IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 11, 2018, accepted April 3, 2018, date of publication April 13, 2018, date of current version May 2, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2826518

INVITED PAPER

Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-Based Co-Authentication in 5G-VANET

PUGUANG LIU[1], BO LIU[2], YIPIN SUN[1], BAOKANG ZHAO[1], AND ILSUN YOU[3], (Senior Member, IEEE)

[1]College of Computer, National University of Defense Technology, Changsha 410000, China
[2]College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha 410000, China
[3]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea

Corresponding author: Ilsun You (ilsunu@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61202482 and in part by the Soonchunhyang University Research Fund.

ABSTRACT The upcoming Fifth Generation (5G) networks can provide ultra-reliable ultra-low latency vehicle-to-everything for vehicular ad hoc networks (VANET) to promote road safety, traffic management, information dissemination, and automatic driving for drivers and passengers. However, 5G-VANET also attracts tremendous security and privacy concerns. Although several pseudonymous authentication schemes have been proposed for VANET, the expensive cost for their initial authentication may cause serious denial of service (DoS) attacks, which furthermore enables to do great harm to real space via VANET. Motivated by this, a puzzle-based co-authentication (PCA) scheme is proposed here. In the PCA scheme, the Hash puzzle is carefully designed to mitigate DoS attacks against the pseudonymous authentication process, which is facilitated through collaborative verification. The effectiveness and efficiency of the proposed scheme is approved by performance analysis based on theory and experimental results.

INDEX TERMS Denial of service, pseudonymous authentication, VANET, puzzles, co-authentication, 5G.

I. INTRODUCTION

The fifth generation (5G) networks are designed to provide good support for ultra-reliable ultra-low latency (URLLC) services [1], such as vehicle-to-everything (V2X) of Vehicular Ad Hoc Networks (VANET) in Intelligence Transportation System [2]. In recent years, 5G-VANET related research and standards development have drawn widespread attention both in industry and academia, e.g., the 5G Automotive Association (5GAA) considers that Cellular V2X (C-V2X) developed in the Third Generation Partnership Project (3GPP) will be a proper technology to provide URLLC for 5G-VANET [3] and Qualcomm Technologies reports that its 5G-VANET chipset, which supports C-V2X, will be available in 2018 [4]. Moreover, with the rapid development of 5G-VANET, the related applications such as automatic driving will also come to real life immediately. However, it is necessary to note that 5G-VANET is the critical point between cyberspace and real space, i.e., attacks against cyberspace are able to cause great harm to real space via VANET, e.g., privacy leaks, traffic paralysis and even more serious traffic accidents [5]–[7]. Therefore, It is of paramount importance to mitigate any attack in 5G-VANET.

In VANET, Dedicated Short Range Communications (DSRC) is a classic protocol designed for communications between vehicles. According to the DSRC, vehicles periodically report real-time traffic information including location, velocity, acceleration of vehicles, critical traffic events, and so forth. By sharing such ciritical information, drivers or autopilot programs can have a good understanding of the surrounding driving environment and take timely action to deal with sudden abnormal situation such as traffic accidents. However, the attractive applications proved to be double-edged [8], which hide the security and privacy risks. For example, an attacker can easily forge fake traffic information to induce traffic accidents or track target vehicles by collecting location information of the vehicles in VANET. To ensure both security and privacy in VANET, pseudonymous authentication schemes have been proposed over the past years [9]–[13].

The basic design of pseudonymous authentication schemes is as follows: each legitimate vehicle applies to a trusted third party for a large number of different digital certificates called pseudonymous certificates, each time period using a pseudonymous certificate to issue traffic information. This scheme enables to prevent illegal attacker from posting false

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

messages and pursue illegal vehicles through the trusted third party while protecting the location privacy of legitimate vehicles by a periodic replacement of the pseudonymous certificates (i.e., the identity of the entity cannot be associated with the location). It can be said that the pseudonymous authentication schemes is the cornerstone of the privacy and security of VANET.

However, in the pseudonymous authentication schemes, the pseudonymous certificate is mostly one-time and often replaced, which causes a large amount of obsolete certificates to be issued. In order to reduce the cost of digital certificates, the composition of vehicle digital certificates is generally more complex, resulting in the higher cost of the initial authentication in pseudonymous authentication schemes. The attackers can forge a large number of fake certificates for the initial authentication to launch DoS attacks. If the attackers use all the transmission bandwidth to send fake certificates, the computing resources of the on-board units (OBUs) will be completely occupied by the verification of massive fake certificates, leading to failure of normal communications. In the low latency and high bandwidth 5G-VANET, this kind of DoS attacks can be launched easily and result in disastrous consequences. Thus, this paper aims at how to refrain attackers from abusing the high cost for the initial authentication for DoS attacks by forging a large number of false pseudonymous identities. It is worth to note that this scenario is far different from the existing DoS mitigation schemes for VANET which focus on protecting communication bandwidth [14] and assume that each entity has an unique identity [15]–[20].

To overcome the above mentioned DoS attack against identity authentication, the cryptographic (hash-mapping) puzzles based authentication scheme has been proposed in wireless ad hoc networks [21] and in VANET [22]. The cryptographic puzzle is a character string whose hash value satisfies a certain format (i.e., the last k bits are all '0'). Due to the one-way character of hash function, a cryptographic puzzle is generated with the cost of a certain amount of computational resources, but it can be easily verified. In the pseudonymous authentication process, if every certificate verification request should be accompanied by a cryptographic puzzle, then attackers could not forge a large number of fake certificates for DoS attacks due to the limitation of its computational resources. Therefore, the cryptographic puzzle can be used to mitigate DoS attacks against pseudonymous authentication.

However, in view of the characteristics of 5G-VANET, improving the pseudonymous authentication based on the hash puzzle needs to address the following challenges:

- Because the inside space of vehicles is larger, the computer resources in the attackers may be much larger than the general users', which means that attackers have the ability to produce higher value puzzles. As higher value puzzles will be preferentially verified, the attacks will still affect the authentication of general users.
- Without the limitation of energy resource in wireless ad hoc networks, the attacker in VANET may precompute puzzles before launching DoS attack.
- The critical timeliness is required by the life-critical road safety related application. Though the low latency of 5G will be helpful to the critical timeliness, the more time-consuming certificate verification process must be completed as soon as possible.

To overcome the above challenges, this paper proposes **PCA**, a Puzzle-based Co-Authentication scheme in 5G-VANET. Basically, during the process of pseudonymous identity authentication, vehicles try to construct trust clusters among legitimate vehicles, and then co-authenticate by trust clusters to accelerate the identity authentication process. Specially, our contributions are threefold:

- Firstly, a computational puzzle is well-designed with the real-time information such as location, the expected receiver, and so on. In this way, puzzles cannot be precomputed, which allows DoS attacks against pseudonymous authentication to be mitigated.
- Secondly, based on the trust transitivity relations between vehicles, the connected components theory is used to construct the trust clusters, which can efficiently speed up the formation of trust clusters.
- Thirdly, the trust clusters co-authentication scheme is proposed. The vehicles inside a same trust cluster work together to verify pseudonymous certificates and recommend the cluster header to other clusters.

The remainder of the paper is organized as follows. In Section II, the related work will be surveyed. The detailed design and the workflow of PCA scheme are presented in Section III. In Section IV, the theory and numeric analysis and experiment results together with their analyses are demonstrated. Finally, some conclusions are drawn in Section V.

