sensors, GPS positioning systems, and pattern recognition technology to collect environmental information, such as vehicles and roads, and applies specific communication technologies to achieve information and interaction. The Internet of vehicles has successfully applied the Internet of Things technology to the transportation field by integrating computer technology with modern urban transportation networks.

The Internet of vehicles includes five types of vehicle communication: vehicle-to-vehicle, vehicle-to-road, vehicle-to-infrastructure, vehicle-to-personal equipment, and vehicle-to-sensor [20] in cellular networks. Vehicle-to-vehicle communication is a modern intelligent transportation system. An important part [21]. Most of the automotive network scenarios are new, very open, and sensitive to privacy, and their system security requirements are very different from traditional network security requirements. Different from the typical mobile self-organizing network, the automobile Internet is large in scale, complex in structure, unfamiliar with neighboring nodes, many potential intruders, and the information security situation is more severe. In order to deal with various security threats, the in-vehicle Internet must meet the following information security requirements: (1) authentication, which is the basic requirement to prevent external attacks, including two aspects that allow vehicle users to make communication decisions. The recipient can determine whether the message source is valid and whether the node has a legal ID. (2) Integrity, that is, the vehicle node can judge whether the received message has been tampered with. (3) Non-repudiation, the vehicle node shall not reject the message being sent or forwarded. If the intruder causes a serious car accident or property damage, he will be punished by law. This attribute is very important for monitoring the cause of road accidents and the basis for insurance claims. (4) Revocation, the authorized management department can revoke the authorization of the vehicle node, so there is no need to publish verifiable messages. This attribute is used to defend against internal intruders and allow the system to recover from internal attacks. (5) Functionality. While resisting internal and external attacks and implementing identity verification mechanisms, the vehicle Internet system ensures that the system delay is controlled within a certain range and can smooth vehicle nodes as needed. It is necessary to ensure the normal operation of the system and obtain resources.

2.3. Consistent Algorithm. The consistent algorithm is an important distributed algorithm. It defines the rules for nodes in the network to communicate with neighboring nodes and use their state to update their own state. The nodes in the network can achieve state convergence by executing a consistent algorithm. The amount of convergence refers to the initial state of all nodes in the network. Nodes can only use the information of neighboring nodes to perform general macro-behaviors. There are many types of existing consistent algorithms, which can be divided into average consistent algorithms and maximum consistent algorithms according to their algorithms and models. These types of algorithms can be applied to share information in order to coordinate multiple distributed generators in the micro-grid [22, 23].

Consider a network consisting of n nodes, the nodes are labeled 1, 2, ..., n. The communication topology of the secondary network is represented by an undirected graph $G = \{V, E\}$, where V represents a set of n nodes, $E \subset V * V$ represents a collection of communication links. Suppose $(i, j) \in E$ if and only if $(j, i) \in E$, that is, the communication between i and j is mutual. The adjacent set of node i is $N_i = \{j | (j, i) \in E, \forall j \in V\}$. Suppose node $i, i \in V$, the state at time t is $x_i(t)$, and the initial state is $x_i(0)$, let $X(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\}$ be the state vector composed of the states of all nodes at time t. When the discrete time is constant, the average consistent algorithm can be described by the following dynamic equation:

$$x_i(t+1) = x_i(t) + \sum_{j \in N_i} w_{ij}\left(x_j(t) - x_i(t)\right), \quad i \in V, \tag{1}$$

where, w_{ij} is the weight given to node j by node i, that is, node i updates its own state to the weight sum of neighbor state. The matrix form corresponding to formula (1) is

$$x(t+1) = W_X(t). \tag{2}$$

In order to achieve average consistency, the weight matrix W has the following properties: (1) W is a non-negative

double random matrix, that is, the elements of W are greater than or equal to 0, and the sum of the rows and columns of W is 1; (2) the characteristic value of W satisfies $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n > -1$, that is, W has one and only one eigenvalue equal to 1, and the modes of other eigenvalues are all less than 1; (3) the convergence speed of the consistent algorithm (2) depends on $\max\{|\lambda_2|, |\lambda_n|\}$.

