



室蘭工業大学

学術資源アーカイブ

Muroran Institute of Technology Academic Resources Archive



AccessAuth : Capacity-aware security access authentication in federated-IoT-enabled V2G networks

メタデータ	言語: eng 出版者: Elsevier 公開日: 2019-08-26 キーワード (Ja): キーワード (En): V2G, Authentication, Capacity, Security 作成者: TAO, Ming, 太田, 香, 董, 冕雄, QIAN, Zhuzhong メールアドレス: 所属:
URL	http://hdl.handle.net/10258/00009983

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



AccessAuth: Capacity-aware Security Access Authentication in Federated-IoT-enabled V2G Networks

Ming Tao^{a,b}, Kaoru Ota^b, Mianxiong Dong^{b,*}, Zhuzhong Qian^c

^a*School of Computer Science and Network Security, Dongguan University of Technology, Dongguan, China*

^b*Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan*

^c*Department of Computer Science and Technology, Nanjing University, Nanjing, China*

Abstract

Vehicle-to-Grid (V2G) systems promoted by the federated Internet of Things (IoT) technology will be ubiquitous in the future; therefore, it is crucial to provide trusted, flexible and efficient operations for V2G services using high-quality measures for security and privacy. These can be achieved by access and authority authentication. This paper presents a lightweight protocol for capacity-based security access authentication named *AccessAuth*. Considering the overload probability and system capacity constraints of the V2G network domain, as well as the mobility of electric vehicles, the ideal number of admissible access requests is first calculated adaptively for each V2G network domain to actively achieve capacity-based access admission control. Subsequently, to provide mutual authentication and maintain the data privacy of admitted sessions, by considering whether there is prior knowledge of the trust relationship between the relevant V2G network domains, a high-level authentication model with specific authentication procedures is presented to enforce strict access authentication such that the sessions are conducted only by authorized requesters. Additionally, efficient session revocation with forward security and session recovery with no extra authentication delay are also discussed. Finally, analytical and evaluation results are presented to demonstrate the performance of *AccessAuth*.

Keywords: V2G, authentication, capacity, security.

1. Introduction

Vehicle-to-Grid (V2G) is a critical network service in the “Smart Grid” (the next-generation power grid) and is considered as one of the most powerful approaches for enabling renewable energy sources to provide ancillary electrical services and for managing and monitoring power usage [1–4]. A typical V2G network includes four main entities, electric vehicles (*EVs*), local aggregators (*LAGs*), certification authorities (*CAs*) and a control center (*CC*). Without loss of generality, *EVs* can be either power consumers or providers; they may belong to a specific group and have corresponding group attributes. The *LAGs* are the service access points for power and wireless communications for *EVs*. The *CAs* are trusted entities that belong to different independent institutions. They maintain secure databases containing detailed power and other information about various certified *EVs* and *LAGs*. Specifically, the components *Profiles Repository*, *Policies Repository* and *Access List* are included in a *CA*. The *Profiles Repository* is composed of the certified *EVs* and *LAGs* as well as their profiles (e.g., their attributes and personal information). The *Policies Repository* is a collection of various policies for available access resources. The *Access List* maintains information about authorized *EVs*. Finally, the *CC* acts as the only entity trusted by all the other entities in the entire V2G network environment.

*Corresponding author: mx.dong@csse.muroran-it.ac.jp

Email addresses: ming.tao@mail.scut.edu.cn (Ming Tao), ota@csse.muroran-it.ac.jp (Kaoru Ota), mx.dong@csse.muroran-it.ac.jp (Mianxiong Dong), qzz@nju.edu.cn (Zhuzhong Qian)

24 To implement the exchange of power and data, the V2G network employs a two-way communication
25 infrastructure. The power links are deployed to charge the batteries of *EVs* by consuming power from the
26 smart grid. They are also able to discharge stored power back to the smart grid. A variety of wireless/wired
27 communication technologies are integrated to support communications between the entities involved in
28 exchanging power-related data. Using this network architecture, an *EV* not only can replenish its power
29 from or discharge unused stored power back to the connected *LAG* but also apply for data services via the
30 *LAG*. Moreover, in a V2G network domain, a number of *LAGs* can be connected to a *CA* based on the
31 capacity of the *CA* to handle the *EVs*' access requests. Due to the inherent mobility of *EVs*, when an *EV*
32 is connected to a *LAG* serving as its default access point for power and wireless communication, we say
33 that the *EV* is working in its "home mode." in contrast, when an *EV* is temporarily connected to a *LAG*
34 managed by a different independent institution, we say that the *EV* is working in "visiting mode" [5].

