Joint timeliness and security provisioning for enhancement of dependability in Internet of Vehicle system

Tao Jing, Hengyu Yu, Xiaoxuan Wang and Qinghe Gao

Abstract
The Internet of Things has emerged as a wonder-solution to numerous problems in our everyday lives, such as smart homes and intelligent transportation. As an extension of the IoTs, the Internet of Vehicles (IoVs) also requires increasingly high security and timeliness. This article proposes a vehicle-assisted batch verification (VABV) system for IoV, in which some vehicles called auxiliary authentication terminal (AAT) are selected to assist the roadside unit for Basic Safety Message (BSM) verification. As a measure to enhance the timeliness performance for system dependability, comprehensive AAT selection strategies are designed. To overcome the security weaknesses of VABV system, a Sybil detection scheme based on Extreme Learning Machine is developed. For the evaluation of VABV system, the quantified Age of Information (AoI) is used as an integrated timeliness and security indicator. The proposed AoI indicator synthesizes the effects of BSM verification, re-verification for failure of some AATs, Sybil attack, and Sybil detection scheme. As illustrated by the simulation results, by employing AoI as a performance evaluation indicator, we can better and more intuitively design an AAT optimal selection strategy based on changes in AoI. Simultaneously, the performance of the proposed Sybil detection scheme can be evaluated more intuitively and effectively under different IoV scenarios based on AoI.

Keywords
IoV, dependability, timeliness, security, Sybil, Age of Information

Date received: 9 January 2022; accepted: 3 May 2022

Handling Editor: Peio Lopez Iturri

Introduction
The advance of IoT technology and the concept of smart cities facilitate the emergence of Internet of Vehicle (IoV). As the automobile industry and transportation network grow rapidly, vehicles provide us with increased conveniences. Nevertheless, our growing demand for a variety of vehicles leads to an increase in traffic accidents and congestion. As a burgeoning paradigm, IoV is the combination of Vehicular Ad Hoc Networks (VANETs) and IoT. Unlike VANETs, IoV utilizes a variety of technologies to enhance the network’s properties, including machine learning, cloud computing, and behavior detection.

In order to coordinate the traffic flow effectively, the vehicles on the roads need to exchange messages with
each other with on-board units (OBUs) mounted. The OBUs also enable vehicles to communicate with the roadside unit (RSU) nearby. In the IoV, messages can be approximately categorized into two types: safety-related messages and value-added messages with the Basic Safety Message (BSM) being the most significant one. Typically known as heartbeat messages, the BSMs are proposed as the primary message set used by connected vehicle safety applications to constantly exchange data within the IoV network. Using real-time exchange of BSMs, safety applications are capable of detecting and identifying any potential hazards before they occur and can then alert drivers or begin vehicle control systems to respond to the situation. In addition, the BSM becomes obsolete as soon as it is used and is disposed of. It is essential to note that BSMs contain much vital information such as the real-time velocity, location, and acceleration of the vehicle and are transmitted via the wireless channel in an open environment, therefore prone to several security threats. This will jeopardize the benefits of such a message-exchange based system and may cause more chaos in traffic. Consequently, in addition to verifying the entities (i.e. vehicles or RSUs) that enter the IoV, the messages (i.e. BSM) must also be verified by the potential receivers in order to prevent attacks by impersonation, tampering, and so on.

In light of the above consideration, numerous researchers propose a variety of security schemes for entities and messages in IoV. The schemes for entities guarantee that entities in the IoV are legitimate, while schemes for messages ensure the integrity of messages with batch verification method adopted to improve the efficiency of verification. Specifically for message verification scheme, some ordinary vehicles are selected to help the RSU with message verification to alleviate the computational pressure of RSUs. Throughout their previous works, they propose improved security mechanisms and either illustrate that their proposed mechanisms are low in overhead or improve the efficiency of verification. Specifically for BSM, they propose the use of batch verification to reduce the computational overhead. However, they do not discuss the security of the underlying communication channel, which is a critical aspect of security in IoV.

In the IoV, the ultimate goal is to provide a high-quality service to the users who are in it. In other words, vehicle users are not concerned with network latency, throughput, and packet loss of the current IoV system, which are the focus of much of current research. What they care is whether the information they need to receive will arrive on time and be of high quality. In fact, in the current research on urban transportation systems, the question of whether a system can actually provide a satisfactory service to its users is increasingly being raised by researchers. Based on the concept of satisfying user needs, and in order to evaluate the performance of each subsystem of IoVs more comprehensively, various models are proposed to define “Everything as a service (XaaS).” Using this model, an evaluation system that evaluates many systems can bring together a comprehensive concept of the service content of each subsystem, including discussions of products, processes, data & information management, and security as a service. Specifically, an IoV metric is anticipated that can be used to assess its performance in all aspects, particularly its timeliness and security to ensure that the system is able to meet the maximum possible user demand for the service.

In recent years, some works introduce the concept of dependability to IoT. The original concept of dependability can be briefly described as the capability of a system to provide users with trusted, reasonable, reliable, and correct services, or, in other words, the ability to ensure continuous and uninterrupted provision of critical services. In Junior and Kamienski, it is attributed by the authors that the two terms Dependability and Trustworthiness refer to the same concept that explains that the trustworthiness of IoT systems is largely determined by their ability to adapt and respond to what vulnerability flaws are present during their operational cycles. Based on a brief review of the current state of research, it can be concluded that the term Dependability is often restricted to the study of security performance in dealing with malicious network attacks under IoV scenarios. It should also be noted that some studies on improving IoV trustworthiness confuse this concept with trust, by studying the trust value management of vehicles and only examining the reputation of each node in the IoV. In these works, reputation, through the acquisition, updating, and sharing of trust value, enables vehicles to evaluate each other’s behavior and determine whether the other vehicle is malicious or has decreased reputation value as a result of malicious behaviors, and therefore cannot be trusted by other vehicles.

In our view, there are few description and studies of the real sense of dependability of IoV for urban transportation, and there is an absence of study of multiple quality requirements for data and information of IoV for vehicle users, not to mention the definition and quantification methods for dependability of the system as a whole. Similarly, we introduce the concept of dependability in our study of IoV networks. And in order to evaluate the IoV system from the perspective of dependability, it is therefore important for the proposed IoV system to satisfy the user’s demand for quality of service, since it is an important medium for the
BSM interaction between users of vehicles, when it comes to ensuring that the data quality of the BSM after transmission is up to user's expectations. From the perspective of the users, we then propose the concept of MIaaS (Message Interaction as a Service), based on the XaaS model, for evaluating dependable IoV systems, that is, evaluating whether the IoV system can provide the service to meet the users' demands in terms of BSM interaction among vehicle users. Beyond that, inspired by Wang et al.,\textsuperscript{28} using the Age of Information, the IoV system is analyzed quantitatively, allowing the system dependability to be uniformly described from the perspective of vehicle users.

The biggest difference of our work with existing related work is that we perform a true dependability analysis of IoV and analyze its properties from the perspective of vehicle users. We pay more attention to the quality of BSM that vehicle users will receive instead of merely considering the possible threats that IoV may face. The proposed IoV system is evaluated with an unified indicator named Age of Information (AoI), which identifies the freshness of BSMs clearly.

**Contributions**

In this article, our contributions are fourfold.

- We analyze the shortcomings of the existing IoV research, and the concept of dependability is creatively introduced to unify the evaluation of IoV performance. A vehicle-assisted batch verification (VABV) system based on BSM interaction is proposed, and its dependability is discussed in terms of its system framework and the security basis for message signatures.
- In order to reduce the VABV system verification latency, we proposed a more comprehensive selection strategy for choosing vehicles that will serve as auxiliary authentication terminal (AAT). By taking data loss into consideration when assigning vehicles as BSM verifier, the distribution of AATs is utilized for optimal AAT selection strategy.
- Considering the possible security threats that may still exist in the VABV system, the Sybil detection scheme is proposed to enhance the security of the system. The machine learning method Extreme Learning Machine (ELM) is adopted to achieve fast detection. We utilize edge servers embedded in IoV to collect information from BSMs in vehicles and extract the characteristics of vehicle mobility patterns, which will then be used to detect Sybil nodes. The Sybil detection scheme includes BSM collection, BSM data preprocessing and Sybil detection.
- The quantified AoI is adopted as the integrated performance indicator, which takes into account both the timeliness and security of the VABV system. Through AoI, the evaluation of the dependability of VABV system can be made more intuitive, and the coordination of VABV system can be improved through the inspection of AoI of VABV system.