In the average consistent algorithm, the state of node i will converge to the average of the initial states of all nodes. The formula is as follows:

$$\lim_{t \longrightarrow \infty} x_i(t) = \frac{1}{n} \sum_{j=1}^{n} x_j(0). \tag{3}$$

Maximum consistent algorithm is another commonly used algorithm model. The discrete-time maximum consistent algorithm can use dynamic equations:

$$x_i(t+1) = \max_{j \in N_i} x_j(t), \quad i \in V. \tag{4}$$

When all nodes form a connected network, formula (4) will make the state of any node i converge to the maximum value of the initial state of all nodes:

$$\lim_{t \longrightarrow \infty} x_i(t) = \max_{j \in V} x_j(0). \tag{5}$$

2.4. Group Signature. The group signature scheme is a brand-new digital signature design proposed in the 1990s. Since then, many scientists have revised it, paying more attention to its safety, effectiveness, and practicality. Group signing allows any group member to sign mail anonymously [24]. In the group signature format, each member of the group can anonymously sign the message sent without revealing their specific identity. For the recipient, the verification process does not affect a single signer, and the confirmation of the message can only prove that the message is from a certain group, but cannot identify the member who signed the specification. If there is a disagreement, you can obtain a signature from the group administrator to confirm the person's true identity.

The group signature scheme mainly includes three types of entity members. The first is the group administrator who is responsible for forming the group, joining the group members, and managing the group; then, the group members assist the specific signers to generate the group signature; and finally, the verification as the receiver to verify the validity of the signature. However, he can only prove where the signature came from, and cannot determine the true identity of the signer. The specific execution steps of the group signature scheme are as follows. (1) Initialization: the group manager establishes the group resource, generates the corresponding group public key (Group Public Key) and group private key (Group Private Key), and system parameters. Member joining: according to the current agreement, team administrators and users who want to join the team will issue digital team certificates and distribute private keys to team members. (3) Group signature: team members use the received digital team certificate to sign the document, create a group signature and use a personal key to encrypt the information through an encryption algorithm. (4) Verification: the recipient uses the digital signature verification algorithm to use the public group key to determine the legitimacy of the signature output from the algorithm in step (3), and to determine whether to verify the signature according to the algorithm output. (5) Identification of the signer: the group administrator uses the signature and private group key to monitor the group signature generated by the user in real time, and displays the actual signer's identity when needed [25].

After the group signature format was proposed, due to its short signature time, easy operation, strong practicability, and many other advantages, it quickly attracted wide attention from experts in various fields and conducted in-depth research. However, in the actual operation process, because the group administrator controls the password of "all team members of the group," when the group administrator is violated, the in-vehicle network system will be fatally hit. Also, if the number of malicious members is greater than a certain number, then, they can tamper with the signatures of group members at will.

2.5. Security and Privacy Protection. Although big data and the Internet of Things bring well-known benefits, they also face a wide range of attack surfaces, causing serious attention to the concepts of trust, security, and privacy [26]. There are too many technologies that define themselves as the Internet of Things, which complicates the development of a complete Internet of Things environment, and when security and privacy are considered, the situation becomes more difficult [27]. Due to the openness of wireless channels and high-speed vehicle mobility, there are many threats to vehicle safety and privacy on the Internet. Intruders can modify the content of information to avoid legal liabilities, transmit high-frequency signals to occupy bandwidth, create false information to satisfy their own interests, and monitor and analyze messages on wireless channels. As the scale of the vehicle Internet expands, the need for accident reports and the difficulty of controlling certain applications sensitive to delays will increase.

In the Internet of vehicles, user privacy and site privacy are interrelated and inseparable. When the Internet of vehicles communicates through wireless channels, it will inevitably face many threats and attacks, such as false or misleading traffic information, information leakage, or information duplication. For example, on the vehicle Internet, beacon information is periodically sent every 300 milliseconds, and the beacon contains data such as vehicle location, driving direction, driving speed, and acceleration. In order to ensure the authenticity of the message, all messages must be signed before they can be sent. These messages are sent along with their signature and digital certificate. Digital certificates contain user identity information, beacons contain vehicle location information, and signal information is sent regularly. Intruders can use advanced wireless tracking technology to monitor the driving process of the vehicle to analyze the daily life of the vehicle user. Personal

information such as lifestyle habits can be associated with the driver's identity information to reveal the user's identity. If the identity information of the vehicle user is leaked, the daily behavior of the vehicle user will be exposed, and the intruder can infer the user's activity process and monitor the vehicle based on the user's daily life habits. The vehicle location information can be tracked through the identity information, and the track of the vehicle is tracked through the vehicle location information, and then, the user identity information can be displayed. These threats and attacks may have dire consequences for the automobile network that transmits safety information related to life. Therefore, it is essential to protect the privacy of the vehicle's identity and the vehicle's Internet privacy in vehicle communication.