II. RELATED WORK AND CONTRIBUTIONS

A. PSEUDONYMOUS AUTHENTICATION IN VANET

The pseudonymous authentication for secure vehicular communication has attracted extensive attentions [9]–[13]. In [9], Raya and Hubaux first proposed that each vehicle in VANET keeps a large number of pseudonymous certificates in a long time and randomly selects one pseudonymous certificate for each time signing the message. However, once a vehicle became illegitimate or revoked, all its pseudonymous certificates, more than 40,000 certificates in [9], need to be added to a Certificate Revocation List (CRL). The CRL may increase so quickly that it cannot be noticed to all entities in VANET on time. To decrease the CRL size, the Efficient Conditional Privacy Preservation (ECPP) protocol was first developed by Lu *et al.* in [10]. According to ECPP, the Roadside Units (RSUs) can help each vehicle to update fewer short-time pseudonymous certificates in time. Furthermore, after Wasef *et al*'s efforts [11], RSUs-aided distribute certificate service was developed to a hierarchical authority architecture and an efficient Distributed Certificate Service (DCS) scheme was proposed to support batch signature verification. Furthermore, Sun *et al.* [12] proposed the proxy re-signature cryptography based Pseudonymous Authentication Scheme (PASS) to decrease certificate updating cost on road. PASS supports RSUs-aided distributed certificate service while the overhead of updating certificates will not be affected by the amount of updated certificates. Moreover, utilizing the one-way hash chains technology in PASS, the size of CRL just increases linearly with the amount of revoked vehicles. In order to achieve efficient and lightweight pseudonyms, Rajput *et al.* [13] proposed a hybrid approach combining the advantages of the pseudonym-based approaches and the group signature-based approaches, which can avoid to manage the CRL.

Although the above introduced schemes have addressed almost all well-known security and performance issues in routine application, the structure of pseudonymous certificates becomes complex, and the first time verification cost increases as well, e.g., increasing from 1.2msec [9] to more than 14.7msec [12]. As introduced in Section I, the pseudonymous authentication schemes may be out of work when an adversary launches DoS attack by broadcasting huge numbers of forged pseudonymous identities.

B. ANTI-DOS ATTACK METHODS IN VANET

Comparatively speaking, few works have been proposed against DoS in VANET. Hasbullah *et al.* [14] surveyed the possible DoS attacks in VANET and proposed serious solution against bandwidth DoS attacks, including Channel Switching, Technology Switching, Frequency Hopping Spread Spectrum (FHSS), etc.. To mitigate the DoS attacks against the message signature, He and Zhu [15] utilized the pre-authentication scheme before verifying signature, which combines the advantages of the one-way hash chain and the group rekeying method. Verma *et al.* [16] designed a Bloom Filter table of IP address to filter DoS traffic in VANET. To mitigate outside attackers, Pooja *et al.* [17] used Hash-based Message Authentication Code (HMAC) to authenticate the communicating vehicles. Mejri *et al.* [18] studied the use of game theory against DoS attacks in VANET.

However, all these works [15]–[17] are not suitable to defend the DoS attack against initial process of pseudonymous identity authentication, because the mitigation technologies (i.e., one-way hash chain [15], IP address [16], HMAC signatures links [17] and game theory models [18]) by default suppose the messages belongs to the same entity while the identity of the entity cannot be associated with the messages in the pseudonymous authentication schemes. Considering the DoS attack against RSUs caused by the signature verification overhead, Sun *et al.* [22] proposed a privacy-preserving mutual authentication resisting DoS attacks by cryptographic puzzle. Because their scheme is an ID-based signature scheme, they didn't analyze the possible DoS attack against OBUs caused by the initial certificate verification overhead.

Different from existing works, we focus on the DoS attack against pseudonymous authentication schemes in 5G-VANET. We mainly address the following issues:

1) The designed cryptographic puzzle attaching to the first time certificate verification request to prevent attackers from forging a large amount of fake pseudonymous certificates in 5G-VANET;
2) The mutual trust cluster co-authentication to reverse the imbalance of computational resources between legitimate vehicles and attackers and to speed up certificates authentication.

C. COOPERATIVE VERIFICATION IN VANET

In recent years, the idea of cooperation among vehicles has been proposed in VANET [23]. Early, COMET(cooperative message-authentication scheme) [24] proposed by Zhang *et al.* is designed to mitigate the message signature verification overhead of each vehicle by collaborative working. In this scheme, each legitimate vehicle will initiatively afford a certain amount of message signature verification based on their computing power. Because of the trust relationship between legitimate vehicles, legitimate vehicles need not to repeatedly verify the message verified by one legitimate vehicle. Considering the possible selfish behavior, Lin and Li in [25] achieve efficient cooperative message authentication by adopting the evidence token which reflects the personal contribution in cooperative authentication. In summary, several methods have been proposed to reduce the overhead of message signature verification. However, compared to the overhead of message signature verification, the overhead of the first time pseudonymous certificate verification is heavier, which is more desired for cooperative verification.

III. PUZZLE-BASED CO-AUTHENTICATION SCHEME

In this paper, we concentrate on mitigating DoS attacks against pseudonymous authentication in 5G-VANET. In our proposed scenario, the attackers will use the cost of the first time certificates verification to forge a large amount of fake verification requests for DoS attacks. In this section, we describe the detail of our PCA scheme, including the definition of the DoS attack against certificate authentication in 5G-VANET, the concept of hash puzzle and mutual trust cluster and how PCA works against DoS attack.

A. DOS ATTACK AGAINST VANET PSEUDONYMOUS CERTIFICATE AUTHENTICATION

Controlling the overhead of the data packet verification in 5G-VANET is very critical to ensure the real-time ability of traffic safety related applications. In order to verify the signature of packets in the pseudonymous authentication scheme, first of all, we have to verify the legality of the information publisher [26]. Although the legitimate pseudonymous certificate list can be cached to avoid multiple verification of the same certificate, the overhead of the first time verification of the certificate cannot be avoided. Moreover, the distributed pseudonymous authentication scheme increases the complexity of pseudo certificate structure and also the authentication overhead [27]. Generally speaking, every vehicle changes pseudo identity frequently, e.g., in a period of 1 minute, so other vehicles cannot analyze the link between the pseudonymous identities that belongs to the same owner. However, the first time verification cost of a pseudonymous identity is more than 14.7 msec, and it causes a risk of DoS attack during the changing process of pseudonymous identities. According to the IEEE 802.11p protocol, the data transmission rate of on-board communication is around 3-27 Mbps. Suppose the communication bandwidth is 15Mbps, an adversary could spam more than 20,000 forge pseudo identities per second while a vehicle could just verify 68 identities. In other words, the vehicle cannot recognize the legitimate identities of neighbor vehicles on time under this kind of DoS attack, and therefore cannot validate the further routine traffic messages, which means the information view of vehicles will be blind and a serious traffic accident may occur. Thus, towards the DoS attackers, the design of proper co-authentication scheme to verify certificates is very critical to preventing DoS attacks and improving the real-time ability and also the practicability of the distributed pseudo certificate authentication schemes.

Towards the on-board DoS attacks, the following assumptions are adopted in this paper:

- The difference of computational resources existed between attackers and common on-board devices is limited;
- The credibility level of majority legitimate vehicles is higher than semi-trusted, which means that semi-trusted vehicles will normally fulfill their role and responsibilities and will not take the initiative to attack other vehicles;
- Packets without verified signature cannot be forwarded by the legitimate vehicles. Personal signatures are attached to the forwarding package by the legitimate vehicles. It means that legitimate vehicles will just process the packets attached with verified signatures which must have been verified in the first time certificate verification.