**Organization**

The remainder of this article is structured as follows. Section “Designed VABV system and corresponding dependability requirements” introduces the security fundamentals and VABV system model, also the corresponding dependability requirements are described. In section “Comprehensive AAT selection strategies for VABV system,” the selection strategies for timeliness of BSM verification are depicted in details. The scheme against BSM generated by Sybil nodes is described in section “Detection scheme against Sybil attacks for VABV system.” Section “Usage of AoI as the integrated indicator for VABV system” describes the novel system evaluation indicator AoI and analysis of dependability for VABV system using AoI. Section “Simulation and discussions” showcases the simulation results and discussions, followed by the conclusion of this article in section “Conclusion and future work.”
the BSM. TA is regulated by government departments and is absolutely credible. It is responsible for the issue of system parameters in the Initialization phase before the whole system runs. At the start of the system, all vehicles in the network are ordinary terminals. After the AAT selection, some of OTs are selected as AATs and such vehicles are used to help the RSU in completing the BSM verification. RSU is established alongside the road or the intersection of roads. It is responsible for the selection of AATs, BSM verification, and validation of confirmation messages sent by the AATs. In the VABV system, the BSM of vehicles not verified by AATs will still be verified by RSU. Simultaneously, via a wired secure communication channel with the TA, the RSU receives system parameters from the TA and distributes them to all vehicles within its coverage area for generation of BSM signatures by the vehicles. The edge server connected to it is responsible for the Sybil detection. It first generates the corresponding steering state transition matrix (SSTM) of each vehicle through BSMs collected by RSU from the vehicles within the coverage of RSU. The driving characteristics of each vehicle are captured by the eigenvalues of SSTM. And based on the dissimilarity of driving features of benign vehicles and Sybil nodes, machine learning algorithms are used to identify Sybil nodes.

### Table 1. Notations and corresponding definitions.

| Notation | Definition |
|----------|------------|
| $V_i$   | The $i$th vehicle |
| $AAT_j$ | The $j$th vehicle which serves as a mobile node that helps the roadside unit (RSU) for Basic Safety Message (BSM) verification |
| $p, q$  | Two large prime numbers |
| $a, b$  | Two parameters used in a non-singular elliptic curve $E: y^2 = x^3 + ax + b \mod p$ |
| $P$     | Generator for $q$-order addition group $G$ |
| $G$     | All the points on curve $E$ and infinity form an addition group |
| $\text{RID}_i$ | The real identity of $i$th vehicle |
| $\text{PID}^1, \text{PID}^2_i$ | Two pseudonyms used for message signature of $i$th vehicle |
| $n_i$   | A random number chosen by $i$th vehicle |
| $s$     | System private key |
| $P_{pub}$ | System public key |
| $T_{act-sm}$ | Computational overhead of dot product calculation |
| $T_{act-sm-small}$ | Computational overhead of small factor dot product operation |
| $T_{act-add}$ | Computational overhead of addition operation |
| $T_h$ | Computational overhead of hash operation |
| $M_i$ | BSM generated by the $i$th vehicle |
| $T_1$ | The generation time of BSM generated by the $i$th vehicle |
| $\sigma_i$ | The signature of BSM generated by the $i$th vehicle |
| $T_2$ | Calculation latency related to the batch size of batch verification |
| $T_3$ | Calculation latency which has no relationship with the batch size of batch verification |
| $T_4$ | Transmission latency of PID |
| $T_e$ | Transmission latency of the extra contents attached to BSMs |
| $h()$ | Hash operation |
| $f_r$ | Computing power of the RSU |
| $f_j$ | Computing power of AAT $j$ |
| $M$ | The overall number of auxiliary authentication terminals (AATs) |
| $N_i$ | The number of BSMs that AAT $i$ verifies in a batch |
| $N$ | The overall number of vehicles in a certain area |
| $r$ | Communication range of AAT |
| $R_{trans}$ | Transmission rate for sending confirmation messages by AATs |
| $A_r$ | Maximum communication coverage range of the RSU which is located in an intersection |

PID: pseudo-identity.
**Dependability requirements.** Based on the proposed VABV system, as the quality of BSMs has a great deal of influence on the functionality of this system, it is of critical importance to evaluate it in terms of BSM. In light of the characteristics necessary to initiate and function a VABV system smoothly and effectively, the dependability requirements for a VABV system can be summarized as follows:

- **Timeliness:** The effectiveness and reliability of the BSM exchange are of great importance; therefore, the verification of the BSMs must meet the criteria of timeliness. In short, the faster a vehicle user receives BSM, the more timely the driver can make better driving decisions based on the received, nearly real-time BSM in order to prevent traffic accidents, or for the IoV to better coordinate and manage vehicle flow.

- **Information Security:** The VABV system rests on reliable BSM exchange, which originates from the security of BSMs. Because of the open wireless environment of IoVs, they are vulnerable to cyber attacks. According to VABV system, the possible and fatal attacks can be concluded as BSM tampering and Sybil attack. Whether the vehicle is able to make the right decisions when driving is directly impacted by how accurate and reliable the information in the BSM is. This, in turn, impacts road safety. In this context, the security of information also contributes significantly to the dependability of the VABV system.

**ECC-based batch verification**

Based on the system’s requirements for timeliness and information security, a cryptography algorithm needs to be chosen that are suitable to our system. The selection of the encryption algorithm must take into account not only the security strength of the algorithm but also the calculation time overhead which has to be minimized for message encryption and verification. Rivest-Shamir-Adleman (RSA), ECC, bilinear mapping, and so on are the most commonly used encryption algorithms on the IoVs. With respect to the RSA algorithm, 160-bit ECC and 1024-bit RSA have the same level of security; however, 160-bit ECC signatures and decryptions are considerably faster than RSA.\(^{29}\) The cost of bilinear pairing operations and scalar multiplication operations is much higher than the cost of the scalar multiplicative calculations performed by ECC.\(^{30}\) In addition, in some previous works, the Map to Point Hash function is used, which also evidently increases computation delay.\(^ {31}\) The upper part of Figure 2 illustrates how a high computational overhead encryption algorithm can result in multiple BSMs not being verified until after the expiration date has passed, resulting in their discard. Overall, the use of ECC as a secure foundation for our work can be more effective in meeting the system’s needs for timeliness. All the messages must be encrypted with ECC and the RSU and AATs should verify these message signatures. In order to confirm the validity of multiple BSM signatures at the same time, we adopt the batch verification method based on ECC. The security process is briefly described as follows.

**Elliptic curve cryptography.** An elliptic curve $E$ over a prime finite field $F_p$ can be defined by the cubic equation $y^2 = x^3 + ax + b$, where $a, b \in F_p$, as well as the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. The set of all points $P = (x, y)$ on $E$ and an additional point at infinity $O$ constitute an additive cyclic group $G$ under the point addition law + explained by a tangent and chord method: Let $P, Q$ be two random elements of the group $G$, $l$ be the line that contains $p, Q$ (tangent line to $E$ if
P = Q) and another point \( R \) intersected of \( l \) with \( E \). \( l \) represents the line which connects \( R \) and parallels to the y-axis. We can define \( P + Q = R \in E \), where the line \( l \) intersects with \( E \) on the point \( R \). Furthermore, the definition of a scalar multiplication is 
\[
kP = P + P + P + \ldots + P.
\]

**Definition 1.** (ECDLP, Elliptic Curve Discrete Logarithm Problem). For a random number \( m \in \mathbb{Z}_q \), given two elements \( P, Q \) of the group \( G \) such that \( Q = mP \), the aim of ECDLP is to calculate out \( m \).

**Initialization.** The TA sets up the system and generates the system parameters based on ECC encryption as \( \{ p, q, a, b, P, P_{pub}, h \} \). Then the TA preloads these parameters into the vehicles’ tamper resistant unit (TPD).

The generation of vehicles’ pseudo-identity and message signature. When the vehicle constructs a message, it must sign it before sending it to ensure the authenticity. The TPD of the vehicle randomly chooses \( r_i \in \mathbb{Z}_q \) and calculates the pseudo-identity \( \text{PID}_i = \{ \text{PID}^1_i, \text{PID}^2_i \} \), where \( \text{PID}^1_i = r_iP \) and \( \text{PID}^2_i = \text{RID} \oplus h(r_iP_{pub}) \). Then the TPD combines the message \( M_i \) with the current timestamp \( T_i \) and generates a signature. The signing result is \( \sigma_i = s \cdot h(\text{PID}_i) + r_i \cdot h(M_i \parallel T_i) \), where \( s \) is the system private key and \( M_i \) is the BSM message generated by vehicle \( i \) with the concurrent timestamp \( T_i \), representing the time \( M_i \) is sent. Both the RSU and the vehicles acting as the verifier, that is, the AATs, receive the digital signatures \( \sigma_i \) corresponding to the different vehicles in its communication range as well as the original information \( M_i \) to complete the batch verification. Finally, the TPD broadcasts \( \{ \text{PID}_i, T_i, M_i, \sigma_i \} \).