3. Consistency Algorithm-Based Implementation of Car Network Security and Privacy Protection

3.1. Test Subject. This paper analyzes vehicles generated randomly in 200 seconds in a connected random network composed of 300 nodes. The vehicle speed range is randomly generated at 50–110 km/h, the OBU communication distance is 330 meters, and the RSU signal coverage range is 1500 meters. Simulate a high-speed one-way lane with a length of 2200 meters.

3.2. Experimental Data. In the experiment, it is set that the number of messages received in each time period and the traffic load do not change with the change of the scheme. In 200 seconds, the number of messages received every 20 seconds and the vehicle load are shown in Table 1.

Within 200 seconds, the rate of messages lost every 20 seconds is shown in Table 2.

In the same time period, the verification delays of signature and certificate verification, certificate verification, and signature verification are shown in Table 3.

It can be roughly seen from the data in Table 3 that in the same time period, the time delay for simultaneous verification of the certificate and the signature is much longer than the time delay of the separate verification of the certificate and the signature alone, but the delay of the simultaneous verification is less than that of the two alone. The sum of the verified delays.

The signature time, verification time, communication consumption, and storage volume under the different mechanisms are shown in Table 4.

From the data in Table 4, we can roughly see that the storage requirements of the maximum consistency algorithm mechanism are significantly smaller than those of the BP algorithm. It can also be seen that the communication cost of the maximum consistency algorithm is small and the signature time requirement is significantly smaller than the other two mechanisms. This further indicates that the maximum consistency algorithm can effectively protect the identity privacy of the vehicle and the Internet privacy of the vehicle.

Table 1: Data table of the number of messages and vehicle load.

Time	Number of messages	Vehicle capacity
0	0	0
20	110	30
40	240	41
60	280	57
80	410	61
100	547	73
120	632	94
140	710	115
160	888	141
180	911	164
200	1000	197

Table 2: Message loss rate.

Time	Message loss rate		
	Group signature	PKI	RSU assistance
0	0	0	0
20	0.29	0.09	0.04
40	0.37	0.14	0.07
60	0.39	0.19	0.10
80	0.43	0.23	0.13
100	0.57	0.27	0.15
120	0.63	0.32	0.19
140	0.65	0.35	0.22
160	0.70	0.39	0.27
180	0.76	0.42	0.30
200	0.81	0.49	0.35

4. Discussion

4.1. The Relationship between the Number of Messages and the Verification Delay. According to the simulation experiment, we obtained the experimental data of the number of messages received and the verification delay in the same time period. According to the number of messages received and the verification delay time, we can draw the signature and certificate between the two. Figure 1 shows the relationship diagrams of simultaneous verification, signature verification, and certificate verification.

The relationship between the number of messages and the time delay shown in Figure 1. The signature verification time, the certificate verification time, and the time to verify both the signature and the certificate will increase as the number of messages increases. The delay of certificate verification is higher than the delay of signature verification, and the delay of verification is less than the sum of the delay of signature verification and certificate verification.

4.2. The Relationship between Information Loss Rate and Vehicle Load. From Tables 1 and 2, we can get the data of the vehicle-mounted quantity and the data of the information loss rate under the three schemes of group signature, PKI signature, and RUS assistance. By sorting and analyzing the data of the two, we can get the information. The relationship between the loss rate and the vehicle load is shown in Figure 2.

Table 3: Verification delay.

Time	Verification of both signatures and certificates	Certificate validation	Signature verification	Certificate + signature
0	0	0	0	0
20	199	161	120	281
40	336	241	154	395
60	504	379	200	579
80	768	554	279	833
100	913	648	314	962
120	1050	742	455	1197
140	1267	894	501	1395
160	1391	923	695	1518
180	1600	1091	761	1752
200	1810	1200	899	1999

Table 4: Comparison of different algorithmic mechanisms.