The key point of DoS attack is to consume huge target computational resource with low cost. In the case of pseudonymous certificate authentication procedure, an attacker can release fake certificates nearly without any cost, while the cost of verifying fake certificates for vehicles is quite huge. In order to reverse the asymmetry of the attack and defense, it is necessary to increase the publishing cost of certificates, and to distributedly verify the pseudonymous certificate with the collaboration of legitimate vehicles. Based on the above idea, PCA scheme is elaborately designed, in which the hash puzzles can efficiently restrict the attacker's capability to release forged pseudonymous certificates and co-authentication mechanism can optimize the overhead of the computational resource among legitimate vehicles.

PCA scheme mainly includes two parts: hash puzzles designing against DoS attacks and co-authentication based on the mutual trust cluster to speed up certificates authentication. The detailed design will be shown in following sections.

B. HASH PUZZLES DESIGNING

Hash function is a kind of one-way function, that is, the function output, called the hash value, can be easily calculated by the function input, but it is difficult to calculate the function input deliberately when we just know the hash value. This property of the one-way hash function is well suited to constructing computational puzzles.

Classic Hash puzzle contains two elements, namely *message* and *answer* [28]. The length of the full zero tail of the binary hash value of these two elements can be used to evaluate the puzzle value, i.e.,

$$Hash(message||answer) = *\underbrace{00\ldots00}_{k}. \tag{1}$$

Here, we have the value of the puzzle,

$$Value(puzzle) = k. \tag{2}$$

The generation of a puzzle is the same as finding *answer* to the puzzle. Assuming that *message* and k are given, due to the one-way direction of hash operation, randomly constructing *answer* that meets this condition is nearly impossible, thus the vehicle can only generate *answer* to satisfy (1) by the parameter traversal search.

Generally, the time complexity of one hash operation is $O(1)$. The average number of hash operations required to calculate *answer* is 2^k. Thus, the time complexity of generating a puzzle is $O(2^k)$. It's clear that the larger k, the more difficult level of the puzzle, i.e., much more computational resource the vehicle costs.

In order to effectively mitigate DoS attacks, the time overhead of creating a puzzle must be properly considered. Assume that the available time of a pseudonymous certificate, i.e., the update time of pseudonymous certificates is T_{cert}, the number of legitimate vehicles is N_L, the certificate verification time overhead is T_V, the number of attackers is N_A, the computational power of a attacker is m times the computational power of a legitimate vehicle, and the time overhead of creating a puzzle is T_{puzzle}. Therefore, to mitigate DoS attacks, the number of certificates (including fake certificates) generated in T_{cert} can not exceed the number of certificates that a legitimate vehicle can verify in T_{cert}, that is,

$$N_L + \frac{m * N_A * T_{cert}}{T_{puzzle}} < \frac{T_{cert}}{T_V}. \tag{3}$$

Moreover, the time overhead of creating a puzzle, T_{puzzle}, should satisfy the inequality as follow,

$$T_{puzzle} > \frac{m * N_A * T_{cert} * T_V}{T_{cert} - N_L * T_V}. \tag{4}$$

Considering the characteristics of VANET and the requirements of collaborative verification of the certificates, we define three different roles related to the puzzles with the aspects of generation, verification and beneficiary.

- The generator: the generator and sender of puzzle. *Scert* is the generator's certificate summary. As this scheme aims to suppress the DoS attacks caused by forge certificate publishing, it is impossible to distinguish the certificate entities by verifying the certificate ID number. Thus, the certificate summary can be used as the distinction.

- The anticipated verifier: the verifier anticipated by generator. *Dcert* is the anticipated verifier's certificate summary. When the actual verifier is exactly the anticipated verifier, the weight of the puzzle will be increased.
- The beneficiary: the first beneficiary of the puzzle value and also the cooperative partner in co-authentication progress. *Bcert* is the anticipated verifier's certificate summary. Once a verified puzzle is valid, the value of the puzzle will be accumulated to both the generator's puzzle value and the beneficiary's puzzle value, which is used in the next co-authentication progress.

Two challenges existed when adopting puzzle to inhibit the number of forged fake certificates released by the attackers: (1) the attackers may precompute puzzles; (2) the attackers may give up the regular traffic process, and generate puzzles for each forged certificate within the released time slices. To address these challenges, on the one hand, the generator is required to provide geographic information L and timestamp information T of the generated puzzle and the receiver can evaluate the weight of the puzzle based on traffic conditions, which can restrict attackers to precompute puzzles. On the other hand, in our PCA scheme, the certificate with higher cumulative puzzle values will be verified at first. Therefore, all normal members will focus on generating puzzles to improve the cumulative puzzle value of themselves and then the co-authentication mechanism can integrate the computational resources of legitimate vehicles against attackers.

TABLE 1. The structure of *Puzzle*.

Element	Description
$Scert$	the certificate of the generator
$Dcert$	the certificate of the anticipated verifier
$Bcert$	the certificate of the beneficiary
L	the geographic information of the generator
T	the current time information of the generator
$answer$	the generated answer of puzzle

To meet these requirements, as shown in Table 1, the message is designed mainly containing five elements, i.e.,

$$message = Scert||Dcert||Bcert||L||T. \quad (5)$$

Moreover, a standard puzzle can be expressed as

$$Cert||Dcert||Bcert||L||T||answer.$$

Parameters of the message, except $Dcert$, must be filled in with valid values. $Dcert$ can be filled with a valid verifier's certificate or 0. Assume that the receiver's certificate is $Rcert$, the receiver's traffic track record is $Trace$, where $Trace(t)$ represents the receiver's location at the time t, the radius of the communication is δ (usually 300 m), the weight coefficient of the response range is γ (related to the traffic condition and communication condition), the weight coefficient of the verification correlation function is α, and the weight coefficient of the benefit feedback function is β, where $\gamma > 0$, $\alpha > 0$ and $\beta > 0$.

In summary, for the hash puzzle as Equation 1, the weighted value of the puzzle can be calculated as follow:

$$value = k * f(message) * g(message) * h(message). \quad (6)$$

These weighting functions are defined as follows:

1) Location correlation function.

$$f\,(message) = \begin{cases} 0, & if\ ||L - Trace(T)|| > \gamma * \delta \\ 1, & else \end{cases} \quad (7)$$

As described above, if the puzzle generator is beyond the receiver's range, this puzzle will not be considered. This function guides the vehicle to preferentially verify certificates of the vehicles near itself in order to obtain the traffic notice of surrounding vehicles as soon as possible.

2) Verification correlation function.

$$g(message) = \begin{cases} 1 + \alpha, & if\ Dcert = Rcert \\ 1, & else. \end{cases} \quad (8)$$

When the receiver is precisely the anticipated verifier, the weighted value of the puzzle will be increased. This function guides the vehicle to preferentially verify the certificates directed to itself, which is conducive to the construction of the mutual trust relationship between the puzzle generator and the receiver.

3) Benefit feedback function.

$$h(message) = \begin{cases} 1 + \beta, & if\ Bcert = Rcert \\ 1, & else. \end{cases} \quad (9)$$

When the receiver is the anticipated beneficiary, the weighted value of the puzzle will be increased. This function guides the vehicle to preferentially verify the vehicles that provide help for itself, which is also conducive to the construction of the mutual trust cluster in the distributed environment.

The above weighting functions are designed to suppress the attacker to precompute puzzles and to guide the vehicle to avoid verifying the same certificates again, which is conducive to optimizing the efficiency of distributed verification.

Summary about, the design of hash puzzle in PCA scheme is the key of anti-DoS attack. First, as the components of the designed puzzle, L and T ensure that attackers can not precompute puzzle for fake messages. Then, the computational complexity of hash puzzles limits the ability of attackers to mass-publish fake messages in real time. Finally, the ingenious composition of puzzles can also speed up the construction of the mutual trust relationship between each vehicles. It is noted that the attacker still have the stronger computational power to forge some fake certificates verification messages, which will interfere the communication of these crucial real-time messages. To address this problem, we design the mutual trust cluster to achieve cooperation among legitimate vehicles for efficient certificates verification and against the stronger computational power of attackers.