The batch verification performed by RSU and AAT. After receiving \( \{ \text{PID}_i, T_i, M_i, \sigma_i \} \), either RSU or the AAT needs to verify it to avoid from being misled. The batch size of AAT\(_j\) is represented as \( N_j \). AAT\(_j\) randomly chooses a small integer \( t \) with 10-bit-length and generates a set of random factors \( v_j(v_{j(1 < i < N_j)} \in [1, 2^t]) \). Then it checks whether the batch verification Eq. (1) holds. If the Eq. (1) holds, it means that the batch verification succeed. Otherwise, there must be at least one invalid message within in the batch.

\[
\left( \sum_{i=1}^{N_j} (v_i \cdot \sigma_i) \right) P = \left( \sum_{i=1}^{N_j} v_i \cdot h(\text{PID}_i) \right) \cdot P_{pub} + \sum_{i=1}^{N_j} v_i \cdot \text{PID}^1_i \cdot h(M_i \parallel T_i)
\]

The establishment of the Eq. (1) indicates that no message is tampered with in the batch. The correctness of the above batch verification is given as follows

\[
\left( \sum_{i=1}^{N_j} (v_i \cdot \sigma_i) \right) P = \left( \sum_{i=1}^{N_j} v_i \cdot h(\text{PID}_i) + r_i \cdot h(M_i \parallel T_i) \right) P
\]

\[
= \left( \sum_{i=1}^{N_j} v_i \cdot h(\text{PID}_i) \right) sP + \sum_{i=1}^{N_j} v_i \cdot h(M_i \parallel T_i)r_iP
\]

\[
= \left( \sum_{i=1}^{N_j} v_i \cdot h(\text{PID}_i) \right) \cdot P_{pub} + \sum_{i=1}^{N_j} v_i \cdot \text{PID}^1_i \cdot h(M_i \parallel T_i)
\]

Regarding the characteristics of batch verification as shown in the lower part of Figure 2, when there is at least one invalid signature in the batch (either tampered with or sent by a malicious vehicle itself), the verification of this batch will not pass and the invalid signature needs to be found with re-batch verification applied and then discarded. In this work, since the main type of attack we consider is the more threatening attack, in order to simplify the model, the case where the batch is re-verified because it contains invalid signatures inside is not considered for now.

**Latency model**

On the basis of aforementioned system model, the corresponding latency model is shown in Figure 3.

According to Figure 3, the system verification latency consists of two parts: one is the latency on the verification by RSU and AAT and we record them as \( T_j \) and \( T_{ru} \), respectively; the other one is induced by the verification of confirmation message by RSU and we record it as \( T_c \). Assume that the number of AAT is \( M \). The time on the RSU is set as a standard, the system verification latency is

\[
T_{overall} = \max\{ T_1, \ldots, T_j, T_{ru} \} + T_c \quad j \in [1, M]
\]

The two parts of the latency model are described as follows:

**Latency from the RSU.** The latency induced by the RSU consists of two parts: one latency \( T_{ru} \) is from the verification of BSMs came from the ordinary terminals, the other latency \( T_c \) is from the validation of verification confirmation messages came from the AATs. The verification latency \( T_{ru} \) is

\[
T_{ru} = T_{tran} + T_{com}^{ru}
\]

where \( T_{tran} \) is the message transmission latency from ordinary terminal to the RSU and \( T_{com}^{ru} \) is the calculation latency of the verification of BSMs. The terminal verified by the RSU is \( N_r \). Hence, according to Eq. (1), the computational cost of batch verification \( T_{com}^{ru} \) is

\[
N_r(T_{ec-sm} + T_{ec-sm-n} + T_{ec-sm} + 2T_h) + 2T_{ec-sm}.
\]

The computational overhead of \( s \cdot P \) is \( T_{ec-sm} \), the computational overhead of \( v_i \cdot P \) is \( T_{ec-sm-n} \), the computational overhead of \( s + T \), \( S \in G \) and \( T \in G \) is \( T_{ec-pa} \),
and the computational overhead of hash operation is $2T_h$. In the batch verification, there also exists operation like $s \cdot P$, so it is defined as $T_{ecc-sm}$. Since the operators of ECC are constants, we define $T_1 = T_{ecc-sm} + T_{ecc-sm-s} + T_{ecc-pa} + 2T_h$ and $T_2 = 2T_{ecc-sm}$. Therefore, the verification latency induced by the RSU can be formulated as follows

$$T_{rsu} = T_{tran1} + T_{com} = N_c T_1 + T_2 + T_{tran1} \quad (5)$$

In order to validate confirmation messages from AATs, batch verification is conducted. Let the total number of AAT to be $M$, then $T_{re}$ is calculated by

$$T_{re} = M T_1 + T_2 \quad (6)$$

Latency from the AAT. For the AAT, the latency consists of three parts. The first one is $T_{tran1}$ which represents the transmission latency induced by the sending of BSMs from the original terminals to the AAT. The second one is $T_{com}$ which represents the latency induced by the verification of BSMs on AAT. The last one is $T_{tran2}$ which represents the latency induced by the sending of confirmation messages from the AAT to the RSU.

For the verification latency of BSMs on AAT, the batch verification is also used. Let the batch size that the AAT takes to be $N_j$. Based on the computing capability of the RSU, the calculation latency that the AAT needs to spend is converted proportional to its own computing power, and is described as

$$T_{com}^j = \frac{f_j}{f} (N_j T_1 + T_2), \quad j \in [1, M] \quad (7)$$

where $f_j$ and $f$ represent the computing resource allocated for the verification of BSMs of the RSU and AAT, respectively.

For the transmission latency induced by the sending of confirmation messages from the AAT to the RSU, the data transmission rate is set as $R_{tran}$, the data length of the pseudo-identity is set as $L_{PID}$, and the length of some extra information that is appended is set as $L_{extra}$. Based on the format of batch information, we define that the length of confirmation packet is $(N_j L_{PID} + L_{extra}) / R_{tran}$, and we use $T_3$ and $T_4$ to represent the former item and the latter one, respectively.

To sum up, the latency on the AAT is

$$T_j = T_{tran1} + \frac{L_j}{R_{tran}} (N_j T_1 + T_2) + N_j T_3 + T_4, \quad j \in [1, M] \quad (8)$$

In the subsequent analysis and calculation, the transmission latency $T_{tran1}$ and $T_{tran2}$ are omitted since they are of a small order of magnitude compared with the calculation latency $T_{com}^j$ and $T_{com}^j$.

**Comprehensive AAT selection strategies for VABV system**

In this section, the proposed AAT selection strategies are described. BSM interaction is improved by selecting a certain number of vehicles as AATs before the BSM verification process begins. The whole process of AAT selection is depicted in Figure 4.

**Initial determination of the number of AATs**

When the RSU needs auxiliary vehicles for message verification, the first step is to determine how many vehicles are required. To achieving this, enlightened by Wu et al., where in an ideal IoV, all the ordinary vehicles have the same computing power for verification, the computing power of the ordinary nodes can
be calculated by \( f' = \sum_{i=1}^{N} \left( f_i / N \right) \). The verification of each ordinary terminal in the IoV is equal and is recorded as \( T_{\text{avg}} \). Then the system verification latency can be simplified as \( T_{\text{overall}} = \max\{T_{\text{avg}}, T_{\text{rsu}}\} + T_{\text{rc}} \). \( N_{\text{avg}} \) is the batch size of each ordinary terminal in this ideal IoV, which is defined as the distance between itself and the vehicles with the aid of GPS. Let \( D(i) \) represent the distance between the RSU and the vehicle \( V_i \), \( R \) represents the maximum coverage of the RSU. Then we evaluate the distance of each vehicle by calculating \( D(i)/R \) which is defined as the distance evaluation indicator.

Next the computing power of each vehicle is described by calculating \( f(i)/f_r \) which is defined as the computing power evaluation indicator.

By the time RSU calculates these two evaluation indicators for all vehicles in its vicinity, it will record and score them as shown in Table 2. On the basis of the vehicle’s current condition, we can assign each vehicle within the system a score indicating its priority to be selected as an AAT.
Table 2. The evaluation of vehicles.

| Vehicle Type | Distance | Computing Power | Score |
|--------------|----------|-----------------|-------|
| Type 1       | Short    | Good            | 1.0   |
| Type 2       | Short    | Moderate        | 0.8   |
| Type 3       | Short    | Bad             | 0.3   |
| Type 4       | Medium   | Good            | 0.7   |
| Type 5       | Medium   | Moderate        | 0.5   |
| Type 6       | Medium   | Bad             | 0.15  |
| Type 7       | Long     | Good            | 0.4   |
| Type 8       | Long     | Moderate        | 0.25  |
| Type 9       | Long     | Bad             | 0 |

\[ \text{SCORE}(V_i) = \omega_d S_d + \omega_p S_p \]  

where \( S_d \) and \( S_p \) represent the score earned in terms of distance and computing power, respectively, and \( \omega_d \) and \( \omega_p \) are the weighing factors for the two indicators satisfying \( \omega_d + \omega_p = 1 \). In our system, we set these two indicators based on the evaluation of computing power since we take the latency of verification as the primary issue. Concerning that when the computing power of vehicles are Good, we set \( w_d \) and \( w_p \) to 0.6 and 0.4, respectively, since the distance should be taken into more consideration to improve the communication quality between the vehicle and the RSU. By that analogy, \( w_d \) and \( w_p \) are set to both 0.5 when the computing power of vehicles are Moderate. And \( w_d \) and \( w_p \) are set to 0.3 and 0.7, respectively, when the computing power of vehicles is Bad. The final score for each type of vehicle is listed in the Table 2. Then the vehicles with a higher score will be chosen first. In the real IoV, if there is no vehicle with a higher score, the vehicles with lower scores will be selected as AATs. However, the lowest bound of score is set as 0.3. The ordinary vehicle scored equal to or less than 0.3 will not be selected even if there is no ordinary vehicles with score more than 0.3. If this happens in the real situation, the RSU will not initiate this AAT-aided verification system and the RSU will verify the messages by itself.