Mechanism	Signature time	Verification time	Communication cost	Storage capacity
Maximum consistency	6.12	4.01	120	129210
BP	7.21	4.32	321	208914
GS	7.68	4.05	331	132196

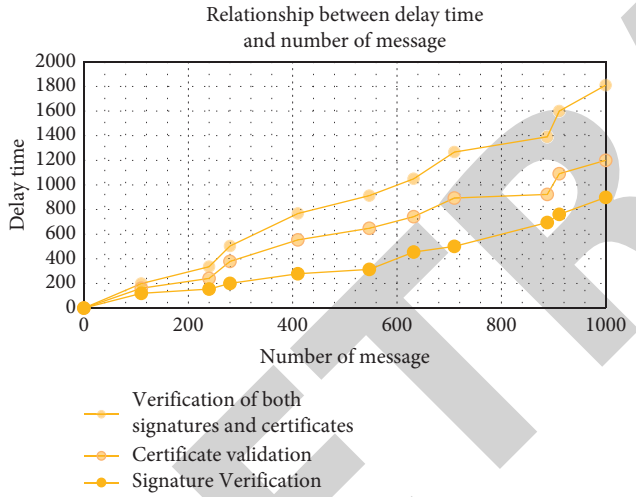

Figure 1: The relationship between the number of messages and the delay.

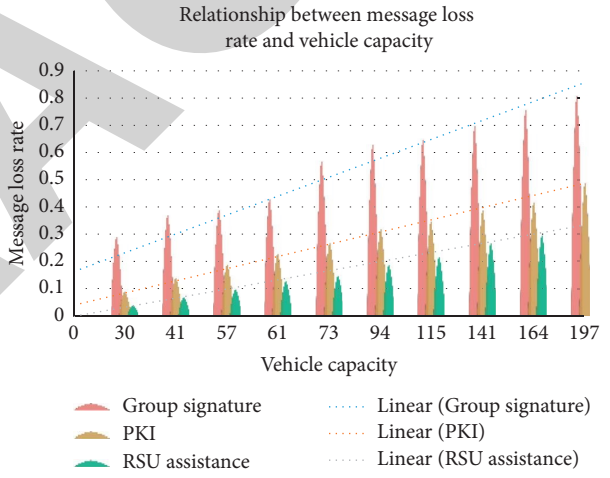

Figure 2: Relationship between information loss rate and vehicle load.

It can be known from the relationship graph between the information loss rate and the vehicle volume that the greater the vehicle volume in the Internet of vehicles among the three schemes, the higher the information loss rate. Among them, the information loss rate of group signature is higher than that of the other two schemes. The loss rate of PKI signature scheme is higher than that of RSU auxiliary scheme, and the information loss rate of RSU auxiliary scheme is the lowest.

4.3. The Relationship between Delay and Vehicle Load. Combining the data in Tables 1 and 3, the relationship between the vehicle load and the delay under the group signature, PKI signature, and RSU assistance scheme within 200 seconds and every 20 seconds was analyzed. According to the data in the table, draw the relationship between vehicle load and time delay as shown in Figure 3.

According to Figure 3, the relationship between the vehicle load and the time delay can be drawn. The larger the vehicle load, the longer the delay. The group signature scheme has the longest delay time, followed by the PKI signature, and finally the RSU auxiliary scheme has the shortest delay. Since the calculation speed of the RSU auxiliary scheme is very fast, the delay of this scheme is mainly determined by the RSU packet release interval. In order to shorten the message delay time, we can reduce the time interval for sending messages, but at the cost of increasing communication overhead, this will bring more conflicts to the wireless communication of the media access control layer.

Combining the data in Figure 3 and Table 4, the relationship between communication consumption and vehicle load was analyzed for different communication mechanisms

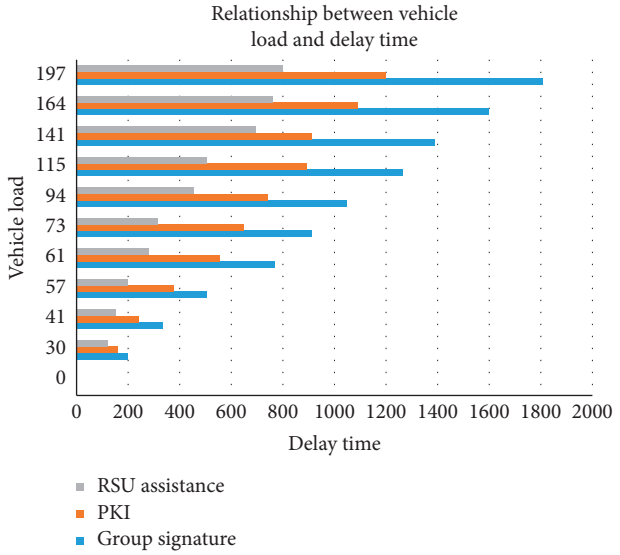

Figure 3: The relationship between vehicle load and delay.

over a period of 200 seconds. By integrating and aggregating the above relevant data, we obtain the relationship between communication consumption and vehicle load as shown in Figure 4.