35 Note that, given these characteristics (e.g., vehicle location and mobility, charging and discharging op-
36 tions, driving patterns and preferences, limited communication range, etc.), V2G networks are different from
37 other broadly applied communications systems. Although V2G technology is considered a critical part of
38 the future "Internet of Energy" [6, 7], to the best of our knowledge, it is still a very young research field.
39 Fortunately, promoted by advances in emerging IoT technology, V2G systems in the smart grid that fit into
40 the broader concept of federated IoT promise a future in which a multitude of physical objects and devices
41 within the V2G networks will be connected to the Internet to create smart environments. These objects and
42 devices are expected to carry embedded computer intelligence that will allow them to connect, cooperate,
43 and communicate within social, environmental and user contexts to achieve better power-load manage-
44 ment and improved power efficiency and reliability. Hence, V2G is also a special type of cyber-enabled
45 application [8, 9].

46 Although the IoT paradigm is a valuable addition for controlling and managing energy appliances in V2G
47 networks, the adopted network infrastructure suffers from a variety of serious security challenges [10–14],
48 and the range of possible security attacks has still not been well investigated; consequently, security and
49 privacy issues remain particularly problematic. Specifically, mutual authentication mechanisms between the
50 *EVs* and the associated *LAGs* are imperative and must be provided to ensure legitimate communications.
51 Moreover, data exchanged between the *EVs* and other entities involved in V2G networks must be secured,
52 data privacy must be preserved throughout the network, and the *LAGs* must be prevented from recognizing
53 and tracing the identities and behavior preferences of the *EVs* they serve. Therefore, to address these
54 security and privacy concerns, this paper proposes *AccessAuth* and offers the following main contributions.

55 1. On the basis of a thorough discussion of the issues of efficiently maintaining security and privacy,
56 which must be achieved in the access authentication mechanisms used by federated-IoT-enabled V2G net-
57 works, *AccessAuth*, a lightweight protocol for capacity-based security access authentication with conditional
58 privacy, is proposed.

59 2. In *AccessAuth*, by considering the overload probability and system capacity constraints of the V2G
60 network domain as well as the mobility and session characteristics of *EVs*, a capacity-based active access
61 admission control scheme is developed to reduce the session-dropping probability (SDP) and the session-
62 blocking probability (SBP) for access requests. Concretely, the ideal number of admissible access requests
63 is adaptively calculated for the V2G network domain using a Markov model. This ideal number can be used
64 to determine whether the V2G network domain will admit a new access request.

65 3. Subsequently, when an access request is admissible for a V2G network domain, by considering whether
66 prior knowledge of the trust relationship exists between the relevant V2G network domains, a high-level au-
67 thentication model with specific authentication procedures is presented that provides mutual authentication
68 while maintaining the data privacy of admitted sessions by ensuring that only authorized sessions can be
69 conducted.

70 4. Within the framework of *AccessAuth*, efficient session revocation with forward security and session
71 recovery that involve no extra authentication delay are also discussed.

72 The remainder of this paper is organized as follows. Section 2 discusses security and privacy issues
73 and provides a review of current research achievements. Section 3 presents a concrete implementation and
74 discussion of *AccessAuth*. Section 4 demonstrates the performance of *AccessAuth* through both analysis
75 and evaluation results. Finally, we summarize and conclude this paper in Section 5.

2. Security & Privacy Issues and Related Works

In V2G networks, security attacks and vulnerabilities suffered during power and data interactions can be categorized into three main types: data capture, data deception and data blocking [5]. Successful breaches will result in cascade effects with disastrous results. Therefore, designed access authentication protocols for V2G networks must address the following critical requirements to maintain security and privacy and to ensure authorized and reliable interactions among legal entities:

1) Mutual authentication, verification and their defense against attacks. Before initializing communications, *EVs* and *LAGs* should authenticate with each other to prevent *redirection*, *impersonation*, and other types of attacks. Verifying that *LAGs* offering access services are authorized by the *CAs* is critical to prevent a disguised *LAG* from disclosing private information acquired from carelessly connected *EVs*. Additionally, the designed access authentication protocols must be able to overcome various types of well-known, feasible security attacks.

2) Session key establishment. Data transmitted over V2G networks should be protected against illegal entities to ensure data confidentiality and against unauthorized manipulation and destruction to ensure data integrity. Adversaries should not be given opportunities to intrude on established communication sessions and perform a variety of malicious activities such as eavesdropping, data tampering, disseminating harmful data, and so forth.