Distribution of AATs

During the verification cycle, if the communication overlap area between the assigned AATs is too large, a large number of redundant verification will be introduced (i.e. an OT verified by one AAT will also be verified by another AAT). The number of OTs verified by the RSU in this case rises, which in turn affects the total verification latency of the system. If the communication overlap area between assigned AATs is small, some assigned AATs may be located far from the RSU, resulting in poor communication quality with the RSU and introducing re-verification problems, which also introduces additional latency. Therefore, when selecting AATs, besides considering the performance of the vehicle itself, the distribution of AATs also needs to be considered.

Regarding this, we consider the model where a RSU is at the intersection and its communication range is \( R \). The area covered by the RSU is divided into several grids. We assume that the specified area is divided into \( m \times m \) grids, the AATs on this area are recorded in the vehicle set \( VS = \{AAT_1, AAT_2, ..., AAT_t\} \), where \( AAT_i = \{x_i, y_i, r_i\} \) is the coverage model of \( AAT_i \), \( (x_i, y_i) \) is the coordinates of \( AAT_i \), and \( r_i \) is the communication range of \( AAT_i \). In our study, we assume that the communication ranges of the vehicles are the same and the communication ranges of the vehicles are centered on the vehicle coordinates in a circular area of radius \( r \). The grid point on the road is taken into account in this distribution model. The coverage area and overlap area of AATs are defined as follows:

Network coverage index. A probability associated with the grid point \( G(x, y) \) being covered by \( AAT_i \) is as follows:

\[ P_{cover}(x, y, AAT_i) = \begin{cases} 1, & \text{if } D(x, y, AAT_i) \leq r_i \\ 0, & \text{otherwise} \end{cases} \]  

where \( D(x, y, AAT_i) \) is the distance between the grid point \( G(x, y) \) and \( AAT_i \). If the grid point \( G(x, y) \) is within the communication range of any AAT, it could be assumed that this point is within the vehicle set. Therefore, the coverage ratio of the vehicle set can be calculated by:

\[ P_{cover}(x, y, AAT) = 1 - \prod_{i=0}^{m} (1 - P_{cover}(x, y, AAT)) \]  

In this case, the network coverage index \( \alpha \) can be calculated by:

\[ \alpha = \frac{\sum_{m} \sum_{y=-R}^{m} P_{cover}(x, y, AAT)}{A_r} \]  

where \( A_r \) is the area of the intersection covered by the maximum communication range of the RSU.

Network redundant index. We calculate the probability of a grid point \( G(x, y) \) being located in the overlap communication range where two or more AATs intersect and record this as the redundant network area.

\[ P_{overlap}(x, y, AAT) = \begin{cases} 1, & G \in CR(AAT), G \in otherAAT \\ 0, & \text{otherwise} \end{cases} \]
where the $CR(AAT_j)$ is the communication range of $AAT_j$. Then we can calculate the network redundant index $\beta$ and is given by

$$\beta = \frac{\sum_{x} \sum_{y} (\sum_{i} P_{\text{overlap}}(x, y, AAT_i) - 1)}{A_r}$$  \hspace{1cm} (19)$$

For simplicity of calculation, we convert the highest coverage rate to the lowest uncovered rate, so that when the RSU chooses the AAT among ordinary vehicles, the following value is used which we call the distribution index $\xi$

$$\xi = k_1(1 - \alpha) + k_2\beta$$ \hspace{1cm} (20)

where $k_1$ and $k_2$ are the weight factor and $k_1 + k_2 = 1$, the value of $\xi$ is between 0~1. The RSU continuously records the $\xi$ to better coordinate the selection of AAT.

### Detection scheme against Sybil attacks for VABV system

To enhance the security of the VABV system, in this section we analyze the security risks that may be present and propose a detection scheme that uses information contained within the BSM to detect abnormal nodes.

#### Vulnerability analysis

Sybil security threat in vehicular networks has attracted much attention in recent times. The proposed system is equally vulnerable to such attacks. In Figure 5, the Sybil attack that may exist in VABV system is shown.

In VABV system, each vehicle is equipped with a TPD storing system parameters. Vehicles periodically broadcast signed BSMs. In order to guarantee the users’ privacy, each vehicle has two pseudonyms $PID_1^i$ and $PID_2^i$ for BSM interaction instead of using their real identity $RID_i$. However, using this pseudo-identity is vulnerable to Sybil attacks. There is a possibility that some original benign vehicles become malicious due to selfish personal reasons, such as trying to take priority for travel. In this situation, the security parameters stored in the TPD of malicious vehicles will be abused to launch Sybil attack. It is feasible for the malicious vehicles to launch this attack since the system private key $s$ is stored in its TPD. Then it will choose multiple nonce to generate multiple fake pseudonyms $\{PID_1^a, PID_2^a, ..., PID_k^a\}$. These fake pseudonyms are used to act as virtual vehicular nodes. As shown in Figure 4, certain originally benign vehicles become malicious for selfish private reasons and cut off the communication between certain benign vehicles. They create virtual nodes and send false BSMs as virtual nodes, which increase the probability of traffic accident, thus achieving the purpose of launching Sybil attack.

To achieve the purpose of launching Sybil attacks successfully, malicious vehicles must calculate the ideal idle space on the road for virtual nodes generation. Due to the virtual nature of Sybil nodes, if they claim a geographic position occupied by an existing physical vehicle, they will be easily detected by other benign vehicles and the attack will not succeed. In addition, malicious vehicles must modify the BSMs that virtual nodes broadcast in order to make them more reasonable.

According to the above analysis, the attacking tricks used by malicious vehicles will be upon the BSMs from benign vehicles. Malicious vehicles will fabricate some unreal BSMs according to the BSMs from its neighbors.

#### Attack detection

In Gu et al., a support vector machine (SVM)-based Sybil detection scheme is proposed, where the detection
rate is relatively high; however, it suffers from high complexity. In addition, the accuracy of such a shallow learner is heavily dependent on feature extraction. If the extracted features cannot effectively show the differences between vehicles well, the detection accuracy will likely be greatly reduced. In vehicular networks, due to the large amount of BSMs, detection scheme with relatively low complexity is needed. To explore the potential of machine learning in this study and overcome the problems such as high complexity that will happen in traditional BP networks, the ELM is adopted. The whole process of proposed Sybil detection scheme is shown in Figure 6. Since the purpose of virtual vehicles is to eliminate the safety of other benign vehicles, the steering states of benign and virtual vehicles should differ, which may not be judged intuitively. Hence, the detection of Sybil nodes can be equivalent to the measurement of difference of steering state.

**Vehicle steering state description.** In order to describe in great detail the transition of steering state of vehicles, a matrix should be used. A matrix is defined as a set of data indicative of the movement of the vehicle in a given period of time. According to the contents in BSM, the steering state transition matrix (SSTM) of vehicles from the time $t_1$ to $t_n$ is formulated as follows

$$H_{V_i} = \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} \\ s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} \\ s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{n,1} & s_{n,2} & s_{n,3} & s_{n,4} & s_{n,5} & s_{n,6} \end{bmatrix}$$

(21)

The above specific matrix $H_{V_i}$ is constructed by time sequence. First the steering state description of $V_i$ at time $t_n$ is represented as a vector $S_{V_i,t_n} = (s_{n,1}, s_{n,2}, s_{n,3}, s_{n,4}, s_{n,5}, s_{n,6})$, where

- $s_{n,1}$ is the time at $t_n$,
- $s_{n,2}$ is the location of vehicle at $t_n$,
- $s_{n,3}$ is the velocity of vehicle at $t_n$,
- $s_{n,4}$ is the variation of velocity of vehicle between $t_{n-1}$ and $t_n$,
- $s_{n,5}$ is the acceleration of vehicle at $t_n$, and
- $s_{n,6}$ is the variation of acceleration of vehicle between $t_{n-1}$ and $t_n$.

**Vehicle steering state transition matrix preprocessing.** From the formulation of SSTM, we can see that it is not suitable for direct analysis since the SSTM of each vehicle varies and the characteristic of them are not obvious at this dimension. Hence, the SSTM should be processed under dimension reduction by the calculation of each SSTM $H_{V_i}$. The details of SSTM preprocessing are described in Algorithm 1.

For each SSTM $H_{V_i}$, the transposed matrix of $H_{V_i}$ is $H_{V_i}^T$. Then $H_{V_i}^T$ is multiplied by $H_{V_i}$ to generate a square matrix $H_{V_i}^z$ with the dimension of $6 \times 6$ since we use six attributes to describe the mobility of vehicle at a specific time. Then an eigenvalues calculation function is applied to $H_{V_i}^z$. The direct calculation of eigenvalues may generate vectors with complex numbers, leading to inaccuracy of representation of mobility of vehicles. To solve this problem, the centering method of matrices is used, the essence of which is the translation of matrices. The mean value $m_j$ of each column $j$ of $H_{V_i}$ is calculated.
and subtracts this value from each element in the corresponding column to replace every original value in $H_{V_i}$.

Next, the eigenvalues of $H_{V_i}^0$ are calculated, where $H_{V_i}^0 = (H_{V_i}^T \cdot H_{V_i})u_j = \lambda_j u_j (1 \leq j \leq 6)$. Each eigenvalue, $\lambda_j$ (w.r.t. $u_j$) of matrix $H_{V_i}^0$ represents the characteristics of the original SSTM $H_{V_i}$.