The relationship between communication consumption per unit time and vehicle load can be seen in Figure 4. It is clear that the RSU scheme has much lower communication consumption than the PKI signature scheme and the group scheme within 10 ms. In particular, as the vehicle load increases, the group signature has the highest communication consumption, the RSU scheme has the second lowest, and finally the PKI signature scheme has the lowest. By looking further at Figure 4, we can see that the communication consumption of the RSU-based assisted scheme is 25.59% of the KPI-based signature scheme and 25.64% of the group scheme.

4.4. Privacy Protection Performance of Maximum Consistent Algorithm. In this network, the connection probability between any two nodes is 0.02. We will consider the performance of privacy protection under monotonic increase, monotonic decrease, Bernoulli distribution, and uniform distribution. Each node has the maximum value with the same probability. After multiple simulation experiments on the maximum consistent algorithm, the distribution of its convergence time is obtained. The theoretical value and the expected simulation time are shown in Table 5.

It can be seen from the data in the table that the simulation results are very close to the theoretical results. This experiment calculates the maximum expected probability of all nodes in the network when the global information is known and the global information is unknown. It can be concluded that the maximum expected probability of more than 90% of the nodes is 0–0.4. When the global information is known, 12% of all nodes fall in the range of 0–0.1, 51% fall in the range of 0.1–0.2, 17% fall in the range of 0.2–0.3, and 9% fall in the range of 0.3–0.4 node; nodes falling between

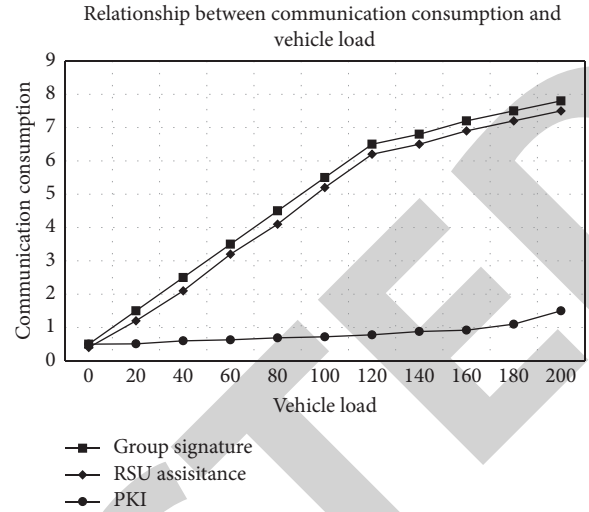

Figure 4: Communication consumption versus vehicle load.

Table 5: Convergence time.

Distribution of convergence time	Monotone increasing	Monotone decreasing	Bernoulli distribution	Uniform distribution
Theoretical results	16.9917	10.3358	13.5193	14.5374
Simulation results	16.9920	10.3416	13.5201	14.5523

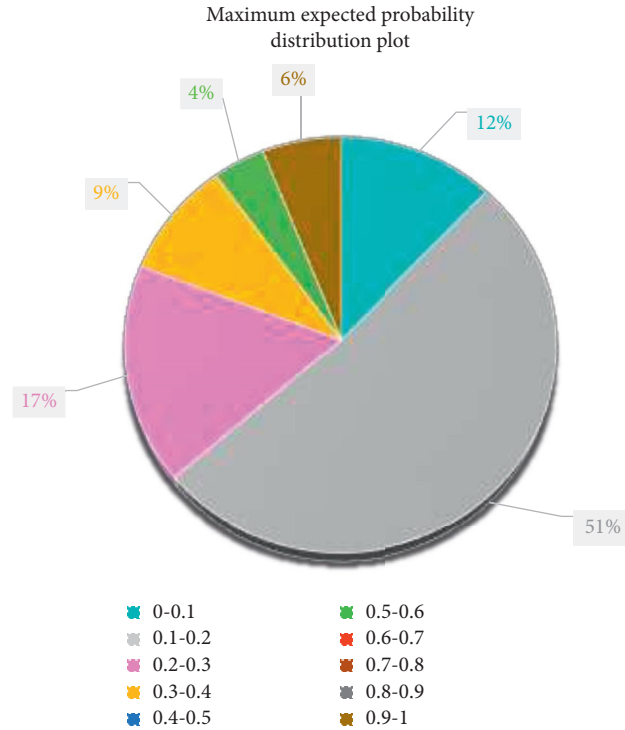

Figure 5: The maximum expected probability distribution with known global information.

