Collaborative-Based Batch Verification Scheme for Event-Driven Messages in Vehicular Ad Hoc Networks

Wenqi Cao[1(✉)], Fan Wu[2], and Cong Zhang[2]

[1] China Asserts Cybersecurity Technology Co., Ltd., Beijing 100041, China
wwenqicao@163.com,wenqicao@bupt.cn
[2] School of Electrical and Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China
{wufanwww,cong1126}@bupt.edu.cn

Abstract. To ensure the information security of the Vehicle Ad hoc Networks (VANETs), it is necessary to verify the integrity and identity of safety messages transmitted in the networks. Previous safety message verification schemes mostly focus on basic security messages, which are not appropriate for emergency messages in event-driven scenarios. The generation of emergency messages in the VANETs is often sudden and massive with strict time requirements, which is a great challenge for verification terminals with the limited computation capabilities. To address these issues, a collaborative-based batch verification scheme is proposed in this paper with the goal of maximizing the number of verified safety messages in the system during some time. This solution provides three message verification strategies for the collaborative node to address verification peaks under different scales emergency message broadcasting. Performance evaluation demonstrates that compared to the RSU centralized batch verification scheme, this scheme can significantly reduce the loss rate of safety messages that fail due to untimely verification in VANETs.

Keywords: Vehicular Ad Hoc Networks · Message Batch Verification · Distributed Network

1 Introduction

Vehicle Ad hoc Networks (VANETs) is committed to improving road traffic safety, making an important role in the solution of Intelligent Transportation System (ITS) [1]. In addition, VANETs can provide various applications for road users in areas, including driving assistance and social interaction. The exchange of information among different terminals in VANETs serves as the foundation of various application services. According to the Dedicated Short Range Communication (DSRC) protocol, there are two types of security applications in VANETs: periodic messages and event-driven messages [2]. VANETs adopt periodic broadcast basic safety messages (BSMs) to transmit safety related

X. Li et al. (Eds.): SmartGift 2024, LNICST 600, pp. 125–144, 2025.
https://doi.org/10.1007/978-3-031-78806-2_8

data, such as vehicles' location, speed, direction, etc. The other refers to emergency messages (EMs) that are sent upon detection of a hazardous event, such as engine brakes or vehicle collision warning [3].

Messages in VANETs are transmitted through wireless channels, which are exposed to various attack risks, such as message replay attack, and denial-of-service attack (DoS). Furthermore, to protect the privacy of road users, information transmission in VANETs usually uses pseudonyms [4]. Consequently, it is necessary to verify the source and integrity of a message before further processing. In order to ensure secure communication, current solutions primarily employ symmetric cryptography verification schemes, asymmetric encryption-based verification schemes, and group signature-based verification schemes [5]. While these security schemes guarantee the confidentiality and integrity of messages, the message verification process relies on computationally intensive cryptographic operations, leading to additional processing delays.

In DSRC communication, vehicles driving in the system broadcast basic safety messages every 100–300 ms. Considering a VANET with about 300 vehicles, every vehicle in the system receives no fewer than 1000 basic safety messages every second [6]. Due to the high-speed movement of vehicles, if messages cannot be verified promptly, they may be discarded upon expiration, potentially resulting in accidents. Consequently, many researchers have begun to concentrate on addressing the efficiency issue of message verification.

Considering the limited computing capability of vehicles, He *et al.* [7] proposed a random verification scheme. The vehicle nodes in the system randomly select messages for verification, which can result in the loss of important safety messages. Hamida *et al.* [8] utilized distance-based multi-priority queue and K-means algorithm to classify and process received messages, using the received signal strength as the basis.

The priority-based message verification scheme may result in the loss of important security messages, leading to security risks. The message batch verification method enables the simultaneous verification of multiple safety messages, reducing the time required to verify a large number of signatures. Vijayakumar *et al.* [9] developed a batch security and key exchange scheme to reduce the burden on the verification nodes in the congested areas. Huang *et al.* [10] proposed a scheme based on anonymous batch verification, which offers a 48% reduction in verification delay compared to ordinary elliptic curve cryptosystem (ECC) method. Tzeng *et al.* [11] proposed an identity-based batch verification method using the ECC method with less communication delay and message drop rate. Chim *et al.* [12] proposed a centralized batch verification scheme, in which the roadside unit (RSU) verifies all messages sent by vehicles and then centrally publishes the verification results of each message. Vehicles in the system can query the verification results of messages through RSU after receiving them. Due to the verification of every message only once in the system, this solution can reduce redundant verification and communication delay costs. However, the centralized message verification method brings significant pressure to a single verification node as VANETs become more complex. Even when batch verification is used, it is hard to meet the requirements of secure message delay.

To address the limitation of the message verification overhead on the verification terminals, Yong *et al.* [13] developed a collaborative verification schemes, in which some assisted vehicles are selected to help RSU verify messages and share the verification results with surrounding vehicles. Hao *et al.* [14] introduced edge computing into VANETs and proposed three collaborative vehicle selection algorithms in their scheme. The results of experiments showed that this scheme significantly reduces message verification computation and communication overhead, but it does not solve the problem of message duplicate verification. Wu *et al.* [15] proposed a distributed message verification system architecture, selecting some assisted verification terminals (AVTs) to help RSU batch verify of BSMs, while avoiding redundant message verification. Simulation results show that it can significantly reduce message verification delay in dense vehicle networks. However, it is important to note that the scheme focuses only on the verification of BSMs and does not address the matter of emergency message verification.

Quick and reliable verification of emergency messages is crucial for the security of the vehicle network as timely response to emergency messages can reduce the risk of accidents. P. Kumar *et al.* [16] proposed a model of a priority-based message batch verification algorithm that prioritizes the verification of messages sent by emergency vehicles to provide response services as soon as possible. Similarly, S. Banani *et al.* [17] proposed a scheme that divides emergency message priority by region, in which vehicles determine the message priority they receive based on the distance and speed of the sending vehicle.

In conclusion, previous research has demonstrated the efficacy of message batch verification and collaborative distributed network structures in enhancing verification efficiency. On top of this, this paper focuses on event-driven scenarios in VANETs, we propose an efficient collaborative-based batch verification scheme for surged emergency message in VANETs. The contributions of this paper are as follows:

(1) Three verification strategies are designed to adapt to occasional verification peaks under different emergency messages quantity scales, aiming to maximize the number of secure messages verified within a unit of time.
(2) Because emergency messages arrive following a Poisson distribution, the uncertainty in their arrival makes it challenging to establish a precise delay model. In this scheme, we utilize queuing theory as the analytical foundation to model the verification delay and apply this model to the emergency message verification scheme.