C. MUTUAL TRUST CLUSTER DESIGNING

The attacker's computational resources are normal users several times or even more than ten times. It's necessary to design a collaborative authentication protocol in PCA scheme to integrate the computing resources among verified legitimate vehicles against the attacker's strong computational resources.

In order to construct such a collaborative authentication protocol, a collaborative group is defined, i.e., a mutual trust cluster. A mutual trust cluster is composed of vehicle members who trust each other already. The members of a same mutual trust cluster can generate puzzles together or cooperate to verify the certificate. Some variables of PCA scheme are shown in Table 2.

TABLE 2. Variables of PCA scheme.

Element	Description
OBU_i	the vehicle i
$Cert_i$	the certificate of OBU_i
$Legal\_set$	the set of vehicles with legitimate certificates
$Fake\_set$	the set of vehicles with fake certificates
$Unverified\_set$	the set of vehicles with unverified certificates
$value_i$	the cumulative value of $Cert_i$ that $Cert_i \in Legal\_set \cup Unverified\_set$
$Value\_set$	the set of $value$
$Trust\_set$	the set of vehicles with trusted certificates

In a directed graph G, if there is at least one path between two vertices, the two vertices are said to be strongly connected. If each two vertices of a directed graph G are strongly connected, G is called a strongly connected graph. The strongly connected subgraph of a non-strongly connected directed graph is called strongly connected components [29]. As shown in Figure 1, the subgraph $\{1, 2, 3, 4\}$ is a strongly connected component, because the vertex 1, 2, 3, 4 are reachable between any two vertexes. Moreover, $\{5\}$ and $\{6\}$ are also two strongly connected components, respectively.

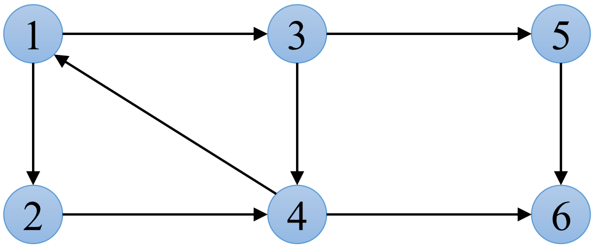


FIGURE 1. An example of the directed graph.

The usage of strongly connected components will be conducive to construction of the mutual trust cluster. As shown in Table 2, in PCA scheme, the vehicle OBU_i maintains the set of legitimate certificates $Legal\_set = \{\langle v_L \rangle\}$, the set of fake certificates $Fake\_set = \{\langle v_F \rangle\}$, the set of unverified certificates $unverified\_set = \{\langle v_U \rangle\}$ and the set of cumulative values of the legitimate and the unverified certificates $Value\_set = \{\langle value_i \rangle\}$. Moreover, each vehicle maintains the trust relationship view $G = (V, E)$, where G is a directed graph, V is the set of all legitimate vehicles and E is the set of the trust relationships. For the vehicle OBU_i, G_i is its trust relationship view and V is the set of the vehicles who are contained in $Legal\_set$. If the edge $e_{i,j} \in E$, it means OBU_i have verified $Cert_j$ is a legitimate certificate, that is, OBU_i trusts OBU_j. In the process of constructing the mutual trust cluster, the trust transfer is used, i.e., if OBU_i trusts OBU_j, then OBU_i trusts the legitimate certificates notification published by OBU_j (As a result, the certificates in the legitimate certificate notification need not to be verified). Based on the above assumptions, thus, the mutual trust cluster of OBU_i is exactly the strong component of OBU_i's trust relationship view G_i.

VANET is a distributed environment, and the trust relationship view of each vehicle like G_i is incomplete or inconsistent. However, in the process of certificate verification, vehicles will broadcast their mutual trust clusters. Thus, the overall directed graph G of each vehicle contains multiple strongly connected components, i.e., mutual trust clusters. With the progress of certificate verification process, when G becomes a strongly connected graph, i.e., all members in the system belong to the same mutual trust cluster, the certificate verification process is finished.

The designed scheme needs to ensure that the vehicles can form a mutual trust cluster. In our proposed scheme, a mutual trust cluster solution scheme for OBU_i is proposed to find the strongly connected component containing the node i. Classical methods to find the strongly connected component in a directed graph include Kosaraju−Sharir algorithm [30], [31], Tarjan algorithm [32], Gabow algorithm [33], etc., which are effective for a usual directed graph. However, unlike a usual directed graph, the trust relationship view G_i is unusual, in which OBU_i trusts others OBUs, that is,

$$\forall v_j \in G_i.V, \quad \exists e_{i,j} \in G_i.E.$$

The above feature is helpful to simplify the mutual trust cluster solution process of OBU_i and reduce the overhead of the mutual trust cluster solution. Specific steps of the simplified solution are as follows:

1) Initialize the mutual trust cluster $Trust\_set = \{v_i\}$, the edge set $E_t = E$, where v_i is corresponding to OBU_i.
2) Let $Trust\_set^* = Trust\_set$, and traverse the edge set E_t. If there is an edge $e_{k,j} \in E_t$ and $OBU_j \in Trust\_set^*$, then we have $E_t = E_t - \{e_{k,j}\}$ and $Trust\_set^* = Trust\_set^* \cup \{v_k\}$.
3) After the traversal, if $Trust\_set \neq Trust\_set^*$, let $Trust\_set = Trust\_set^*$, then repeat (2), otherwise the solution is completed and return the mutual trust cluster $Trust\_set$.

The pseudo-code of the mutual trust cluster solution algorithm is shown as Algorithm 1.

Algorithm 1 The Mutual Trust Cluster Solution Algorithm

```
Require: $E$: edge set of graph $G$; $v_i$: graph node of car $i$;
Ensure: $Trust\_set$: the mutual trust cluster
$Trust\_set = \{v_i\}$
$E_t = E$
$Trust\_set^* = 0$
while $Trust\_set \neq Trust\_set^*$ do
    if $Trust\_set^* \neq 0$ then
        $Trust\_set^* = Trust\_set$
    end if
    $Trust\_set = Trust\_set^*$
    for each $e_{k,j} \in E_t$ do
        if $OBU_j \in Trust\_set^*$ then
            $E_t = E_t - \{e_{k,j}\}$
            $Trust\_set^* = Trust\_set^* \cup \{v_k\}$
        end if
    end for
end while
return $Trust\_set$
```

Compared with the time complexity $O(V + E)$ of these classical algorithm, the time complexity of our algorithm is $O(E)$, which can better accelerate the formation of the mutual trust.

In conclusion, the mutual trust cluster actually is the mutual trust relationship among legitimate vehicles. Once an unknown certificate have been verified by one vehicle of the mutual trust cluster, the other vehicles of the mutual trust cluster need not to verify this certificate again, which can significantly save the average computational resources of legitimate vehicles. Besides, in our PCA scheme, when the mutual trust cluster is regarded as the object to be verified, the computational resources of all the members in the mutual trust cluster can be integrated to increase the puzzle value corresponding to the certificate to be verified, which is the other hand of solution against the attacker's stronger computational power. These features will be described in the following subsection.

D. PCA DETAILS

In this section, first of all efforts are made to show the working flow of our proposed PCA scheme and then describe details of PCA scheme.