0.4–0.5 and 0.6–0.9 account for 0%, nodes falling between 0.5-0.6 account for 4%, and nodes falling between 0.9-1 account for 6%. According to the data obtained in the experiment, the distribution of the maximum expected probability of the node can be obtained as shown in Figure 5.

When the global information is unknown, no matter which node has the largest initial state, the probability of it being recognized by neighboring nodes is less than 10%. Therefore, it can be concluded that the performance of privacy protection is better when the global information is unknown. The algorithm can converge in a finite time, and when the global topological information is unknown, the privacy of the node can be well protected; when the global topological information is known, the maximum node can be easily identified by neighboring nodes.

From the above analysis, we can see that based on intelligent multi-sensors and consistency algorithms, the article achieves car networking privacy protection and increases the security of car networking technology. Also, based on the algorithms and strategies proposed in the article, the communication consumption of car networking is significantly reduced, and the message loss and verification delay rates continue to decrease.

5. Conclusions

With the development of Internet technology, smart multi-sensor networks have played a pivotal role in daily life. They have been applied in various fields, and more and more new technologies have emerged. Among them, the Internet of vehicles technology, which is a combination of smart multi-sensor networks and traffic systems, has become a powerful guarantee for solving traffic problems. The application of the Internet of vehicles technology brings people a lot of convenience. The internalization of vehicles through wireless communication can use vehicles to perceive the surrounding road conditions and effectively avoid a series of traffic such as traffic jams and rear-end collisions. The Internet of vehicles technology can also be used as a transportation system cloud. While the Internet of vehicles technology is convenient for everyone, the security and privacy protection issues it brings are also getting more and more attention. Due to some deficiencies in the Internet of vehicles technology, vehicle information and user privacy are easily stolen and leaked by others, which gives people using Internet of vehicles a great sense of insecurity.

Through simulation experiments, this paper under the three schemes of group signature, KPI signature, and RSU assistance, the data such as the number of received information of the vehicle, the information loss rate, the verification delay, and the number of vehicles on the road were analyzed and the relationship between the factors were studied. In the results of the research on the privacy protection performance of the maximum consistent algorithm, the maximum expected probability of the network node being recognized by the neighboring node was obtained. It was analyzed when the global information was known and the global information was unknown. When unknown, the node's privacy protection performance was good.

However, there is still no standardized and unified privacy measurement mechanism for vehicle Internet security and privacy protection, which also has a significant impact on research. Although the current research mainly focuses on the protection of personal privacy of the automobile Internet from various angles, it does not consider privacy practices from an overall perspective. Future research needs to consider privacy protection from the perspective of system scope in order to effectively protect the privacy of the vehicle Internet. The current experimental data are all completed in an ideal virtual simulation environment, without considering the complexity of the real network environment, and lacking certain convincing power. Therefore, we need to improve and perfect these problems in the future.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] W. Jiafu, L. Jianqi, S. Zehui, and A. Vasilakos, "Mobile crowd sensing for traffic prediction in internet of vehicles," *Sensors*, vol. 16, no. 1, p. 88, 2016.

[2] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for Internet of Vehicles: a survey," *Journal of Communications and Information Networks*, vol. 2, no. 2, pp. 1–17, 2017.

[3] D. He, S. Chan, and M. Guizani, "An accountable, privacy-preserving, and efficient authentication framework for wireless access networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1605–1614, 2016.

[4] W. Xu, H. Zhou, N. Cheng et al., "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[5] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I Humar, "Cognitive internet of vehicles," *Computer Communications*, vol. 120, pp. 58–70, 2018.

[6] J. Kang, R. Yu, X. Huang et al., "Location privacy attacks and defenses in cloud-enabled internet of vehicles," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 52–59, 2016.