The rest of this paper is organized as follows. Section 2 introduces safety-related applications in VANETs, Sect. 3 presents system architecture and message verification process. Section 4 discusses the verification scheme for emergency messages. Section 5 discusses performance analysis of the proposed scheme. Section 6 concludes the paper.

2 Preliminaries

2.1 Safety Applications in VANETs

The safety applications in VANETs can be divided into periodic safety applications and event-driven applications. Based on this, there are two driving modes for vehicles in the VANETs [18]:

(1) Normal mode: In the system where no accidents have occurred, all vehicles are in normal state and exchange safety information periodically through BSMs.
(2) Warning mode: When a vehicle notice an accident situation, it immediately transitions to warning state and broadcast event-driven emergency messages to remind all vehicles exposed to potential danger in the relevant area, which is called the Zone of Relevance (ZoR). Vehicles in other areas of the VANET continue to drive normally without being affected. The generation of EMs is often abrupt and may lead to an exponential growth of messages within the relevant area.

2.2 Message Batch Verification Basics

A typical VANET system is mainly composed of vehicles, a trust authority (TA) and a roadside unit (RSU). Among them, TA is the completely trusted service organization, responsible for generating and publishing security parameters of the VANET. RSU is the main verification center for messages in the system. Vehicles in VANET are equipped with On-board units (OBUs) for direct communication with adjacent vehicles or RSUs. Usually, the communication radius of the RSU is 1Km, and the communication range between vehicles is 300 m. The definitions of symbols used in this article are shown in Table 1.

The message batch verification method is based on the ECC encryption algorithm. The generation and verification process of message packets is briefly described as follows: TA publishes system security parameters during initialization. When a vehicle joins VANETs, the tamper-resistant unit(TPD) of the vehicle loads system parameters from TA. The vehicle first calculates a pseudonym AID_i, then the TPD signs the message M_i and timestamp T_i, and the result is σ_i. The vehicle finally broadcasts the secure message package$\{AID_i, M_i, T_i, \sigma_i\}$. All receiver terminals in the system need to verify the signature upon receiving a safety message. The verification formula for a single message is as follows:

$$\sigma_i P = h(AID_i)P_{pub} + h(M_i||T_i)AID_{i,1} \tag{1}$$

By aggregating messages and performing batch verification, a verification node can reduce the number of computation operations and thus decreases the verification delay. For n_i message packages, the node selects a random factor v_i, then multiplies the signature σ_i with v_i and combine it with the parameters

Table 1. Symbol Definition

Symbol	Defination
$h(.)$	Hash equation for encryption
BSM	Basic safety message
EM	Emergency message
RSU	Roadside Unit
TA	Trust Authority
ZOR	Zone of Relevance
VE	Vehicles of normal state in the system
CM	Vehicles of warning state in relevant area
CV	Collaborative Vehicle
CH	Collaborative Vehicle in warning state
t_{pro}^{j}	The process delay on CV_j
t_{comp}^{r}	The computational batch-verification delay at the RSU
T_{tran}^{c}	The transmission delay of the message confirmed packets sent by the CH to RSU
T_B	The period of vehicle broadcast BSM
T_M	The period of vehicle broadcast EM
T_k	The delay tolerance of the safety message
t_R	The period of RSU aggregated-bath verification
t_c	The period of aggregated-bath verification at the CH node
λ_n	The arrival rate of EMs in the system
λ_c	The arrival rate of EMs at the CH node
λ_r	The arrival rate of EMs at the RSU
γ_c	The discount factor of computing power between the CH and RSU
μ_0	The verification efficiency of a single EM at the CH node
n_b	The number of ordinary vehicles verified by the RSU
n_c	The number of collaborative vehicles in the system
n_{tol}	The total number of verified messages in the system over a period of time
N_r	The number of messages accumulated on the RSU during a period
N_b^r	The number of accumulated BSMs at the RSU during a period
N_c^r	The number of message confirmed packets sent by CVs during a period
N_m^r	The number of EM confirmed packets sent by the CH node during a period
r	The number of EMs verified in each batch
δ	The EM reassigned-verification ratio

published by TA to verify whether the message signature has been tampered with. The verification formula is as follows:

$$(\sum_{i=1}^{n_i}(v_i s_i))P = (\sum_{i=1}^{n_i} v_i h(AID_i))\sum_{i=1}^{n_i} v_i h(M_i||T_i)AID_{i,1} \tag{2}$$

To further quantify the delay overhead of verification, the computational costs of encryption operations in ECC can be obtained by referring typical papers [19]. Let the computational overhead of small factor dot product operation, the dot product calculation, the addition operation and hash operation in the message verification Formula (1) be denoted as $T_{ecc-m}, T_{ecc-sm}, T_{ecc-pa}$, and T_h, respectively. The computational overhead for a single message verification

can be obtained as follows:

$$t_e = 2T_h + 3T_{ecc} + T_{sm} \tag{3}$$

To simplify the calculation, let $T_{ecc-m} = T_{ecc-m} + T_{ecc-sm} + T_{ecc-pa} + 2T_h$, and $T_{sm} = 2T_{ecc-m}$. According to Formula (2), the computation overhead for batch verification of n messages is shown as follows:

$$t_{comp} = nT_{ecc} + T_{sm} \tag{4}$$

3 Overview

3.1 System Framework of VANETs in Safe Scenarios

The distributed message batch-assisted verification system architecture used in this paper is slightly different from the regular system. In a safe scenario, all vehicles drive in the normal state, and the batch-assisted verification scheme determine the list of collaborative verification vehicles (CVs) with strong computational capabilities to help verify basic safety messages (BSMs) [15]. Every selected collaborative vehicle (CV) is responsible for verifying the messages from vehicles (VEs) within its communication range. Due to the limitation of vehicle communication range, for ordinary vehicles not assigned to CVs, their messages are batch-verified by the RSU. The message verification process is shown in Fig. 1. First, the VEs send BSMs to the CVs. The CVs first batch-verify the messages and then report the message verified confirmation packets to the RSU. The RSU first verifies BSMs from the VEs and then performs the final verification of the message confirmation packets.