3) Strong anonymity and untraceability of *EVs*. Private information concerning *EVs*, such as their battery status, behavior preferences, and so on, should not be disclosed during the authentication process to help protect against misuse of this information by *insider* attacks.

4) Conditional privacy preservation. As part of the strong anonymity and untraceability of *EVs*, their location information should not be associated with their identities as they roam between different V2G networks. However, in emergency situations, the *CAs* and the *CC* are responsible for interrogating the related private information of *EVs* (e.g., their identities and locations).

5) Anonymity for *CAs* and the *CC*. The identities of *CAs* and the *CC* must also be hidden from unauthorized entities; otherwise, domino effects may occur. For example, eavesdroppers or adversaries could conduct traffic analyses to reveal private information about *EVs*.

6) Low computational load and communication overhead. Because huge numbers of entities will participate in these future V2G networks, the overhead generated during access authentication (e.g., computation and communication) must be minimized, and the delay due to authentication should be small enough so that the system can respond quickly to *EVs*' access requests.

Currently, an extensive body of research exists that focuses on security and privacy issues in V2G networks. Based on discussions of V2G network architectures and the state-of-the-art security challenges faced during power and communication interactions, Zhang et al. [5] proposed a context-aware authentication solution that considers battery statuses and their roles. *EV* batteries may exist in different states (e.g., charging, fully charged and discharging) during communication interactions. Zhang et al. [15] proposed a battery-status-aware authentication scheme (BASA) by identifying unique security challenges relevant to an *EV*'s various battery states and considering that an *EV* may have a variety of roles (e.g., energy demand, energy storage or energy supply). Zhang et al. [16] also proposed a role-dependent privacy preservation scheme (ROPS) by demonstrating that dissimilar security and privacy concerns exist. By exploiting a fuzzy identity-based encryption method with lattice-based access control and dedicated error-correction coding, Wu et al. [17] proposed a dedicated data access authentication scheme able to enforce fine-grained access authentication that resists corruption from noisy channels and environmental interference. To address the issue that most current identity authentication (IA) schemes and technologies face various kinds of attacks and large-scale certification problems, Xu et al. [18] proposed the HyCPK, which is an improved CPK algorithm based on a single-double hybrid matrix.

Because mobility is an important characteristic of V2G networks, an *EV* may work in different modes (e.g., home mode and visiting mode), causing security and privacy issues to become even more challenging due to the untrusted entities in visiting mode. By employing a bilinear pairing technique with an accumulator and performing batch verification, Saxena et al. [19] proposed a mutual authentication scheme to preserve the privacy of *EVs* working in different modes. Considering that *EVs* present different security

127 challenges in different modes, Liu et al. [20] proposed an aggregated-proofs based privacy-preserving authentication scheme (AP3A) to achieve simultaneous identification and secure identification. In mobile networks
128 that employ smart grids, it is widely accepted that Demand-Response (DR) techniques help in improving
129 efficiency, reliability and security. However, the security requirements of different DR events (e.g., security
130 access service, security communication service and security analysis service) are dynamic for various practical
131 demands. To address this issue, Guo et al. [21] proposed an event-oriented dynamic security service
132 mechanism for DR that dynamically composites the above three types of security services into fine-grained
133 subservices. Also, considering the communications characteristics among *EVs*, Guo et al. [22] proposed a
134 unique batch authentication protocol named UBAPV2G, in which, rather than verifying each message for
135 each individual *EV*, the aggregator checks the responses from a batch of *EVs* using only one signature
136 verification and then broadcasts a signed confirmation message to inform the batch of *EVs* using only one
137 signature.

138
139 Similarly, based on previously identified emerging privacy issues in V2G networks, Yang et al. [23]
140 considered the trade-off between the rewards obtained by the *EVs* and the financial benefits obtained by
141 the power grid and proposed a privacy-preserving communication and precise reward architecture for V2G
142 networks. In this approach, an *ID*-based blind signature is introduced to enhance anonymity. Wang et
143 al. [24] enhanced Yang et al.'s framework with formal definitions of unforgeability and restrictiveness and
144 proposed a new traceable privacy-preserving communication and precise reward scheme using available
145 cryptographic primitives. Generally, in V2G networks, multiple levels of charging services must be provided
146 for *EVs*; therefore, some private information of *EVs* may be disclosed to determine the charging service
147 quality. He et al. [25] proposed a privacy-preserving multi-quality charging (PMQC) scheme, in which
148 both authentication and an evaluation that determines the charging service level that can be offered to
149 *EVs* are efficiently achieved without revealing private information. Considering several security concerns
150 such as identity-irrelevant location privacy, frequent authentication for *EVs*, and the confidentiality and
151 integrity of the exchanged electricity trade data, Abdallah et al. [26] proposed a lightweight, secure and
152 privacy-preserving V2G connection scheme. However, the maintained traces for accountability and electricity
153 exchange operations also result in a large risk of exposing the private information of *EVs* to eavesdroppers
154 and adversaries.