[7] J. Zongpu, W. Xiaojuan, G. Hairu, W. Peng, and C. Song, "A privacy protection strategy for source location in WSN based on angle and dynamical adjustment of node emission radius," *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 180–188, 2017.

[8] I. Memon, "Authentication user's privacy: an integrating location privacy protection algorithm for secure moving objects in location based services," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1585–1600, 2015.

[9] I. Memon and Q. A. Arain, "Erratum to: dynamic path privacy protection framework for continuous query service over road networks," *World Wide Web-internet & Web Information Systems*, vol. 20, no. 4, pp. 1–33, 2016.

[10] Q. Zhang, Y. Gan, L. Liu, X. Wang, X. Luo, and Y Li, "An authenticated asymmetric group key agreement based on

attribute encryption," *Journal of Network and Computer Applications*, vol. 123, pp. 1–10, 2018.

[11] B. Muthusenthil and S. Murugavalli, "Privacy preservation and protection for cluster based geographic routing protocol in MANET," *Wireless Networks*, vol. 23, no. 1, pp. 79–87, 2017.

[12] Z. Zhao, J. Chen, Y. Zhang, and L. Dang, "An efficient revocable group signature scheme in vehicular ad hoc networks," *Ksii Transactions on Internet & Information Systems*, vol. 9, no. 10, pp. 4250–4267, 2015.

[13] Y. Guan, L. Meng, C. Li, J. C. Vasquez, and JM. Guerrero, "A dynamic consensus algorithm to adjust virtual impedance loops for discharge rate balancing of AC microgrid energy storage units," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4847–4860, 2018.

[14] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, April 2016.

[15] S. Ghaly, M. O. Khan, and S. Ould, "Implementation of a broad range smart temperature measurement system using an auto-selecting multi- sensor core in LabVIEW," *Engineering, Technology & Applied Science Research*, vol. 9, no. 4, pp. 4511–4515, 2019.

[16] K. Nisar, "Smart home: multisensor information fusion towards better healthcare," *Advanced Science Letters*, vol. 24, no. 3, pp. 1896–1901, 2018.

[17] C. Michael and Multisensor-Cnc-Bildverarbeitungsmessgerat, "Bauteile prazise non-taktil sowie taktil vermessen," *Elektro-Automation: Elektrotechnik + Elektronik Inder Industrie*, vol. 71, no. 4, pp. 104–105, 2018.

[18] Z. Lv and L. Qiao, "Analysis of healthcare big data," *Future Generation Computer Systems*, vol. 109, pp. 103–110, 2020.

[19] Y. Zeng, D. Zhang, P. Qi, and L. Zheng, "Label-free simultaneous sensor for multi-components detection based on G-Quadruplex DNA structure," *Sensors and Actuators B: Chemical*, vol. 265, pp. 468–475, 2018.

[20] O. Kaiwartya, A. H. Abdullah, Y. Cao et al., "Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[21] L. Yang and H. Li, "Vehicle to vehicle communication based on a peer to peer network with graph theory and consensus algorithm," *IET Intelligent Transport Systems*, vol. 13, no. 2, pp. 280–285, 2019.

[22] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," *IEEE Transactions on Smart Grid*, vol. 7, 2016.

[23] M. Shuai, N. Yu, H. Wang, L. Xiong, and Y. Li, "A lightweight three-factor Anonymous authentication scheme with privacy protection for personalized healthcare applications," *Journal of Organizational and End User Computing*, vol. 33, no. 3, pp. 1–18, 2021.

[24] D. Choi and S. Guilley, "Information security applications," in *Proceedings of the International Workshop, WISA 2016*, Jeju Island, Korea, August, 2017.

[25] S. Sengan, O. I. Khalaf, P. Vidya Sagar, D. K. Sharma, L. Arokia Jesu Prabhu, and A. A. Hamad, "Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare*, vol. 11, no. 3, pp. 1–11, 2022.

[26] F. Li, H. Li, C. Wang, K. Ren, and E. Bertino, "Guest editorial special issue on security and privacy protection for big data and IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1446–1449, 2019.

[27] O. Sarychikhina, E. Glowacka, and B. Robles, "Multi-sensor DInSAR applied to the spatiotemporal evolution analysis of ground surface deformation in Cerro Prieto basin, Baja California, Mexico, for the 1993–2014 period," *Natural Hazards*, vol. 92, no. 1, pp. 225–255, 2018.