Also, it is of necessity to select out some eigenvalues that well depict the mobility characteristic of a vehicle, the suitability of which can be represented by the Energy (E) of the eigenvalues. A total Energy higher than well depict the mobility characteristic of a vehicle, neurons in hidden layer can be mathematically defined for each vehicle.

\[ H_{V_i} = \sum_{j=1}^{6} \beta_j G(w_j \cdot x_j + b_j) = t_j \quad j = 1, 2, ..., K \]  

The vector $w_j$ and $b$ are randomly set, then vector $\beta$ can be calculated and is expressed mathematically by

\[ H\beta = T \]  

where

\[ H = \begin{bmatrix} G(w_1 \cdot x_1 + b_1) & \cdots & G(w_6 \cdot x_1 + b_6) \\ \vdots & \ddots & \vdots \\ G(w_1 \cdot x_k + b_1) & \cdots & G(w_6 \cdot x_k + b_6) \end{bmatrix}_{k \times o} \]  

\[ \beta = \begin{bmatrix} \beta_1^T \\ \vdots \\ \beta_6^T \end{bmatrix}_{o \times l} \quad T = \begin{bmatrix} t_1^T \\ \vdots \\ t_k^T \end{bmatrix}_{k \times l} \]  

Hence, the ELM training process is described as follows:

1. Choose activation function $G(x)$ and number of neurons in hidden layer $o$. In our network, sigmoid function is selected

\[ G(x) = \frac{1}{1 + e^{-x}} \]  

2. Given training data $x_t$ and target value $t_i$, the input weights $w$ and the bias $b$ are randomly set.
3. Calculate the output matrix $H$ of hidden layer using $G(x)$, $w$ and $b$ and $x$.
4. Determine the output weight vector $\beta$

\[ \beta = H^\dagger T = (H^T H)^{-1} H^T T \]  

where $H^\dagger$ is the Moore-Penrose generalized inverse of the matrix $H$.

**Usage of AoI as the integrated indicator for VABV system**

In VABV systems, the periodic transmissions of BSMs from vehicles are closely related to the system’s dependability. The large BSM verification latency and hazardous attacks can cause havoc in the VABV system. Indicators of IoV traditionally used to evaluate IoV are not appropriate for evaluating timeliness and security performance synthetically. Therefore, the concept of the AoI is proposed to be used as a key indicator for VABV systems in order to quantify the dependability.
The analysis of AoI as indicator for evaluation of timeliness and security

According to the aforementioned analysis of dependability requirements of VABV system, the AoI is adopted to quantify the dependability of VABV system.

First introduced into the area of research for vehicular networks in Kaul et al., Aoi is used to quantify the freshness of information at a destination node (i.e. a receiver vehicle) generated by the source node (i.e. a sender vehicle). To describe it in a more formal way, AoI in IoV networks can be defined as the time elapsed since the last successfully received BSM at the side of receiver vehicle which is generated at the sender vehicle. Even if a fabricated BSM is received, the safety-related application cannot generate correct driving decision according to the contents in it. Hence, it cannot be considered a successfully reception of BSM. Any disturbance happens in VABV system will be reflected by the AoI. Hence, through AoI, we can better analyze the VABV system from the perspective of IoV users. For better understanding the AoI, Figure 7 illustrates a formation of AoI, denoted by $Aoi_{s,r}(t)$, at the receiver vehicle $r$ as a function of time when a nearby sender vehicle $s$ sends the BSMs. Assuming that in one verification period each sender vehicle just send one BSM to the expected receiver vehicle, let $t$ represents the generation time of BSM by the sender vehicle $s$, then AoI at the receiver vehicle $r$ at the current time $t'$ in the $i$-th verification period is calculated by

$$Aoi_{s,r}(t) = t' - t$$

As depicted in Figure 7, the curve of $Aoi_{s,r}$ can be described in Eq. (30), which is shown at the bottom of this page. $Aoi_{s,r}^{-1}$ is the final AoI of the last successfully received BSM verification cycle.

$$Aoi_{s,r}(t) = \begin{cases} t - t_{i-1} + Aoi_{s,r}^{-1}, & \text{no BSM reception between } t_{i-1} \text{ and } t_i \\ t_i - t, & i_{th} \text{ BSM is received successfully by receiver vehicle at } t_i \\ 0, & \text{final BSM is received successfully at } t_n \end{cases}$$

Note that from the definition of AoI, the lower the value of AoI, the fresher the information. Also, the sending time of BSM makes no sense to the AoI. It is also noteworthy that $Aoi_{s,r}(t)$ is a zigzag-like curve with a slope of 1 during each BSM inter-reception intervals and is reset to $(t' - t)$ in each time instance once the sender vehicle’s BSM is successfully received by the receiver vehicle. It is evident from the Figure 7 that at $t_2$ (marked by the red dashed line) the sender vehicle sends a BSM; however, due to an attack or other causes, the receiver vehicle does not receive or cannot make a correct driving decision based on the received BSM. At this point, the receiver vehicle does not reset the AoI, but continues to rise it until at $t_3$ it successfully receives a BSM that can generate the correct driving decision, and then resets the value of AoI. As a result of the above rules of AoI accumulation, it can be seen that any disturbance to the system will increase the value of AoI and ultimately decrease the dependability of the system.

For the convenience of quantification, the area under the envelope of AoI is calculated. And in order to calculate in an easier way, the area of envelope curved by the AoI is divided into three parts: a polygon area $S_1$, the trapezoidal area $S_2$, $i \geq 2$, and a triangular area $S_3 = \frac{1}{2}A_n$. Therefore, in a complete verification process in VABV system, the AoI calculated by the driving user can be denoted as

$$Aoi_{s,r} = S_1 + \sum_{i=2}^{n} S_i + \frac{1}{2}A_n^2$$

The broadcast interval of BSM is given by $\Delta t$, $t_{i+1} - t_i$ represents the inter-departure time between the adjacent successfully received BSMs and we denote it as $B_i$. Then the calculation of $S_i$ is given by

$$S_i = \frac{1}{2}(A_i + B_i)^2 - \frac{1}{2}A_i^2 = \frac{1}{2}B_i^2 + A_iB_i \ (i \geq 2)$$
Using Eq. (31) and Eq. (32), the average AoI between the sender vehicle \(s\) and receiver vehicle \(r\) can be calculated by

\[
AoI_{s,r}^{avg} = \frac{1}{T} \int_{0}^{T} AoI_{s,r}(t) = \sum_{s \leq r} \frac{S_{s,r}}{T} \tag{33}
\]

Considering that for a specific receiver vehicle \(r\), it has \(R_r \subseteq N\) neighboring vehicles, that is, \(s \in R_r\) where \(N\) is the overall number of vehicles in the VABV system. Then the average AoI at a receiver vehicle \(r\) can be given by

\[
AoI_{r}^{avg} = \frac{1}{R_r} \sum_{s \in R_r} AoI_{s,r}^{avg} \tag{34}
\]

Eventually, the VABV system average AoI with \(N\) vehicles can be calculated as

\[
AoI^{avg} = \frac{1}{N} \sum_{r \in N} AoI_{r}^{avg} \tag{35}
\]

In VABV system, \(AoI_{s,r}\) and \(AoI_{r}^{avg}\) represent the wholly and average dependability for a vehicle user in a specific time period, respectively. However, some instantaneous disturbance will result in the fluctuation of AoI in some verification period. Whenever the disturbance disappears, the AoI drops down with the dependability in some verification period. In this situation, \(AoI_{s,r}\) and \(AoI_{r}^{avg}\) cannot precisely describe this phenomenon. In order to analyze the instantaneous dependability of VABV system, the peak AoI is defined as follows

\[
AoI_{r}^{peak} = A_i + B_i \tag{36}
\]

In a verification period, the peak AoI represents the time when the dependability of the VABV system is at its worse. The analysis of peak AoI can provide timely information about the effect some disturbances have on the VABV system.

The performance of AoI indicator on timeliness

The first issue that influences AoI is necessary BSM verification latency. In the above analysis of AoI, it is easily concluded that the value \(A_i\) in AoI is equal to the VABV system verification delay, which is given by follows

\[
A_i = T_{overall} = max\{T_1, \ldots, T_j\} + T_r \tag{37}
\]

It is easy to find that the number and computing power of AATs influence the performance of AoI in each BSM verification cycle, which is closely related to the AAT selecting strategies.

Another issue that influence AoI is data loss. To make the verification system function better, the success of confirmation messages delivered to the RSU should be guaranteed. To achieve this, the distance of AATs to the RSU is considered, which can be reflected by the distribution of AATs. In Cui et al.,\textsuperscript{15} the authors think that the relatively short distance from the AAT to the RSU will provide a more reliable communication. Since the longer the distance between the AAT and the RSU is, the more path loss (PL) will be generated, which will affect the communication quality between them as well as the possibility of data loss. Hence, by the time some vehicles have been assigned to be AATs, the transmitting power \(P_j\) of \(AAT_j\) at the time of sending confirmation message should be recorded. And the estimated receiving power \(P_{r,j}\) of \(AAT_j\) at the RSU side is calculated by

\[
P_{r,j}[dBm] = P_j[dBm] + K_j - d_{(d_0, d_f)} \tag{38}
\]

where \(K_j\) is related to the computing power of AAT and the interference and noise it endures. \(d_{(d_0, d_f)}\) is related to the power loss induced by the transmission distance \(D(i)\) described in the second part of section “Comprehensive AAT selection strategies for VABV system.” It is noteworthy that due to the mobility of IoVs, the distance to the RSU is changed during one verification cycle, \(d_0\) is the initial distance when verification starts, and \(d_f\) represents the final distance once the same verification ends. However, with the small latency for verification, the difference between \(d_0\) and \(d_f\) could be neglected.