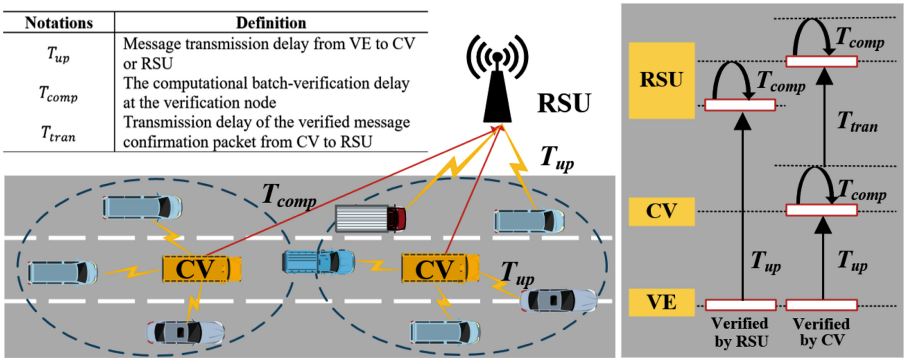

Fig. 1. The process of Message verification

3.2 Message Batch Verification Delay Basics

Message Batch Verification Delay of the Cooperative Vehicle. Assuming the cooperative Vehicle CV_j is responsible for the messages verification of n_j vehicles in the system. First, CV_j batch verifies n_j messages broadcasted by vehicles. Then, CV_j aggregates the authenticated messages pseudonym (AID) and sends it as a confirmed packet to the RSU. Therefore, the process delay t^j_{pro} on CV_j can be calculated as follows:

$$t^j_{pro} = T_{up} + t^j_{comp} + T^j_{tran} \tag{5}$$

To simplify the complexity of the model, the transmission delay of messages to verification nodes is uniformly denoted as T_{up}. Assuming the computing power of RSU is f_r and the computing power of the OBU on CV_j is f_j. Let $\gamma_j = f_j/f_r$. From Formula (4), the computational delay on CV_j for batch-verification is $t^j_{comp} = \gamma_j(n_j T_{ecc} + T_{sm})$. And T^j_{tran} is the transmission delay of the verified messages confirmed packet from CV_j to RSU. For the confirmed packet, the data length of AID is $l_{aid}n_j$, and the length of fixed data is l_0. Assuming the transmission rate of data in the system is donated to B, T^j_{tran} can be calculated as follows:

$$T^j_{tran} = l_{aid}n_j/B + l_0/B \tag{6}$$

Message Batch Verification Delay of RSU. Assuming RSU is responsible for the safety messages verification of n_b vehicles in the system. RSU first batch verifies the safety messages from normal vehicles, and then confirms the verified message packets sent by the CV nodes, which are also verified in batch. For n message packages, the computational delay of batch-verification on the RSU is as follows:

$$t^r_{comp} = T_{ecc}n + T_{sm} \tag{7}$$

3.3 System Framework

In this paper, we consider a densely populated VANETs scenario as shown in the Fig. 2. When a vehicle CM encounters an accident, it immediately switches to warning mode and reminds all other vehicles CMs within the relevant area L_m, triggering them to warning mode and broadcasting emergency messages (EMs) intensively for some time. Normal driving of vehicles in other areas of the system will not be affected. The explosive growth of EM scale can lead to excessive verification delay on the collaborative vehicle (CH) in the relevant area. If selection algorithm for assisted verification terminals is performed in such cases, it would result in additional communication overhead and computational delay for the system. As a result, it is necessary to propose a rapid and dependable emergency message verification solution to the node CH, without adversely affecting the message verification processes of other normal vehicles in the system.

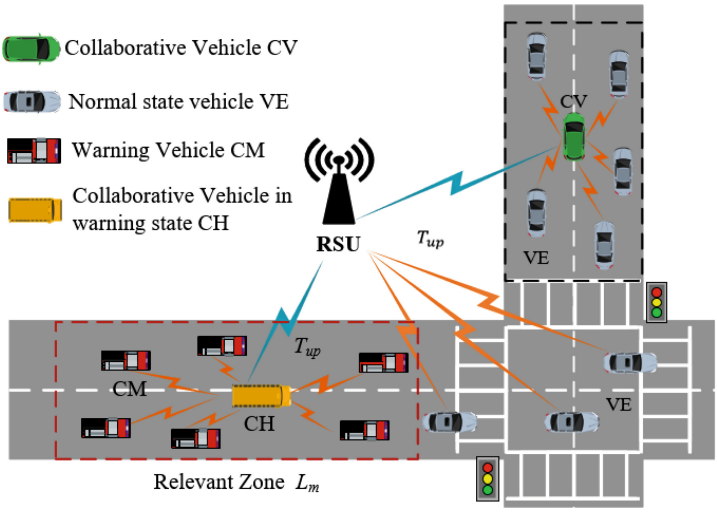

Fig. 2. Emergency messages broadcast scenario of VANETs

4 Collaborative-Based Emergency Message Batch Verification Scheme

The broadcasting frequency of different types of emergency messages varies from 1 Hz to 10 Hz, resulting in varying sizes of message quantities. Our scheme adopts different verification strategies to ensure the success rate of secure message verification in the system. For the batch-verification method, verification nodes first store the secure messages received during the verification period in the message queue, and then the accumulated messages are batch verified at the end of period. Due to the uncertainty of the accident, this scheme constructs different message queuing models on the node CH under different strategies to characterize the average verification delay of EMs. Based on the cooperative message batch verification process, the aggregated verified period on the node CH is derived, which maximizes the number of verified secure messages in the system within a certain period of time, thus reducing the loss rate of message verification in the system.

4.1 Emergency Message Arriving Model

Due to the dense broadcast frequency of emergency messages and the high-speed mobility of vehicles, it is difficult to achieve clock synchronization in the system. The arrival of EMs at the verification terminal can be considered as an asynchronous periodic message stacking process [20], which is usually approximated as a Poisson distribution process [21].

Assuming that there are n warning mode vehicles broadcasting emergency messages in the system, with a broadcasting period of T_M, the arrival rate λ_n

of EM in the system is as follows:

$$\lambda_n = \frac{n}{T_M} \tag{8}$$

Due to the uncertainty of the Poisson distribution, it is difficult to quantify the waiting time of EMs during the aggregation process. Therefore, this paper utilizes queuing theory to the analysis of the EM batch verification process. By optimizing the performance metrics of the queuing system, the verification efficiency of EM can be improved.

4.2 Emergency Messages Single-Verified Strategy on the Collaborative Node

If the EMs are broadcasted at low frequency, it is likely to spend a lot of time waiting for batch-verification. In this case, single sequential by CH node can improve the efficiency of EM verification.