As shown in Figure 2, in PCA scheme, after system initializing, the received messages will be processed firstly to ensure timely response to messages. Then, puzzles will be generated for these certificates of vehicles in $Legal\_set - Trust\_set$ to speed up the formation of the mutual trust cluster. Finally, these certificates of vehicles in $Unverified\_set$ will be verified to form the trust relationship between legitimate vehicles. Moreover, throughout the process,we subdivide the working time into periods. Each period, noted as ΔT, is used to ensure the legitimate certificates broadcast at a certain cycle.

Let OBU_i be the vehicle member, and $Cert_i$ denotes the certificate of OBU_i. As presented in section III-C, the vehicle OBU_i maintains several sets, including $Legal\_set$, $Fake\_set$, $unverified\_set$ and $Value\_set$, the trust relationship view $G_i = (V, E)$, the certificate of the mutual trust cluster header $Cert_{header}$, $Puzzle$, $Scert$, $Dcert$, $Bcert$, L, T, ΔT and the timer t.

Choosing the vehicle OBU_i as an example, specific steps of PCA scheme are as follows:

Step 1: Initialize PCA system. Let $Legal\_set = 0$, $Fake\_set = 0$, $Unverified\_set = 0$, $Value\_set = \{value_i\}$, $G_i.V = \{v_i\}$, $Trust\_set = \{v_i\}$, $Scert = Cert_i$, $Dcert = 0$, $Bcert = Cert_{header} = Cert_i$.

Step 2: Reset the timer $t = 0$, generate the legitimate certificates mutual trust relationship set,

$$\left\{\langle (Cert_a, Cert_b)\rangle \,|e_{a,b} \in E\right\},$$

and publish the notification of the legitimate certificates mutual trust relationship with the signature of OBU_i, where the signature is used to ensure the legality of the notification.

Step 3: Firstly, if $t > \Delta T$, it's time to publish the legitimate certificates broadcast, so return to **Step 2**. Secondly, if receive messages, jump to **Step 4**. Then, if $Legal\_set - Trust\_set \neq 0$, let $Dcert_i = Cert_{max}$, where $Cert_{max} \in Legal\_set - Trust\_set$ and $value_{max}$ is the maximum in $Value\_set$, jump to **Step 6**. Finally, if $Unverified\_set = 0$, repeat **Step 3**, otherwise jump to **Step 7**.

Step 4: If receive the legal certificate trust relationship notification, update the local trust relationship view $G_i = (V, E)$ and calculate the mutual trust cluster by the algorithm presented in section III-C, and return to **Step 3**. Otherwise, if receive the certificate verification request with the puzzle from OBU_j, continue to **Step 5**.

Step 5: The puzzle received from OBU_j puzzle is

$$Cert_j||Dcert_j||Bcert_j||L||T||answer.$$

If $Cert_j = Cert_{header}$, the verification request is from the mutual trust cluster header, which means the mutual trust cluster header OBU_{header} try to establish the trust relationship with the target vehicle whose certificate is $Dcert_j$. Therefore, as the member of the mutual trust cluster, OBU_i should help OBU_{header} to generate puzzles to improve the puzzle value of $Bcert_j$, which reflects our proposed co-authentication mechanism. Thus, if find $Cert_j = Cert_{header}$, let $Dcert_i = Dcert_j$ and $Bcert_i = Bcert_j$, and jump to **Step 6**.

If $Cert_j \in Fake\_set$, then drop the verification request and return to **Step 3**. Otherwise, calculate the puzzle value, $value_{puzzle}$, by (6). If $Cert_j \notin Legal\_set \cup Unverified\_set$, $Cert_j$ will be added to $Unverified\_set$. Then, OBU_i will update cumulative puzzle values of $Cert_j$ and $Bcert_j$ with the calculated value of the received puzzle as follow,

$$value_j = value_j + value_{puzzle}, \tag{10}$$

$$value_b = value_b + value_{puzzle}, \tag{11}$$

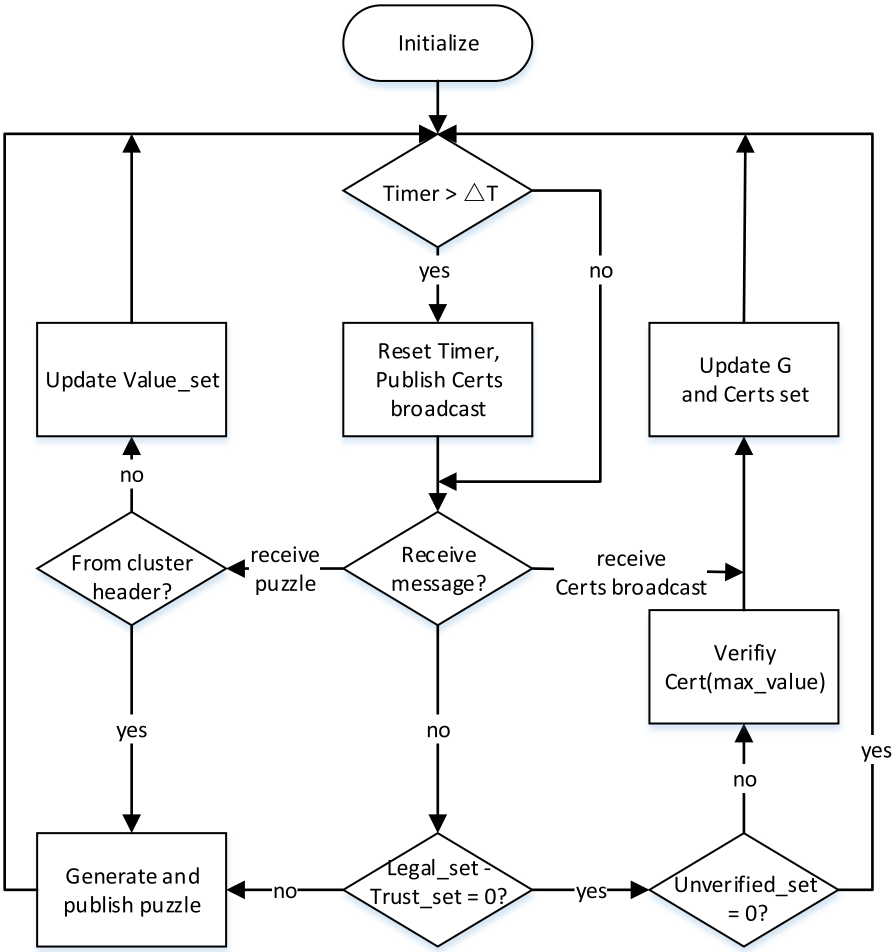


FIGURE 2. The working flow of PCA scheme.

where $value_j$ is the puzzle value of $Cert_j$ and $value_b$ is the puzzle value of $Bcert_j$. After this step, return to **Step 3**.

Step 6: Generate puzzles. During the puzzle calculation period Δt_{puzzle}, OBU_i constructs the following hash puzzle:

$$Cert_i||Dcert_i||Bcert_i||L||T||answer,$$

where L represents the current geographic location of the puzzle generator OBU_i, T represents the current timestamp, *answer* represents the solution to the puzzle, and $Dcert_i$ and $Bcert_i$ use the current variable value.

Repeatedly calculate the hash puzzle with the above variables and random *answer*, meanwhile recording the maximum puzzle value and the corresponding puzzle, until the puzzle calculation period is over. Then, the puzzle with the maximum puzzle value will be chosen and published.

After this step, return to **Step 3**.