The estimation value of receiving power for each AAT is compared with the threshold value \(P_{r,th}\), the confirmation message sent by the AAT, with an estimation value smaller than \(P_{r,th}\) will not be successfully received by the RSU.

If a confirmation message failure is reported on an AAT during each BSM verification cycle, the vehicles near that AAT that fails to deliver the confirmation message will be evaluated by the RSU and selected to complete the BSM verification for that BSM cycle in its place and to resend the confirmation message. Then the value \(A_i\) of vehicle \(r\) within coverage of \(AAT_{fail}\) in AoI is given by

\[
A_i' = T_r + T_{rc} + T_{re-as} + T_{re-tr} + T_{re-com} \tag{39}
\]

where \(AAT_{fail}\) is original assigned AAT that failed to send the confirmation message to the RSU, \(T_{re-as}, T_{re-tr}, T_{re-com}\) represent the latency induced by re-assigning another vehicle, re-sending new confirmation message and re-verifying BSMs to compensate for the failure of \(AAT_{fail}\), respectively.

From the above analysis, we can infer that both verification for BSM and data loss ratio influence the performance of AoI by the variation of \(A_i\) in each verification cycle.
To sum up, the AoI performance with respect to the BSM verification in VABV system is

\[
A_i = \max_i \{T_1, \ldots, T_j\} + T_{rc} + TK^1[\max((T_{re-as} + T_{re-tr} + T_{re-com})_m)] \quad (40)
\]

\[m \subseteq AAT_{fail}, TK^1 \in (0, 1)\]

where then token TK^1 indicates whether any sending failure of AAT_{fail} happens in a verification cycle. TK^1 = 1 means some AATs fail to send confirmation message to the RSU and no such situation happens when TK^1 = 0.

The performance of AoI indicator on information security

In the first part of this section, we can infer that the quantitative factors that affect the VABV system AoI include \(A_i\) and \(B_i\), of which \(A_i\) is effected by the latency while \(B_i\) is effected by whether the BSM can be successfully received and the correct driving decision can be made based on it. In order to analyze the VABV system from the perspective of BSM security, in this subsection, we first consider the calculation of \(A_i\) and \(B_i\) of the VABV system under the Sybil attack. Then we consider the calculation of \(A_i\) and \(B_i\) of the VABV system using ELM-based Sybil BSM detection.

AoI performance of VABV systems considering Sybil attacks. From the above analysis on Sybil attack that may happen in VABV system, we can infer that if a vehicle suffers a Sybil attack, the malicious node intercepts the BSM of the benign vehicle with which it would otherwise interact with a normal BSM, pretends to be real by forging a PID and furthermore fabricating a virtual node, and sends a fake BSM to it. Unless the attacked vehicle is able to take security detection measures in time, it may not receive the correct BSM for several consecutive BSM verification cycles, which will result in an incorrect driving decision, which will pose a significant risk to road safety. In this case, the \(B_i\) will become larger due to the attack, resulting in a steep increase in the AoI curve for a certain period of time. Thus, in the case of a Sybil attack, the \(B_i\) of the victim receiver vehicle \(r\) can be given by

\[
B_{r-Sybil} = \left[1 + \frac{T_{effect} + T_{recover}}{\Delta t}\right] \cdot \Delta t \quad (41)
\]

where \(T_{effect}\) is the duration of the Sybil attack, during which the BSMs received by the vehicle are spurious. \(T_{recover}\) is the time required for the vehicle to become aware of the Sybil attack and request to the RSU to disconnect communication with the virtual node of the Sybil identity and recover from the Sybil attack. \(\Delta t\) is the predefined BSM broadcast interval in IoV. \([\cdot]\) is ceiling operation.

Since the BSMs received when they are attacked by Sybil are spurious, it is meaningless to analyze \(A_i\) at this time because it cannot be counted as a successful reception. Therefore, we only consider \(A_i\) after the vehicle \(r\) has recovered from the Sybil attack, and at this time, the \(A_i\) of the vehicle \(r\) will only be affected by the BSM verification latency and can be given by

\[
A_i' = T_{rc} + TK^1[(T_{re-as} + T_{re-tr} + T_{re-com})_m] \quad (42)
\]

\[m \subseteq AAT_{fail}, TK^1 \in (0, 1)\]

From the above analysis, it can be seen that if appropriate and efficient Sybil detection method is not adopted, the \(B_i\) of the vehicle attacked by Sybil will be greatly affected, which in turn will affect the AoI performance of the whole VABV system, and the dependability of the VABV system will be significantly reduced. At the same time, as the vehicle under Sybil attack cannot receive the correct BSM, it cannot generate correct and reliable driving decision, which will pose a threat to road safety.

AoI performance of VABV systems considering detection scheme against Sybil attacks. By using Sybil BSM detection based on machine learning, Sybil attacks can be effectively countered and thus the dependability of the VABV system can be improved. However, there is a certain error in identifying Sybil BSM, and the unnecessary processing latency brought by it will likewise have an impact on the system AoI. Therefore, we also need to make a dependability analysis of the VABV system that utilizes Sybil detection. A Sybil detection parameter \((F_r, D_r)\) is introduced, where \(F_r\) stands for whether the vehicle \(r\) is actually attacked by Sybil launchers and \(D_r\) stands for the detection results of the received BSM. \(F_r = 1\) means that the vehicle \(r\) is actually under Sybil attack and \(F_r = 0\) means the vehicle \(r\) is in normal condition. \(D_r = 1\) indicates the detection result is that some BSMs received by vehicle \(r\) are Sybil BSMs. \(D_r = 0\) indicates the detection result is that some BSMs received by vehicle \(r\) are all genuine and valid BSM. Based on Sybil detection parameter, we can summarize the \(B_{r-De}\) of vehicle \(r\) as Eq. (43) describes.

\[
B_{r-De} = \begin{cases} 
\frac{\Delta t}{(1 + \left[\frac{T_{effect} + T_{recover}}{\Delta t}\right]) \cdot \Delta t}, & (F_r, D_r) = (0, 0) \\
\frac{\Delta t}{(1 + \left[\frac{T_{effect} + T_{recover}}{\Delta t}\right]) \cdot \Delta t}, & (F_r, D_r) = (1, 0) \\
\frac{\Delta t}{(1 + \left[\frac{T_{effect} + T_{recover}}{\Delta t}\right]) \cdot \Delta t}, & (F_r, D_r) = (1, 1) \\
\frac{\Delta t}{(1 + \left[\frac{T_{effect} + T_{recover}}{\Delta t}\right]) \cdot \Delta t}, & (F_r, D_r) = (0, 1)
\end{cases} \quad (43)
\]

As described by the Eq. (43), based on the actual condition of the vehicle and the detection results, it can
be divided into four scenarios, which correspond to the corresponding $B_{i}^{r}_{-De}$. As for the first situation $(0,0)$, the vehicle is in normal condition and the detection results are consistent with it. In this scenario, $B_{i}^{r}_{-De}$ is equal to the broadcast interval of the BSM because there is no Sybil attack causing the vehicle to fail to receive the BSM successfully. However, the detection latency will have an impact on $A_{i}^{r}_{-De}$. In scenario $(1,0)$, the vehicle is actually under Sybil attack and the detection result is not consistent with it, which can cause the vehicle to be affected by the Sybil attack for a longer period of time and not receive the correct BSM. At this point, the value of $B_{i}^{r}_{-De}$ is consistent with $B_{i}^{r}_{-Sybil}$. In $(1,1)$, the vehicle is actually suffering from Sybil attack and the detection result is consistent with it. Then the impact time of Sybil attack is negligible and the vehicle needs to do is to recover from the Sybil attack. At this point, the value of $B_{i}^{r}_{-De}$ is much smaller than $B_{i}^{r}_{-Sybil}$. As for the last case $(0,1)$, the vehicle is not under attack, but the wrong detection result causes that the vehicle will take unnecessary time to recover from the already non-existent Sybil attack at this time, which increases the value of $B_{i}^{r}_{-De}$ needlessly.

After recovering from the attacks, for a receiver vehicle $r$, its dependability parameters $A_{i}^{r}_{-De}$ can be given by

$$A_{i}^{r}_{-De} = T_{De} + T_{r} + T_{rc} + TK^{1}[T_{rc} + T_{rc} + T_{rc-com}]_{m}$$

where $T_{De}$ is the latency required for Sybil detection.

From the perspective of information security, the Sybil attack detection latency and the accuracy of detection are the two most significant factors that impact the dependability of VABV systems.

**Simulation and discussions**

In this part, we analyze the AoI performance with respect to Timeliness and Information Security based on simulations.