Emergency Messages Single-Verified Queuing Model. For the CH node, the arrival process of EMs follows a Poisson distribution, and the computation time for a single message verification t_e from Formula (3) is fixed. Thus an M/D/1 queuing model can describe the single message verification process of EM on the CH node. In this case, the EM arrival rate on the CH node λ_c is equal to the EM arrival rate in the system, i.e. $\lambda_c = \lambda_n$. The single EM verification rate is $\mu_0 = 1/t_e$. According to the M/D/1 queuing system, the average residence time w_0 of a single EM can be obtained, which is the time from arrival at the CH to departure from the CH node:

$$w_0 = \frac{2\mu_0 - \lambda_c}{2\mu_0(\mu_0 - \lambda_c)} \tag{9}$$

Since the CH node must transmit the verified packets to the RSU for final confirmation, the total verification delay of a single EM on the CH is $t_0^c = w_0 + T_{tran}^c$. Among them, T_{tran}^c is the transmission delay of CH sending packets to RSU, which is $T_{tran}^c = T_{aid} + T_l$.

Emergency Messages Sequential Single-Verified Strategy on the CH Node. In this strategy, the RSU requires a verification period t_R. All the safety messages arriving during a period of t_R are first stored in the message queue, and then the accumulated messages are verified in batch at the end of the period of t_R. The verification tasks of the RSU include n_b BSMs from regular vehicles, the message confirmed packets sent by n_c collaborative vehicles (CVs) and the EM confirmed packets sent by the CH node.

It is assumed that there are n_b vehicles broadcasting BSMs verified by RSU with period of T_B. During a period of t_R, the number of accumulated BSMs at the RSU is denoted as $N_b^r = n_b t_R / T_B$, and the number of message confirmed packets sent by n_c CVs is denoted as $N_c^r = n_c t_R / T_0$. Also, the number of EM

confirmed packets sent by the CH node is denoted as $N_m^r = t_R/t_0^c$. Thus, the number of messages accumulated on the RSU during a verification period is $N_r = N_b^r + N_c^r + N_m^r$.

The computational batch-verification delay during a verification period at the RSU can be obtained from Formula (4), where $t_{comp}^r = T_{ecc}N_r + T_{sm}$. In order to improve the efficiency of message verification in the system within a fixed period of time, let Δt represent a longer period of time, during which the number of messages verified at the RSU is as follows:

$$n_{tol} = \frac{\Delta t N_r}{t_R + t_{comp}^r} \tag{10}$$

For an emergency message, the longest delay from generation to completion of verification includes the transmission delay to the CH node T_{up}, the total verification delay at the CH node T_0^c and the batch verification delay at the RSU T_r. The sum of these delays shall not exceed the delay tolerance of the safety message T_k, which is as follows:

$$T_{up} + T_0^c + T_r \leq T_k \tag{11}$$

From the stability requirements of the EM queue on CH, it can be concluded that:

$$\frac{\lambda_n}{\mu_0} < 1 \tag{12}$$

In addition, the verification period t_R needs to be greater than 0, which is as follows:

$$t_R > 0 \tag{13}$$

This strategy modifies the verification period t_R of the RSU based on the actual arrival rate of EMs in the system. The goal is to ensure timely verification of EMs and to maximize the number of verified messages in system over a period of time. The optimization objective function is as follows:

$$max\, n_{tol} = \frac{\Delta t N_r}{t_R + t_{comp}^r} \tag{14}$$

And the objective function is constrained by Formulas (11)–(13).

4.3 Emergency Messages Batch-Verification Strategy on the Collaborative Node

If the arrival rate of EMs in the system λ_n is greater than the verification efficiency at the CH node μ_0, that is, $\lambda_n > \mu_0$, single sequential verification cannot guarantee the stability of the EM queue. To speed up the verification efficiency of EM, the CH node adopts a message batch-verification method. In this case, the CH node needs to set the aggregated-bath verification period t_c for EMs. During the period, the incoming EMs are first queuing in the message queue. At

the end of the period the r EMs aggregates accumulated during the period are batch-verified.

Due to the random character of the arrival of EMs at the CH node which makes it difficult to quantify the waiting time, a queuing model can help solve the problem to quantify the batch-verification delay. The total number of verified messages in the system per unit of time can be optimized by determining the period of t_c.

Emergency Message Aggregated-Batch Verification Queuing Model. For the CH node, the aggregated-bath verification period t_c is equivalent to the sum of the average residence time of the EMs at the CH node w_c, and the transmission delay of the message confirmed packets to the RSU. In order to specifically describe the verification delay of EMs, we establishes a queuing model for the message queue on the CH node, and transforms the period t_c into solving the residence time w_c of EMs in the queuing model.

According to Formula (4), the computation overhead for batch verification of x messages on the CH node is donated as $t^c_{comp}(x) = \gamma_c(T_{ecc}x + T_{sm})$, where the γ_c is the discount factor of computing power between the CH and RSU. According to the queuing theory, the average verification rate of EMs at CH node is $\mu_c = 1/(\gamma_c T_{ecc})$. Since the arrival process of EMs at the CH node follows a Poisson distribution with λ_n, and the verification rate μ_c is fixed, the verification process of EMs at the CH node can be modeled as an $M/D^r/1$ queuing system, where r is the number of EMs verified in a single batch.

Emergency Message Aggregated-Batch Verification. The method of establishing an embedded Markov chain is a common approach in queuing theory. In this case, we derive the stationary distribution of the embedded process to obtain the steady-state distribution of message queue length, which make it possible to analyze the batch-verification problem of EMs on the CH node in a more specific manner. Let x_n represent the number of queued EMs at the CH node when the verification of the EMs in the n_{th} batch is completed, $\{x_n, n \geq 0\}$ forms a Markov chain [22]. In order to maintain the stability of the queuing system, the average number of messages received on the CH node during message verification for each batch $\lambda_c d_{(r)}$ should be less than the number of EMs verified in each batch, denoted as r. Therefore, the condition for message queue stability is $\lambda_c d_{(r)} < r$, which is organized as follows:

$$r > \frac{\lambda_c \gamma_c T_{sm}}{1 - \lambda_c \gamma_c T_{ecc}} \tag{15}$$

Figure 3 illustrates the state transition process of the Markov chain x_n. The stationary distribution π_j is defined as $\pi_j = \lim_{n\to\infty} P(x_n = j)\, j = 0, 1, 2...$, subject to the constraint $\sum_{i=0}^{\infty} \pi_j = 1$.