Step 7: Select $Cert_{max} \in Unverified\_set$ that $value_{max}$ is the maximum puzzle value in $Value\_set$. Verify $Cert_{max}$, and if the verification fails, $Cert_{max}$ will be added to the fake certificates set $Fake\_set$, other verification requests containing $Cert_{max}$ will be dropped and $Cert_{max}$ will be submitted to the trust authority (TA) that the TA will investigate related illegal vehicles. If the certificate $Cert_{max}$ is valid, $Cert_{max}$ will be added to the legal certificate set $Legal\_set$ and the local trust relationship view $G_i = (V, E)$ will be updated that v_{max} will be added to $G_i.V$ and $e_{i,max}$ will be added to $G_i.E$.

Through these above steps, PCA scheme can effectively mitigate DoS attacks against pseudonymous authentication in 5G-VANET. In normal pseudonymous authentication scheme, the certificate verification will be done firstly, while the higher verification cost can cause the DoS attacks. However, in our proposed PCA scheme, all certificates to be verified will be sorted by the descending order of their puzzle values and the certificate with the maximum puzzle value will be verified firstly as shown in Figure 3. Therefore, the DoS attacks against pseudonymous authentication will be fundamentally mitigated because the attacker cannot create a large number of forged certificates with valid puzzle values.

As shown in Figure 4, according to our co-authentication mechanism, as the member of the mutual trust cluster $\{1, 2, 3, 4\}$, OBU_1, OBU_2 and OBU_3 help their cluster header OBU_1 to generate puzzles to improve the puzzle value

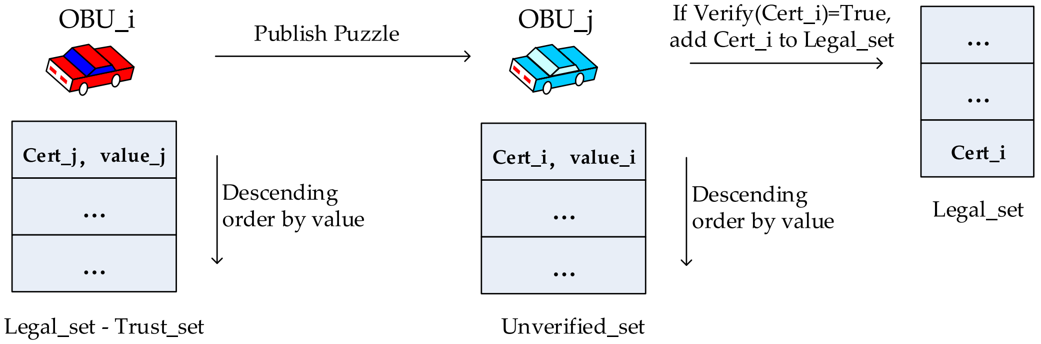


FIGURE 3. The process of verification.

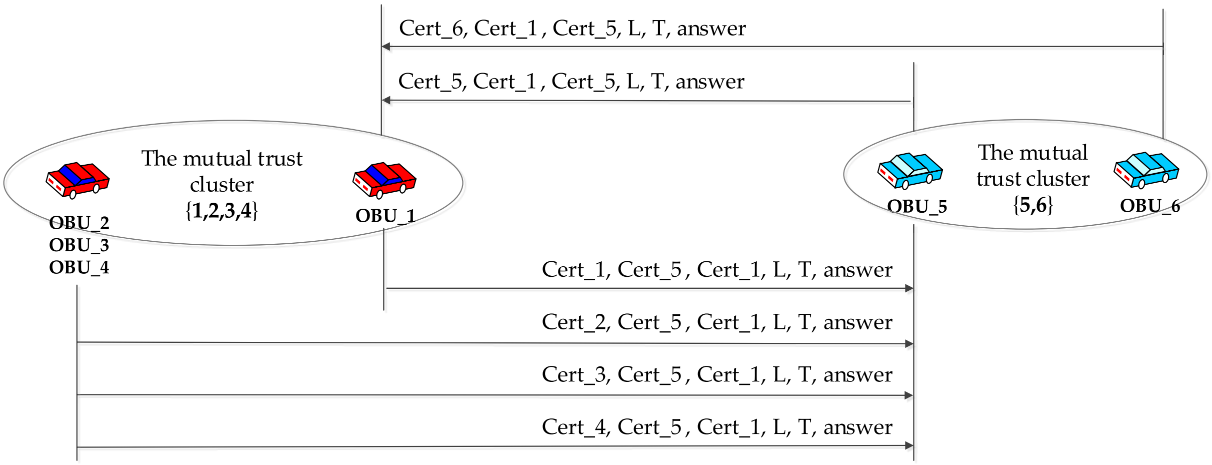

Cert_6, Cert_1 , Cert_5, L, T, answer
Cert_5, Cert_1 , Cert_5, L, T, answer
The mutual trust cluster {1,2,3,4}
OBU_2
OBU_3
OBU_4
OBU_1
The mutual trust cluster {5,6}
OBU_5
OBU_6
Cert_1, Cert_5 , Cert_1, L, T, answer
Cert_2, Cert_5 , Cert_1, L, T, answer
Cert_3, Cert_5 , Cert_1, L, T, answer
Cert_4, Cert_5 , Cert_1, L, T, answer

FIGURE 4. The process of co-authentication.

of $Cert_1$. Similarly, OBU_6 helps its cluster header OBU_5 to generate puzzles to improve the puzzle value of $Cert_5$. Even if the DoS attackers use their all computational resources to generate puzzles, the co-authentication mechanism can integrate all computational resources of the mutual trust cluster to ensure that the puzzle values of legitimate vehicles will higher than attackers. Thus, these co-authentication actions will help to establish the mutual trust relationship between OBU_1 and OBU_5, and furthermore speed up the integration of the two mutual trust clusters, meanwhile unaffected by the stronger computational power of attackers. Conclusively, in PCA scheme, the co-authentication based on the mutual trust cluster can greatly speed up the mutual authentication between legitimate vehicles in 5G-VANET to ensure rapid response to the routine traffic related messages.

IV. PERFORMANCE ANALYSIS

The two significant contributions of PCA scheme is mitigating DoS attacks against pseudonymous authentication by hash puzzle and optimizing the overhead of authentication through mutual trust cluster mechanism. The performance analysis of these two aspects are described respectively in following subsections.

A. CONSTRAINT CAPABILITY EVALUATION OF COMPUTATIONAL PUZZLES

Comparing with the classical schemes, PCA restricts the attacker's ability to release forge certificate packets based on computational hard problems. In order to conduct quantitative comparison, we assume that bilinear pairings are implemented by the Tate pairing on the MNT curve [34] with the degree of 6, where G can be represented as 161 bits, the order q can be represented as 160 bits, and the hash function is SHA-1. T_{mul} indicates the time of a completion of a multiplication computation in G, and T_{par} indicates the pairing operation time [12]. The processing time has been measured in [34], in which RSUs and vehicles are equipped with the Intel Pentium IV 3.0 GHZ CPU, then $T_{mul} = 0.6$ msec and $T_{par} = 4.5$ msec. Table 3 shows the certificate length, certificate verification overhead, and signature verification overhead of three typical distributed alias methods. The available time of a single certificate $\Delta t_{available} = 1$ min.

In the traditional schemes, the ability of DoS attackers to release forge certificates depends on the ability to forward packets. According to the IEEE 802.11p protocol, the data transmission rate of on-board communication is around 3-27 Mbps, and the average value is around 15 Mbps while

TABLE 3. Communication and computational overheads of classical distributed pseudonymous authentication schemes .

Scheme	Length of certificate (bits)	Overhead of the certificate verification	Overhead of the signature verification
ECPP	147	$3T_{par}+9T_{mul}$	$2T_{mul}$
DCS	167	$3T_{par}+2T_{mul}$	$3T_{par}+T_{mul}$
PASS	175	$3T_{par}+2T_{mul}$	$2T_{mul}$

the data transmission rate would be higher in 5G-VANET. If the PASS scheme is adopted, the number of the forged certificate notifications issued by a single attacker per second is about 11234, and the overhead caused by the forge certificates is about 165 s which is more than $\Delta t_{available}$, i.e., resulting that the verification of even one certificate cannot be completed in a valid period.