---

**Table 3.** The execution time of the basic cryptographic operations.

| Cryptographic operation | Symbol      | Execution time/ms |
|-------------------------|-------------|-------------------|
| The dot product operation | $T_{sec-sm}$ | 0.442             |
| The small factor dot production operation | $T_{sec-sm-s}$ | 0.0138            |
| The addition operation | $T_{sec-pa}$ | 0.0018            |
| The hash operation | $T_{h}$ | 0.0001            |

**Table 4.** Simulation parameters.

| Parameter                        | Value          |
|----------------------------------|----------------|
| Number of vehicles               | 50 100 200     |
| Data transmission rate           | 12 Mbps        |
| BSM size                         | 100 Bytes      |
| Vehicles communication radius    | 300 m$^{-1}$   |
| Vehicles transmitting power      | 20 dBm         |
| RSU receiving power threshold    | -99 dBm        |
| BSMs frequency                   | 10 Hz$^{-1}$   |
| Channel frequency                | 5.9 GHz$^{-1}$ |
| Sybil attacker percentage        | 2% 6% 10%      |

BSM: Basic Safety Message; RSU: roadside unit.

**Simulation scenario and parameters setting**

In order to evaluate the timeliness of the VABV system, the simulation is built on a scenario where the RSU is located at the junction. The coverage range of the RSU is set to a circular area with a radius of 1000 meters. We refer to Wu et al.14 and get the execution time of the basic cryptographic operations shown in Table 3. As we describe in the section “Comprehensive AAT selection strategies for VABV system,” compared with RSUs, all ordinary vehicles will be classified into three categories with respect to their CPU frequency, that is, computing power. Assuming that the CPU frequency of RSU is 3 GHz, vehicles with CPU frequencies equal to, two-thirds of, and one-third of the computing power of RSU will be classified as Good, Moderate, and Bad, respectively. Therefore, in the simulated IoV, there are three kinds of ordinary vehicles with the computing power evaluated as Good, Moderate, Bad, and the computing power of them are set to 3 GHz, 2 GHz, and 1 GHz, respectively. In the IoV, 30% ordinary vehicles are with a computing power of 3 GHz, 40% of the ordinary vehicles are with a computing power of 2 GHz, and 30% of the ordinary vehicles are with a computing power of 1 GHz. The computing power of the RSU is set to 3 GHz and 2 GHz. Simulation of Urban MOBility (SUMO) simulator is used to simulate traffic flows in an urban environment for the purpose of evaluating the information security of VABV system. In the simulation scenario, each Sybil attacker generates three Sybil nodes and sends BSMs in an attempt to launch attacks based on the traffic information it knows. The remaining simulation parameters used are listed in Table 4.

**AoI performance of VABV system on timeliness**

First, we analyze the relationship between the number of AATs and the system average AoI. As we analyze in
section “Usage of AoI as the integrated indicator for VABV system,” the verification latency affects $A_t$ in AoI curve. Various distributions are simulated and we take the average verification latency as the results. In Eq. (12), the initial number of AATs $M$ is determined with the AAT selection strategy, whereby values in both directions around $M$ are taken to minimize the system average AoI (i.e. considering the total number of terminals is 200, we can calculate the initial number of AATs $M$ is 14 and take values to both sides around this number and analyze the variation of the system average AoI with the number of AATs). In Figure 8, for the different density of vehicles in simulated area, the system average AoI decreases first and then increases with the constant increase of the number of AATs. This changing trend occurs since with the assist of AATs for verification, the latency can be reduced to a certain degree as the pressure of verification is alleviated from the RSU. However, when the numbers of AATs increases continuously, the number of confirmation messages increases in each verification period, which makes the system average AoI increase accordingly. With different density of ordinary terminals simulated, we can see that the changing trends are similar. Hence, from the prospect of selection strategy on the number of AATs, we can find out the optimal number of AATs $M_{opt}$ that minimizes the system average AoI.

Then the improvement of VABV system average AoI compared to the RSU-only BSM verification system is depicted in Figure 9. The higher the percentage improvement, the better the optimization performance of VABV system. We can see from Figure 9 that comparing to the RSU-only BSM verification system, the average AoI performance of the VABV system has been improved for a certain number of terminals. However, the improvement percentage of system average AoI varies for different number of terminals. When the number of terminals is relatively small, the RSU is capable for BSM verification, thus being not put under stress for BSM verification. Consequently, the average system AoI improvement is not apparent compared to the RSU-only verification system. However, when the number of terminals is high, the average system AoI improvement becomes increasingly evident. When the total number of vehicles is 200, the maximum system average AoI improvement percentage is 47.4 % in comparison with the RSU-only verification system, showing that the VABV system has a more significant performance improvement than the RSU-only system when the number of terminals is large.

Next, the system verification latency and the data loss, both of which effect the $A_t$, are combined to assess the benefit and loss of the selection strategy from the perspective of the distribution of AATs. Figure 10 is chosen simulation results of changes in system AoI from 0 s to 10 s under different settings of distribution index $\xi$ which is described in Section “Comprehensive AAT selection strategies for VABV system.” We observe the variation of the system AoI with the AAT distribution index $\xi$ for a fixed number of terminals $N$ and number of AATs $M$. We can see from the Figure 10 the times of small-scale fluctuation in system AoI under different AAT distributions. Although a small-scale fluctuation in system AoI may not have severe consequences, a relatively small number of small-scale fluctuation can provide greater levels of BSM interaction quality for vehicle users. The times of small-scale

![Figure 8. System average AoI varies with the number of AATs when N = 50, 100, 200, respectively.](image)

![Figure 9. Average AoI improvement varies with the number of terminals in VABV system compared to the RSU-only BSM verification system.](image)
fluctuation decreases with the distribution index increases. The reason for this phenomena is that when $\xi$ is small, which means that the vehicles selected as AAT distributes in a scattered manner and the communication overlap area between them is small. In this situation, some selected AATs are far away from the RSU. The computing resources of AATs can be fully used since there is less redundant verification. However, when transmission power of some AATs is insufficient, the RSU cannot receive the confirmation message sent by them in a verification period, resulting in a need for re-verification. On the contrary, when $\xi$ is relatively high, the AATs are distributed in a concentrated manner, with the selection priority based on scoring system, it is less likely that the data loss happens since the distance from AAT to the RSU is more likely to be short, which guarantees the transmission of confirmation messages. Nevertheless, in this situation, as a large amount of computing resources of AATs are wasted, the average system AoI increases compared with the scenario with smaller $\xi$. From Figure 10, we can figure out the number of fluctuation times are 17, 16, 12, 9, and 5, respectively, while the system average AoI increases. To find the optimal AAT distribution selection strategy, we calculate the ratio of the increase in the average AoI of the system for each distribution case to the decrease in the number of small-scale fluctuations and we mark this ratio as $k$. The value $k$ for scenario $\xi = 0.2, 0.4, 0.6,$ and $0.8$ are $0.3, 0.1, 0.53,$ and $0.25$ respectively, which means that when $\xi = 0.4$, minimal AoI increase in exchange for a decrease in the number of AoI fluctuations is achieved. Under this situation, the optimal AAT selection strategy from the prospect of distribution is let $\xi$ to be 0.4 around.

**AoI performance of VABV system on information security**

In this subsection, the BSM security reflecting on AoI variation is analyzed. The attackers randomly launches a total of 100 attacks in the simulation scenario. The performance of aforementioned Sybil detection scheme is analyzed. Figure 11 is the chosen simulation results of system AoI under different Sybil percentage under the simulated scenario from 0 s to 10 s and 40 s to 50 s. In light of the analyses in section “Usage of AoI as the integrated indicator for VABV system,” the $A_i$ and $B_i$ of system AoI are related to Sybil attack and the performance of Sybil detection scheme, respectively. Large-scale fluctuations in the AoI can result in severe traffic accidents; hence, the VABV system is expected to have fewer instances of large-scale AoI fluctuation. From Figure 11, under the scenario where the total number of vehicles is 50 and the number of AATs is 8, we can see that with an increase in the number of Sybil nodes, the performance of the Sybil detection scheme improves since the fluctuation in the AoI is less frequent. However, the performance is relatively poor when the proportion of Sybil nodes is small in low traffic density scenario. This is consistent with the stated hypothesis in Li and Zhang. Since in low traffic density scenario, the average headway distance between vehicles in not tightly restricted and the mobility
patterns among them are not that similar, thus increasing the difficulty of identifying Sybil nodes. Also, the low traffic density provides malicious nodes with more options for generating virtual nodes, which reduces the accuracy for detecting Sybil BSMs.

As a way to analyze the Sybil detection scheme reflected by AoI curve, the number of peak AoI violation times under different proportions of Sybil nodes are quantitatively compared. The number of peak AoI violation times is calculated without taking into account the effects of BSM verification latency or re-verification by setting a peak AoI threshold of 400 and exceeding token of 1. When peak AoI in some verification cycles exceeds the preset threshold, the exceeding token will be set as 2. We can clearly figure out in Figure 12 the total number of peak AoI violation times under different proportions of Sybil nodes. During the operation time, with Sybil detection scheme, the

![Figure 11. AoI of VABV system with Sybil detection scheme under different Sybil percentage. (a) N = 50, M = 8, Sybil Percentage = 2%; (b) N = 50, M = 8, Sybil Percentage = 6%; (c) N = 50, M = 8, Sybil Percentage = 10%.