The common method for solving the steady-state distribution of a system is to introduce the generation function $X(z)$ of the queue length to solve. The average queue length $E[x]$ at the steady-state can be obtained by differentiating $X(z)$ with respect to z at $z = 1$ [22]. According to Little's law, we can obtain

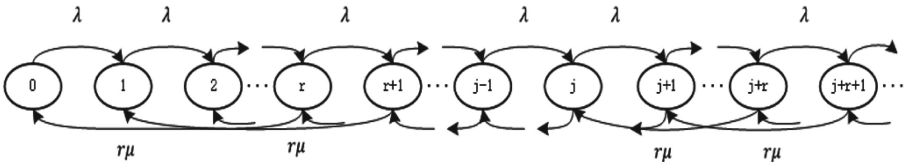

Fig. 3. Markov chain $\{x_n\}$ state transition process

the average residence time w_c of any EM in the n_{th} batch at the CH node, which is the sum of waiting delay and computational verification delay of a EM at the CH node. The average residence time $w_c = E[x]/\lambda_c$.

The aggregated-batch verification period of an EM at the CH node is denoted as t_c, which is composed of the average residence time of the EM w_s, and the transmission delay of the message confirmed packets sent by the CH T^c_{tran}. And t_c can be calculated as follows:

$$t_c = w_s + T_{aid}r = \frac{\gamma_c(T_{ecc} + T_{sm}) - \lambda_c\gamma_c^2 T_{ecc}T_{sm} + r\gamma_c T_{ecc}(1 - \lambda_c\gamma_c T_{ecc})}{2(1 - \lambda_c\gamma_c T_{ecc})} + \frac{\frac{\gamma_c T_{sm}}{2(1-\lambda_c\gamma_c T_{ecc})^2}}{r - \lambda_c\gamma_c T_{sm}/(1 - \lambda_c\gamma_c T_{ecc})} + \frac{1}{\lambda_c}\sum_{n=1}^{r-1}\frac{1}{1-\delta_n} + T_{aid}r \tag{16}$$

According to the Rouche's theorem [23], δ_n represent the roots of the characteristic equation. By analyzing Formula (16), it can be seen that for a CH node with a given EM arrival rate λ_c, the size of the aggregation batch-verification period t_c node is determined by the number of EMs per batch verification r.

Emergency Message Aggregated-Batch Verification Strategy. In this strategy, the CH node first aggregates and verifies r EMs in batch, and then the CH node sends the confirmed package to the RSU. To ensure that EMs can be verified in time, after receiving the EM confirmed package, the RSU immediately batch verifies the accumulated messages within an aggregated-bath verification period t_c.

In this system, the verification tasks on the RSU includes verifying BSMs with the broadcasting period of T_B from n_b ordinary vehicles, and the confirmed message packages sent by n_c CV nodes. During an aggregated-bath verification period t_c, the number of BSMs accumulated on the RSU is donated as $N_b^r = n_b t_c/T_B$, and the number of message confirmed packets sent by n_c CVs is denoted as $N_c^r = n_c t_c/T_B$. In addition, there is a EM confirmed packet sent by the CH node. Thus, the number of messages accumulated within a period of t_c is donated as:

$$N_r = N_b^r + N_c^r + 1 \tag{17}$$

The computational batch-verification delay during a period of t_c at the RSU is donated as t^r_{comp}, $t^r_{comp} = T_{ecc}N_r + T_{sm}$. During the time period $\Delta t (\Delta t >> T_B)$, the total number of verified messages in the system n_{tol}, includes the sum

of the messages verified by RSU, collaborative nodes and CH node, which can be represented as follows:

$$n_{tol} = \frac{\Delta t}{t_c + t_{comp}^r} N_r + \frac{\Delta t}{T_B} \sum_{j=1}^{n_c} \frac{\Delta t}{T_B} n_j + \frac{\Delta t}{t_{comp}^r} r \tag{18}$$

The sum of all the delays shall not exceed the delay tolerance of the safety message T_k, which is as follows:

$$T_{up} + t_c + t_{comp}^r \leq T_k \tag{19}$$

The condition for message queue stability is organized as follows:

$$r > \frac{\lambda_c \gamma_c T_{sm}}{1 - \lambda_c \gamma_c T_{ecc}} \tag{20}$$

In addition, the period of t_c should be greater than 0, which is as follows:

$$t_c > 0 \tag{21}$$

In this scheme, it is necessary to determine the aggregated-bath verification period t_c of CH node, with the goal of maximizing the total number of verified messages in the system per unit time. The optimization objective is as follows, constrained by Formulas (19)–(21):

$$max\, n_{tol} \tag{22}$$

4.4 Emergency Messages Reassigned-Verification Strategy

When the broadcast scale of EM messages is large, the number of messages in the system that fail due to untimely verification increases. Due to the limited computing power of the CH node, the aggregated-bath verification strategy still cannot meet the time requirements of large-scale EM verification. At this time, re-election to add collaborative verification nodes will cause the change of network topology, resulting in extra computational and communication delay overhead. Therefore, in order to ensure the message verified in time, this strategy reassigns the EMs verification tasks of warning vehicle CMs which were responsible by the CH node, to both RSU and the CH node. This strategy aims to maximize the number of verified safety messages in the system while ensuring timely message verification.

In this strategy, the CH node still adopts the method of batch-verification for EMs, and the CH node aggregated-bath verification period t_c can be obtained from Formula (16). For the RSU, in order to ensure the timely verification of EMs, upon receiving the message confirmation packet reported by the CH node, the RSU immediately batch verify on the accumulated messages in its message queue over that period of time.

Assuming that the number of warning vehicles (CMs) verified by the CH node is n_c^m, then the arrival rate of the CH node can be obtained as $\lambda_c =$

n_c^m/T_M, where the T_M is the EM broadcasting period. Let the number of warning vehicles(CMs) verified by the RSU be n_r^m, then the arrival rate of EM at the RSU is $\lambda_r = n_r^m/T_M$. Define the EM reassignment ratio as δ, where $\delta = \lambda_c/\lambda_n$, and λ_n is the arrival rate of EMs in the system.