Conducting our proposed scheme, the capability of DoS attack depends on its computational capability. According to Moore's Law, we assume the lifetime of vehicle computational platform is 5 years, the maximum performance difference of coexisted vehicle platform is about 6-10 times. As a result, even if an attacker has 10 times the computational power of an ordinary car user, the number of fake certificates that can be forged during a normal puzzle calculation period Δt_{puzzle} is 10, with a verification cost of about 0.147 s, far less than $\Delta t_{available}$. From the above comparison, we can find that the basic assumption of our proposed scheme significantly limits the constraint capability of a single attacker.

To further evaluate the effectiveness of our scheme, a simulation experiment have been conducted by ns-2 [35]. We design a simulation scenario with 20 legitimate vehicles, one attack vehicle and one victimized vehicle. The experiment time of is 9 s. The update time of pseudonymous certificates is 1 min. The certificate verification time overhead is 0.0147 s. The computational power of a attacker is 10 times the computational power of a legitimate vehicle. According to 4, the time overhead of creating a puzzle must be greater than 0.1477 s, which is set to 0.5 s in the experiment. According to DSRC in VANET, each legitimate vehicle on the road broadcasts the routine traffic related messages in a period of 300 ms. Thus, the valid packets sent by legitimate vehicles in 9 s is 600. The performance of mitigating DoS attacks are measured by the number of valid packets received by the victimized vehicle.

Figure 5 describes the results of this experiment. As shown in Figure 5, when using our PCA scheme, the number of valid packets received by the victimized vehicle is 600, i.e., the victimized vehicle receives all packets sent by other legitimate vehicles, which means that the victimized vehicle is affected by DoS attacks. Comparatively, without our PCA scheme, the number of valid packets received is between 26 and 43 and the packet loss rate is about 94%, i.e., almost all valid packets are not received which means that the DoS attacks against pseudonymous authentication do have a huge impact in VANET. Thus, according to Figure 5, our proposed PCA scheme can effectively mitigate DoS attacks against pseudonymous authentication in 5G-VANET.

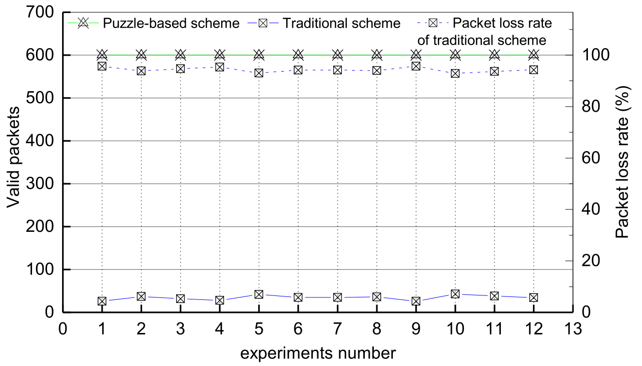


FIGURE 5. The number of valid packets received by the victimized vehicle when using puzzle-based scheme and traditional scheme and the packet loss rate when using traditional scheme.

B. CO-AUTHENTICATION CAPABILITY EVALUATION BASED ON MUTUAL TRUST CLUSTER

Co-authentication mechanism of PCA scheme is the key method to optimize the construction of mutual trust cluster and decrease the time overhead of all vehicles. Suppose that there are N_L legitimate vehicles in the system, and the attackers has the equally computational resource as M times of a single legitimate vehicle. As the computational puzzles limit the generation of certificates, in order to achieve the optimal attack effect, it is assumed that the attackers adopt an equal resource strategy to imitate the M false vehicles and publish computational hard problems and certificates. In traditional scheme, without collaborative mechanisms, each vehicle needs to verify $(M+N)$ certificates, i.e., the overhead is approximately $(M+N)\cdot T_{cert}$. For the collaboration mechanism of mutual trust cluster, the legitimate vehicles take about average $\left(\frac{M}{N}+1\right)$ verifications to verify the first legitimate certificate. According to the weighting mechanism of our proposed scheme, a computational puzzle is directed issued to accelerate the construction of mutual trust clusters when a legitimate vehicle is found. In the worst case, it takes $O\left(\log_2 N\right)$ times to complete the verification of all certificates. We verify a certificate and signature at each time, and consequently the total overhand is $\left(\frac{M}{N}+1\right)\cdot T_{cert}+O\left(\log_2 N\right)\left(T_{cert}+T_{sign}\right)$, i.e., as shown in Figure 6, the certificate verification overhead increases logarithmically with the number of vehicles when using mutual trust cluster scheme, while the certificate verification overhead increases linearly with the number of vehicles without mutual trust cluster scheme. Obviously, our proposed scheme is better than the schemes which do not take the collaborative mechanism.

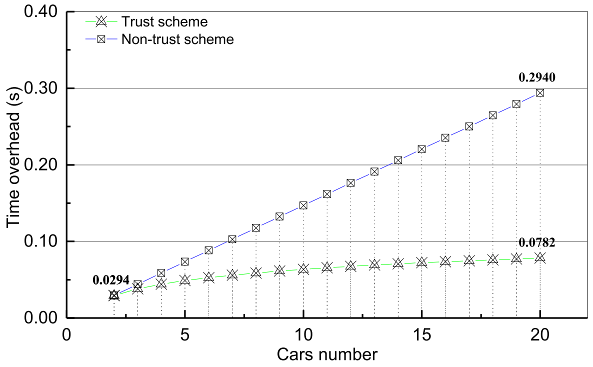


FIGURE 6. The theoretical time overhead of certificate verification when applying mutual trust cluster scheme and traditional scheme scheme.

The entire pseudonymous authentication progress starts with the fact that all vehicles do not trust each other until each vehicle trusts the others. To further evaluate the time overhead optimization of our PCA scheme for the entire pseudonymous authentication progress, we practice the entire pseudonymous authentication progress with and without PCA scheme in ns-2. In addition to the overhead of certificate verification, the overhead of the entire pseudonymous authentication progress includes the puzzles generation overhead, signature verification overhead, data transfer overhead, etc., which increase with the number of vehicles in the traditional scheme. The entire pseudonymous authentication progress is practiced with different number of vehicles, and the average time overhead of all vehicles are adopted to measure the performance of different scheme.

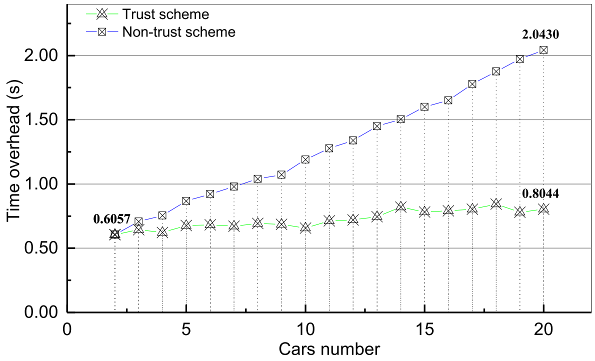


FIGURE 7. The average time overhead of all vehicles during the entire pseudonymous authentication progress when applying PCA scheme and traditional scheme.