![Figure 12. Times of violated peak AoI of VABV system under different Sybil percentage.](image-url)
number of peak AoI violation times are 32, 23, and 14 when the proportion of Sybil nodes are 2%, 6%, and 10%, respectively. The times at which the peak AoI violation occurs decrease as the proportion of Sybil nodes increases. This implies that the proposed Sybil detection scheme performs better in scenarios with a high proportion of Sybil nodes, and that further optimization is needed to enhance the scheme’s security performance in low-Sybil proportion scenarios.

Conclusion and future work

In this article, we proposed a novel vehicle-assisted IoV in which some vehicles are assigned for BSM verification. By more comprehensive AAT selection strategy, the efficiency and VABV system can be enhanced. By using machine learning–based Sybil detection scheme, the security performance of VABV system can be further enhanced. The AoI was proposed as an indicator to evaluate the VABV system from the prospect of timeliness and information security in a unified and intuitive way. The system average AoI and peak AoI were used to synthetically evaluate the dependability of VABV system, through which optimal AAT selection strategy can be made and performance of proposed Sybil detection scheme can be intuitively tested. For future work, we will apply the proposed dependability analysis method to more complex scenarios in IoV and make modification and optimization to the Sybil detection scheme to fit proposed VABV system better.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2021RC225, in part by the National Natural Science Foundation of China under Grants 62102019 and 61931001.

ORCID iDs

Xiaoxuan Wang https://orcid.org/0000-0003-3308-0759
Qinghe Gao https://orcid.org/0000-0002-4397-9154

References

1. Contreras-Castillo J, Zeadaally S and Guerrero-Ibañez JA. Internet of vehicles: architecture, protocols, and security. IEEE Int Thing J 2018; 5(5): 3701–3709.
2. Liu J, Li Q, Cao H, et al. MDBV: monitoring data batch verification for survivability of internet of vehicles. IEEE Access 2018; 6: 50974–50983.
3. Ferng H-W, Chen J-Y, Lotfolahi M, et al. Messages classification and dynamic batch verification scheme for VANETs. IEEE Trans Mobile Comput 2021; 20(3): 1156–1172.
4. Benaisa K, Bitam S and Mellouk A. Context-based BSM aggregation for broad-scale applications in vehicular networks. In: IEEE 43rd conference on local computer networks (LCN), Chicago, IL, 1–4 October 2018, pp.360–368. New York: IEEE.
5. Qu F, Wu Z, Wang F-Y, et al. A security and privacy review of VANETs. IEEE Trans Intell Transp Syst 2015; 16(6): 2985–2996.
6. Kerrache CA, Calafate CT, Cano J-C, et al. Trust management for vehicular networks: an adversary-oriented overview. IEEE Access 2016; 4: 9293–9307.
7. Wazid M, Bagga P, Das AK, et al. AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment. IEEE Int Thing J 2019; 6(5): 8804–8817.
8. Gope P and Sikdar B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Trans Vehi Technol 2020; 69(11): 13621–13630.
9. Aman MN, Javaid U and Sikdar B. A privacy-preserving and scalable authentication protocol for the internet of vehicles. IEEE Int Thing J 2021; 8(2): 1123–1139.
10. Zhang C, Lin X, Lu R, et al. An Efficient message authentication scheme for vehicular communications. IEEE Trans Vehi Technol 2008; 57(6): 3357–3368.
11. Lo N-W and Tsai J-L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans Intell Transp Syst 2016; 17(5): 1319–1328.
12. Huang J-L, Yeh L-Y and Chien H-Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans Vehi Technol 2011; 60(1): 248–262.
13. Liu Y, Wang L and Chen H-H. Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Trans Vehi Technol 2015; 64(8): 3697–3710.
14. Wu F, Zhang X, Zhang C, et al. Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks. IEEE Int Thing J 2020; 7(9): 8144–8156.
15. Cui J, Wei L, Zhang J, et al. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 2019; 20(5): 1621–1632.
16. Sudhro AH, Rodrigues JPC, Pirbhulal S, Zahid N, et al. Link optimization in software defined IoV driven autonomous transportation system. IEEE Trans Intell Transp Syst 2021; 22(6): 3511–3520.
17. Jiang D, Wang Z, Huo L, et al. A performance measurement and analysis method for software-defined networking of IoV. IEEE Trans Intell Transp Syst 2021; 22(6): 3707–3719.
18. Duan Y, Fu G, Zhou N, et al. Everything as a service (XaaS) on the cloud: origins, current and future trends. In: *IEEE 8th international conference on cloud computing*, New York, 27 June–2 July 2015, pp.621–628. New York: IEEE.

19. Avizienis A, Laprie J-C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans Depend Secure Comput* 2004; 1(1): 11–33.

20. Junior FMR and Kamienski CA. A survey on trustworthiness for the internet of things. *IEEE Access* 2021; 9: 42493–42514.

21. Sharma P and Liu H. A machine-learning-based data-centric misbehavior detection model for internet of vehicles. *IEEE Int Thing J* 2021; 8(6): 4991–4999.

22. Khan IA, Moustafa N, Pi D, et al. An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles. *IEEE Trans Intell Transp Syst*. Epub ahead of print 20 August 2021. DOI: 10.1109/TITS.2021.3105834.

23. Gyawali S, Qian Y and Hu RQ. A privacy-preserving misbehavior detection system in vehicular communication networks. *IEEE Trans Vehi Technol* 2021; 70(6): 6147–6158.

24. Wang Q, Chen X, Jin X, et al. Enhancing trustworthiness of internet of vehicles in space-air-ground integrated networks: attestation approach. *IEEE Int Thing J* 2021; 9: 5992–6002.

25. Tangade S, Manvi SS and Lorenz P. Trust management scheme based on hybrid cryptography for secure communications in VANETs. *IEEE Trans Vehi Technol* 2020; 69(5): 5232–5243.

26. Javaid U, Aman MN and Sikdar B. A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Int Thing J* 2020; 7(12): 11815–11829.

27. Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks. *IEEE Int Thing J* 2019; 6(2): 1495–1505.

28. Wang X, Liu L, Zhu L, et al. Train-centric CBTC meets age of information in train-to-train communications. *IEEE Trans Intell Transp Syst* 2020; 21(10): 4072–4085.

29. Bansal M, Gupta S and Mathur S. Comparison of ECC and RSA algorithm with DNA encoding for IoT security. In: *6th international conference on inventive computation technologies (ICICT)*, Coimbatore, India, 20–22 January 2021, pp.1340–1343. New York: IEEE.

30. Li Y, Chen X, Yin Y, et al. SDABS: a flexible and efficient multi-authority hybrid attribute-based signature scheme in edge environment. *IEEE Trans Intell Transp Syst* 2021; 22(3): 1892–1906.

31. Pournagh SM, Zahednejad B, Bayat M, et al. NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput Netw* 2018; 134: 78–92.

32. Sun J, Chi Z, Zhang Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans Parallel Distrib Syst* 2010; 21: 1227–1239.

33. Iwendi C, Uddin M, Ansere JA, et al. On detection of Sybil attack in large-scale VANETs using spider-monkey technique. *IEEE Access* 2018; 6: 47258–47267.

34. Gu P, Khatoun R, Begriche Y, et al. Support vector machine (SVM) based Sybil attack detection in vehicular networks. In: *2017 IEEE wireless communications and networking conference (WCNC)*, San Francisco, CA, 19–22 March 2017, pp.1–6. New York: IEEE.

35. Liu M, Liu Z, Lu W, et al. Distributed few-shot learning for intelligent recognition of communication jamming. *IEEE J Select Topic Signal Process* 2021; 16: 395–405.

36. Liu M, Wang J, Zhao N, et al. Radio frequency fingerprint collaborative intelligent identification using incremental learning. *IEEE Trans Netw Sci Engi*. Epub ahead of print 10 August 2021. DOI: 10.1109/TNSEN.2021.3103805.

37. Huang G-B, Zhou H, Ding X, et al. Extreme learning machine for regression and multiclass classification. *IEEE Trans Syst Man Cybernet, Part B* 2012; 42(2): 513–529.

38. Gu P, Khatoum R, Begriche Y, et al. Vehicle driving pattern based Sybil attack detection. In: *IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPC/SmartCity/DSS)*, Sydney, NSW, Australia, 12–14 December 2016, pp.1282–1288. New York: IEEE.

39. Kaul S, Gruteser M, Rai V, et al. Minimizing age of information in vehicular networks. In: *8th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks*. In: *IEEE INFOCOM 2021—IEEE conference on computer communications*, Vancouver, BC, Canada, 10–13 May 2021, pp.1–10. New York: IEEE.

40. Choudhury B, Shah VK, Dayal A, et al. Joint age of information and self risk assessment for safer 802.11p based V2V networks. In: *IEEE INFOCOM 2021—IEEE conference on computer communications*, Vancouver, BC, Canada, 10–13 May 2021, pp.1–10. New York: IEEE.

41. How connected vehicles work, https://www.transportation.gov/research-and-technology/how-connected-vehicles-work

42. Safety band testing plans technical info, https://www.transportation.gov/research-and-technology/safety-band-testing-plans-and-technical-info

43. Li W and Zhang D. RSSI sequence | vehicle driving matrix based Sybil nodes detection in VANET. In: *IEEE 11th international conference on communication software and networks (ICCSN)*, Chongqing, China, 12–15 June 2019, pp.763–767. New York: IEEE.