For the RSU, during an aggregated-bath verification period t_c, the number of BSMs accumulated on the RSU is donated as $N_b^r = n_b t_c/T_B$, and the number of message confirmed packets sent by n_c CVs is denoted as $N_c^r = n_c t_c/T_B$. In addition, the number of EMs sent by the CMs can be calculated as $N_m^r = n_r^m t_c/T_M$. Thus, the number of messages accumulated on the RSU within a period of t_c is donated as:

$$N_r = \frac{n_b t_c}{T_B} + \frac{n_c t_c}{T_B} + \frac{n_r^m t_c}{T_M} \tag{23}$$

The verification delay at the RSU is donated as t_{comp}^r, $t_{comp}^r = T_{ecc} N_r + T_{sm}$. Our goal is to maximize the total number of verified messages in the system during the time period $\Delta t (\Delta t >> T_B)$, which can be represented as follows:

$$max\, n_{tol} = \frac{\Delta t}{t_c + t_{comp}^r} N_r + \frac{\Delta t}{T_B} \sum_{j=1}^{n_c} \frac{\Delta t}{T_B} n_j + \frac{\Delta t}{t_{comp}^r} r \tag{24}$$

The constraints of the total arrival rate of EMs in the system λ_n is given by:

$$\lambda_n = \lambda_c + \lambda_r \tag{25}$$

The sum of all the delays shall not exceed the delay tolerance of the safety message T_k, which is as follows:

$$T_{up} + t_c + t_{comp}^r \leq T_k \tag{26}$$

According to formula (20), the condition for message queue stability is organized as follows:

$$r > \frac{\lambda_c \gamma_c T_{sm}}{1 - \lambda_c \gamma_c T_{ecc}} \tag{27}$$

In addition, the period of t_c should be greater than 0, which is as follows:

$$t_c > 0 \tag{28}$$

In this case, our optimization goal is constrained by Formulas (25)–(28). We need to determine the aggregated-bath verification period t_c of CH node and the EMs reassigned-verification ratio δ.

4.5 Emergency Message Verification Algorithm

For EM verification schemes, different strategies need to be adopted based on different emergency message arrival rates. The following pseudocode describes the specific algorithm.

Algorithm 1. Emergency Messages Verification Algorithm

Input: The total number of vehicles in the system N, the broadcasting frequency of EM f, and the number vehicles in warning state n.

Output: The total number of verified messages in the system over a period of time n_{tol} and the loss of the verification safety messages in the system α.

System Initialization: Determine the number of collaborative vehicles and the CV_lists.

Stage1: Emergency Messages Sequential Single-verified Strategy

if $\lambda_n < \mu_0$ **then**
  Calculate w_0; // Calculating the Single-verified
  $max\ n_{tol} \leftarrow t_c$;
end if

Stage2: Emergency Messages Batch-Verification Strategy

if then$\alpha > 0.15$
  for $r = 1 : n$ **do**
    for $i = 1 : (r - 1)$ **do**
      Calculate δ_i; // Calculating the roots of the characteristic equation
    end for
    Calculate t_c; // Calculate the period of aggregated-bath verification
    Calculate $N_{tol} \leftarrow t_c$;
  end for
end if
$max\ n_{tol} \leftarrow t_c$;
Observing the effect of system safety message loss rate α

Stage3 Emergency Messages Reassigned-Verification Strategy

if $\alpha > 0.15$ **then**;
  for $\lambda_m = 1 : \lambda_n$ **do**;
    for $r = 1 : n$ **do**;
      Calculate $t^r_{m,s} \leftarrow \delta_i$; // Calculate the period of aggregated-bath
    end for
    Calculate $maxN^{\lambda_m}_{tol} \leftarrow t_c$;
  end for
  $max\ N_{tol} \leftarrow \lambda_m$;
end if

5 Performance

In order to analyze the performance of proposed scheme, we use SUMO (Simulation of Urban Mobility) to simulate a traffic heavy VANET scenario. The simulation area is set to a vertical intersection of 2000 m × 2000 m. The wireless communication protocol IEEE 802.11p provides a transmission rate of 12 Mbit/s in the VANETs. Besides, we use the SUMO Traffic Control Interface (TracI) in Python to achieve the interaction and acquisition of vehicle status and data information in the running traffic simulation environment.

Firstly, in a secure system scenario, the list of assisted vehicles can be determined according to batch-assisted verification scheme [15]. Based on this, we evaluate our proposed scheme in an event-driven scenario. The communication

Table 2. Caption

Parameters	Description	Value
N	The number of vehicles in the system	300
n	The number of vehicles of warning state in relevant area	30
λ_n	The arrival rate of EMs in the system (message/ms)	[0.15, 2.7]
n_b	The number of ordinary vehicles verified by the RSU	19
n_c	The number of collaborative vehicles in the system	14
T_k	The delay tolerance of the safety message	100 ms
f_r	The computing power of the RSU	2–3 GHz
f_c	The computing power of the OBU	1.3–1.5 GHz
B	Transmission rate in VANET	12 Mbit/s
l_{BSM}	The length of basic safety message packet	184 bytes
$l_R(n)$	The length of verified comfirmation packets of n messages	$60n$+84 bytes

radius of RSU and Vehicles are set to 1 km and 300 m respectively. The broadcast frequency of different types of EMs is generally between 1 Hz and 10 Hz, and for other vehicles in normal state in the system, they broadcast BSMs at the period of 100ms. The execution time of basic encryption operations can be obtained from MIRACL library [24]. T_{ecc}, $T_{ecc\_sm\_s}$, T_{ecc_pa}, and T_h, are 0.42, 0.0138, 0.0018 and 0.0001 ms, respectively. All the relevant parameters are shown in the Table 2 below.

In this section, we define the total loss rate of safety messages is the ratio of the number of safety messages that fail to be verified within their delay tolerance to the number of safety messages generated in the system. Here, we evaluate the performance of the proposed schemes EM single-verified strategy (CH-SV), EM aggregated-batch verification strategy (CH-ABV) and EM reassigned-verification strategy (CH-RV), and compare them with the traditional scheme, which is the RSU centralized batch-verification algorithm (RCBV). The RCBV scheme centrally verifies all the security messages in the system at the RSU. This scheme aims to maximize the number of verified messages per unit time by establishing a $M/D^r/1$ queuing model.