As shown in Figure 7, the trend of time overhead of different schemes is basically consistent with the previous theoretical analysis. Compared with the theoretical analysis, the time overhead of the two schemes are significantly increased due to the addition of the puzzles generation overhead, signature verification overhead, data transfer overhead, etc.. We can see that the overhead of traditional scheme increases linearly with the number of vehicles while the overhead of PCA scheme remains at a lower level. Thus, our proposed PCA scheme can effectively optimize the construction of mutual trust cluster and decrease the time overhead of all vehicles in 5G-VANET.

V. CONCLUSION

Several mature pseudonymous authentication schemes have been proposed for 5G-VANET to achieve security and privacy of vehicles. However, the initial certificates verification overhead of pseudonymous authentication schemes may cause serious DoS attacks. In this paper, we have proposed a puzzle-based co-authentication scheme called PCA scheme. The hash puzzle is carefully designed to fundamentally restrict the attacker's capability to forge fake pseudonymous certificates, and collaborative verification is used to integrate the computing resources among legitimate vehicles, either as the certificate verifier or the certificate owner. Thus, our PCA scheme can provide capacity of resisting DoS attacks against pseudonymous authentication and improving the efficiency of certificates verification in 5G-VANET. Moreover, the PCA scheme can be easily combined with mutual pseudonymous authentication schemes to enhance the capacity of resisting DoS attacks and improving the efficiency of certificates verification.

The PCA scheme's capacity for mitigating DoS attacks and decreasing the overhead of pseudonymous authentication is experimented in ns-2. Performance analysis based on theory and experimental results validate the effectiveness and efficiency of our proposed scheme. Through deploying the PCA scheme, the DoS attacks against pseudonymous authentication in 5G-VANET can be totally mitigated and the growth trend of certificate verification overhead with the number of vehicles significantly changes from linear to logarithmic.

In the PCA scheme, the hash function is adopted to generate puzzles. However, based on the stochastic theory and our experimental analysis, the distribution of hash puzzle values generated in a same given time is not very concentrated, which may affect the function of the puzzle. Our future work will be focused on solving this problem with different computational puzzles and finding better method to facilitate pseudonymous authentication progress.

REFERENCES

[1] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[2] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[3] 5GAA. (2016). *The Case for Cellular V2X for Safety and Cooperative Driving*. Accessed: Nov. 1, 2017. [Online]. Available: http://5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf

[4] Qualcomm. *Qualcomm Announces Groundbreaking Cellular-V2X Solution to Support Automotive Road Safety, Helping to Pave a Path for the Future of Autonomous Driving*. Accessed: Nov. 1, 2017. [Online]. Available: http://www.qualcomm.com

[5] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Inf. Sci.*, vols. 412–413, pp. 223–241, Oct. 2017.

[6] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowl.-Based Syst.*, vol. 79, pp. 18–26, May 2015.

[7] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generat. Comput. Syst.* vol. 74, pp. 76–85, Sep. 2017.

[8] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2005, pp. 11–21.

[9] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1370616.1370618

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.

[11] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed-certificate-service scheme for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.

[12] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, 2010.

[13] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.

[14] H. Hasbullah, I. A. Soomro, and J.-L. A. Manan, "Denial of service (DOS) attack and its possible solutions in VANET," *Int. J. Electron. Commun. Eng.*, vol. 4, no. 5, pp. 813–817, May 2010. [Online]. Available: https://scholar.waset.org/1307-6892/15804

[15] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng.*, May 2012, pp. 261–265.

[16] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," *Wireless Pers. Commun.*, vol. 73, no. 1, pp. 95–126, 2013.

[17] B. Pooja, M. M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," in *Proc. Asia–Pacific Conf. Comput. Aided Syst. Eng.*, 2014, pp. 152–157.

[18] M. N. Mejri, N. Achir, and M. Hamdi, "A new security games based reaction algorithm against DOS attacks in VANETs," in *Proc. Consum. Commun. Netw. Conf.*, 2016, pp. 837–840.

[19] J. Li *et al.*, "Secure distributed deduplication systems with improved reliability," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3569–3579, Dec. 2015.

[20] J. Li *et al.*, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Security*, vol. 72, pp. 1–12, Jan. 2018.

[21] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 1, pp. 1–35, 2008.

[22] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting dos attacks in vanets," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.

[23] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[24] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[25] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, Sep. 2013.

[26] H. Sun, W. Wang, H. Lu, and P. Ren, "AutoMal: Automatic clustering and signature generation for malwares based on the network flow," *Secur. Commun. Netw.*, vol. 8, no. 10, pp. 1845–1854, 2015.

[27] H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices," *Softw., Pract. Experim.*, vol. 47, no. 3, pp. 421–441, 2017. [Online]. Available: http://dx.doi.org/10.1002/spe.2420

[28] A. Juels and J. Brainard, "Client puzzles: A cryptographic defense against connection depletion attacks," in *Proc. NDSS*, 1999, pp. 151–165.

[29] Wikipedia. (2017). *Strongly Connected Component—Wikipedia, the Free Encyclopedia*. Accessed: Nov. 1, 2017. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Strongly_connected_component&oldid=807193113

[30] M. Sharir, "A strong-connectivity algorithm and its applications in data flow analysis," *Comput. Math. Appl.*, vol. 7, no. 1, pp. 67–72, 1981.

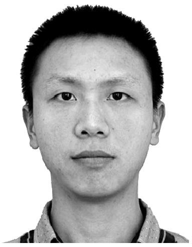
[31] Wikipedia. (2017). *Kosaraju's Algorithm—Wikipedia, the Free Encyclopedia*. Accessed: Nov. 1, 2017. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Kosaraju

[32] R. Tarjan, "Depth-first search and linear graph algorithms," in *Proc. Switching Autom. Theory*, 2008, pp. 114–121.

[33] H. N. Gabow, "Path-based depth-first search for strong and biconnected components," *Inf. Process. Lett.*, vol. 74, no. 3, pp. 107–114, 2000.

[34] M. Scott. (2007). *Efficient Implementation of Cryptographic Pairings*. Accessed: Nov. 1, 2017. [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[35] (2017). *The Network Simulator—NS*. Accessed: Nov. 1, 2017. [Online]. Available: http://nsnam.sourceforge.net/wiki/index.php/Main_Page



PUGUANG LIU received the B.E. degree from the College of Computer, National University of Defense Technology, Changsha, China, in 2016, where he is currently pursuing the M.E. degree. He is interested in topics related to vehicular networks, especially for security and privacy protection.

BO LIU received the B.S. degree from the School of Computer Science, Fudan University, and the M.E. degree from the College of Computer, National University of Defense Technology. He is currently a Professor with the College of Computer, National University of Defense Technology. His current research interests include computer networks and information security.

YIPIN SUN received the Ph.D. degree from the College of Computer, National University of Defense Technology. From 2008 to 2009, he was with the Broadband Communications Research Group, University of Waterloo. His research interests include intrusion detection, network security, and applied cryptography.

BAOKANG ZHAO received the B.S., master's, and Ph.D. degrees from the National University of Defense Technology, all in computer science. He is currently an Associate Professor with the College of Computer, National University of Defense Technology. His current research interests include computer networks, artificial intelligence, distributed computing, and information security.

ILSUN YOU (SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the second Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with the THINmultimedia Inc., Internet Security Co., Ltd., and Hanjo Engineering Co., Ltd. as a Research Engineer. He is currently an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University. He has served or is currently serving as a Main Organizer of international conferences and workshops, such as MobiWorld, MIST, SeCIHD, AsiaARES, and IMIS. His main research interests include internet security, authentication, access control, and formal security analysis. He is a fellow of the IET. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. He is in the Editorial Board for *Information Sciences*, the *Journal of Network and Computer Applications*, the IEEE ACCESS, *Intelligent Automation & Soft Computing*, the *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, and the *Journal of High Speed Networks*.