Figure 4 (a) shows the total loss rate of system safety messages as the arrival rate of EMs in the system λ_m changes under CH-SV strategy, CH-ABV strategy, CH-RV strategy and RCBV strategy. From the figure, it can be seen that the message loss rate of the RCBV algorithm is always around 30%. When λ_m is between [0.1,0.3], the CH-SV strategy results in the lowest total loss rate of messages, which is basically zero, while the other three strategies, due to batch verification, result in long waiting delay for EMs. When λ_m is between [0.15, 0.75], adopting the CH-ABV strategy can ensure that the total loss rate of system security messages is controlled below 15%. When λ_m is greater than 1.05, the safety message loss rate of the CH-ABV strategy is much smaller than that of the CH-ABV strategy due to the limitation of the computing power on

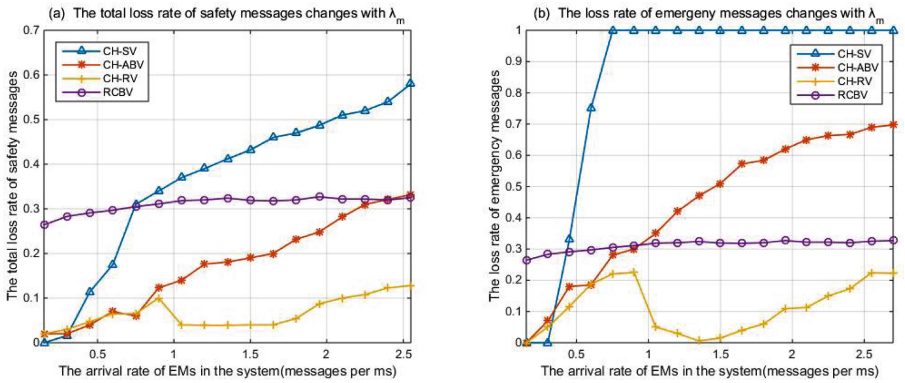

Fig. 4. The loss rate of messages changes with the arrival rate of emergency messages in the system

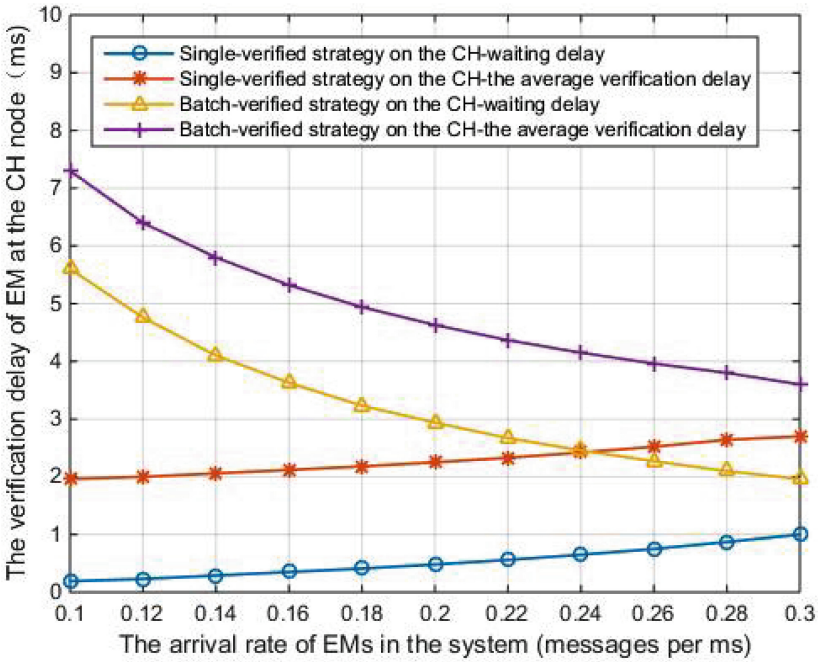

Fig. 5. The verification delay of the emergency messages at the CH node changes with the arrival rate of emergency messages in the system

the CH node. Even if the arrival rate of EMs in the system is 2.7 messages per ms, which corresponds to the maximum broadcast frequency of EMs at 10 Hz, the message loss rate of the RABV strategy can be kept within 15%. The system can choose an appropriate scheme based on the different sizes of EMs to reduce the total loss rate of system safety messages.

Figure 4 (b) shows the loss rate of EMs as the arrival rate of EMs in the system λ_m changes under four strategies. The trend of the loss rate of EMs under four strategies is similar to that of the total loss rate of safety messages in the system. The CH-SV strategy can ensure that the loss rate of EMs in the system is basically 0 when λ_m is between [0,0.3], which is much less than the other three strategies. Due to the limitation of the computing power of the CH node, when the EM arrival rate increases, the CH-ABV strategy has a significant advantage in EM loss rate among the four strategies.

According to Fig. 4 , when the EM arrival rate is less than 0.3, the EM single-verified strategy on the CH node is adopted to decrease verification delay. Figure 5 shows the average waiting time and average verification time for EMs under the EM single-verified strategy and batch-verified strategy on the CH node within the [0.1,0.3] range of EMs arrival rates of the system. When the arrival rate of the system is less than 0.3, batch verification would require some time for message aggregation, causing an increase in the waiting and verification delay. When a CH node adopts EM single-verified strategy, its verification process corresponds to a $M/D/1$ queuing system, and the average verification time of EMs increases with the arrival rate. When CH nodes adopt batch verification strategy, their verification process corresponds to a $M/D^r/1$ queuing system. The

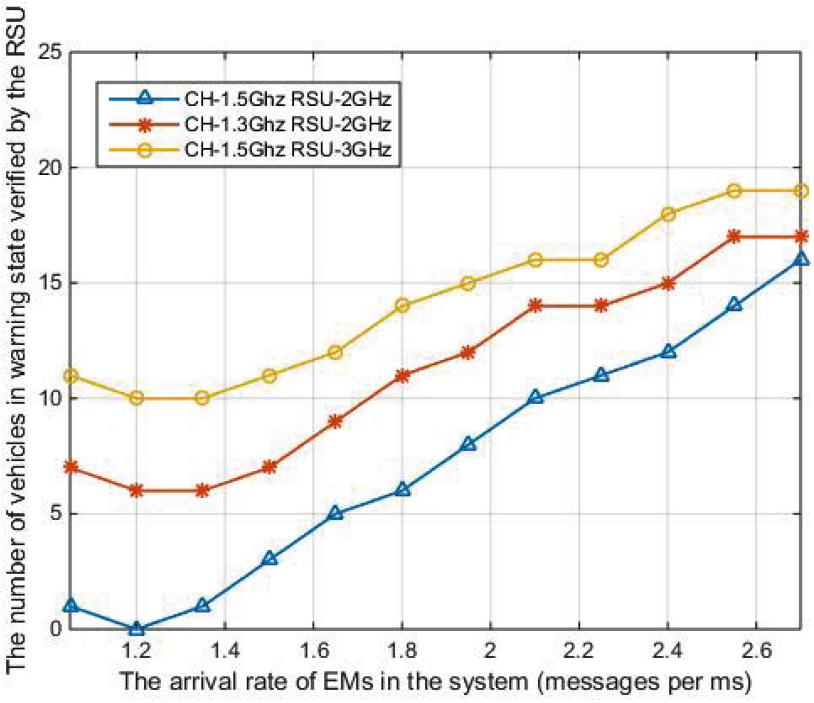

Fig. 6. The number of warning vehicles verified by the RSU under different computing power of RSU and CH node

waiting delay and average verification delay of EMs decrease with the increase of message arrival rate. Therefore, adopting batch verification strategy is more effective when the arrival rate is high.

When the arrival rate of EMs is greater 1.05 messages per ms, the system adopts the CH-ABV strategy. Figure 6 shows the relationship between the number of warning vehicles (CM) verified by the RSU and the EMs arrival rate under the CH-ABV strategy with different computing power of RSU and the CH vehicle. It can be seen that the CH-ABV strategy tends to assign more EMs to the RSU to be verified. This strategy optimizes the success rate of safety message verification by adjusting the allocation ratio of EM verification tasks between the RSU and CH nodes at different EM broadcast frequencies.

6 Conclusion

This paper is based on the system structure of collaborative distributed message batch verification. It considers the scenario of accidents in VANETs and addresses the situation where there is a surge of emergency messages in a specific area due to sudden accidents. It proposes a message collaborative verification scheme to ensure timely verification of all safety messages in the system.

Simulation results demonstrate that compared to the RSU centralized batch verification scheme, this scheme can significantly reduce the loss rate of safety messages in the system caused by untimely verification under different message scales.

Acknowledgements. This work is supported by the National Natural Science Foundation of China under Grant 62301078 and the China Postdoctoral Science Foundation under Grant Number GZB20230086.

References

1. Mchergui, A., Moulahi, T., Zeadally, S.: Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (Vanets). Vehicul. Commun. **34**, 100403 (2022)
2. St. Amour, B., Jaekel, A.: Data rate selection strategies for periodic transmission of safety messages in Vanet. Electronics **12**(18) (2023)
3. Zhou, H., Shouzhi, X., Ren, D., Huang, C., Zhang, H.: Analysis of event-driven warning message propagation in vehicular ad hoc networks. Ad Hoc Netw. **55**, 87–96 (2017)
4. Jan, S.A., Amin, N.U., Othman, M., Ali, M., Umar, A.I., Basir, A.: A survey on privacy-preserving authentication schemes in Vanets: attacks, challenges and open issues. IEEE Access **9**, 153701–153726 (2021)
5. Al-Shareeda, M.A., Anbar, M., Hasbullah, I.H., Manickam, S.: Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sens. J. **21**(2), 2422–2433 (2021)
6. Jiangwei, X., Wang, L., Wen, M., Yu, L., Chen, K.: DPB-MA: low-latency message authentication scheme based on distributed verification and priority in vehicular ad hoc network. IEEE Trans. Veh. Technol. **72**(4), 5152–5166 (2023)

7. He, D., Zeadally, S., Baowen, X., Huang, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**(12), 2681–2691 (2015)
8. Ben Hamida, E., Javed, M.A.: Channel-aware ECDSA signature verification of basic safety messages with k-means clustering in Vanets. In: 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), pp. 603–610 (2016)
9. Vijayakumar, P., Azees, M., Kozlov, S.A., Rodrigues, J.J.P.C.: An anonymous batch authentication and key exchange protocols for 6g enabled Vanets. IEEE Trans. Intell. Transp. Syst. **23**(2), 1630–1638 (2022)
10. Huang, J.-L., Yeh, L.-Y., Chien, H.-Y.: Abaka: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **60**(1), 248–262 (2011)
11. Tzeng, S.-F., Horng, S.-J., Li, T., Wang, X., Huang, P.-H., Khan, M.K.: Enhancing security and privacy for identity-based batch verification scheme in Vanets. IEEE Trans. Veh. Technol. **66**(4), 3235–3248 (2017)
12. Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K.: Specs: secure and privacy enhancing communications schemes for Vanets. Ad Hoc Netw. **9**(2), 189–203 (2011). Advances in Ad Hoc Networks (I)
13. Yong Hao, Yu., Cheng, C.Z., Song, W.: A distributed key management framework with cooperative message authentication in Vanets. IEEE J. Sel. Areas Commun. **29**(3), 616–629 (2011)
14. Yong Hao, Yu., Cheng, C.Z., Song, W.: A distributed key management framework with cooperative message authentication in vanets. IEEE J. Sel. Areas Commun. **29**(3), 616–629 (2011)
15. Fan, W., Zhang, X., Zhang, C., Chen, X., Fan, W., Liu, Y.: Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks. IEEE Internet Things J. **7**(9), 8144–8156 (2020)
16. Vinoth Kumar, P., Maheshwari, M.: Prevention of sybil attack and priority batch verification in Vanets. In: International Conference on Information Communication and Embedded Systems (ICICES2014), pp. 1–5 (2014)
17. Banani, S., Gordon, S.: Selecting basic safety messages to verify in Vanets using zone priority. In: The 20th Asia-Pacific Conference on Communication (APCC2014), pp. 423–428 (2014)
18. Sanguesa, J.A., et al.: A survey and comparative study of broadcast warning message dissemination schemes for Vanets. Mobile Inf. Syst. **2016** (2016)
19. Zhong, H., Huang, B., Cui, J., Yan, X., Liu, L.: Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. IEEE Access **6**, 2241–2250 (2018)
20. Kan, W.: Classification of queueing models for a workstation with interruptions: a review. Int. J. Prod. Res. **52**(3), 902–917 (2014)
21. Hafeez, K.A., Zhao, L., Mark, J.W., Shen, X., Niu, Z.: Distributed multichannel and mobility-aware cluster-based mac protocol for vehicular ad hoc networks. IEEE Trans. Veh. Technol. **62**(8), 3886–3902 (2013)
22. Chaudhry, M.L., Templeton, J.G.C.: A first course in bulk queues. (No Title) (1983)
23. Gabrel, V., Murat, C., Thiele, A.: Recent advances in robust optimization: an overview. Eur. J. Oper. Res. **235**(3), 471–483 (2014)
24. Lo, N.-W., Tsai, J.-L.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. **17**(5), 1319–1328 (2016)