155 To establish a session key built on an elliptic curve cryptography-based restrictive partially blind signature,
156 a security and privacy-preserving mechanism for aggregator-based V2G networks was proposed in [27];
157 however, in this scheme, the *EVs* must open their accounts at the *LAGs*, which increases the risk of *insider*
158 attacks. Additionally, by utilizing a restrictive partially blind signature to protect *EV*'s identities and certificateless
159 public key cryptography to simplify the certificate management required by traditional public key
160 infrastructure (PKI) and to overcome the key escrow problem in identity-based public key cryptography, T-
161 seng [28] proposed a secure and privacy-preserving communication protocol for V2G networks. In contrast,
162 Vaidya et al. [29] analyzed the shortcomings of using traditional PKI for V2G networks and proposed a
163 multi-domain PKI model built on elliptic curve cryptography along with a self-certified public key technique
164 that uses implicit certificates.

165 While acknowledging the proposals in the literature that have been found to be efficient, each still has
166 some limitations. For example, some generate additional overhead [19–22], and some present practical
167 solutions to only some of the well-known security concerns [5, 15–18, 23–29]. To the best of our knowledge,
168 the challenges of security and privacy in V2G networks must still be investigated to a much greater extent
169 to achieve an optimal balance of performance and security.

170 **3. AccessAuth: The Proposed Protocol**

171 *3.1. Capacity-based Active Access Admission Control*

172 In a typical federated-IoT-enabled V2G network domain, the *LAG* needs to communicate with the
173 external network on behalf of active sessions triggered by authorized *EVs*. The logical positions of *LAGs*
174 will determine whether they are potential forwarding efficiency bottlenecks in network communications.
175 Additionally, objects (e.g., *EVs*) served within a V2G network domain also need to communicate with each

176 other; consequently, the scarcity of available spectrum bandwidth will be another communication bottleneck.
 177 To guarantee the Quality of Service(QoS) of active sessions and provide adequate services for new access
 178 requests—including both migrated sessions and newly initiated access requests triggered by the *EVs*—we
 179 propose a capacity-based active access admission control scheme in which each *LAG* in the V2G network
 180 domain will periodically analyze the arrival rate of new access requests, the probability of migration, and the
 181 probability of active session termination and, finally, obtain the ideal number of admissible access requests
 182 during the current period. The results of these calculations will be used to determine whether new access
 183 requests should be admitted. The pseudocode for the proposed capacity-based active access admission
 184 control scheme is shown in Algorithm 1.

Algorithm 1 Capacity-based active access admission control

Input: for the i -th V2G network domain, N_i^{new} : the number of admitted newly initiated access request-
 s; $N_i^{accessed}$: the number of accessed sessions; $N_i^{capacity}$: the capacity limitation of served sessions;
 $N_i^{admissible}$: the ideal number of admissible newly initiated access requests.

Output: The admissible new access requests.

```

/* at time  $t$  */
/* admission for a migrated session */
1: if ( $N_i^{accessed} + 1 \leq N_i^{capacity}$ ) then
2:   admissible;
3:    $N_i^{accessed}++$ ;
4: else
5:   reject;
6: end if
/* admission for a newly initiated access request */
7: if ( $(N_i^{new} + 1 \leq N_i^{admissible}) \ \& \ (N_i^{accessed} + 1 \leq N_i^{capacity})$ ) then
8:   admissible;
9:    $N_i^{new}++$ ;
10:   $N_i^{accessed}++$ ;
11: else
12:   reject;
13: end if

```

185 From Algorithm 1, to enhance the systemic benefit of a V2G network domain, we assume the processing
 186 capacity of the V2G network domain as a constraint and enable as many admissible new access requests as
 187 possible to reduce the SDP for migrating sessions while maintaining a low SBP for newly initiated sessions.
 188 To this end, Algorithm 1 is intended to obtain the defined $N_i^{admissible}$ and is solved as follows. Note that
 189 the performance loss resulting from dropping an ongoing session is more serious than that from blocking an
 190 attempt to initiate a new session; therefore, we assign higher admission priorities to migrating sessions than
 191 to newly initiated sessions.

192 Before stating specifically how Algorithm 1 calculates $N_i^{admissible}$, we must provide some definitions.
 193 First, we assume that $\vec{S} = \{S_1(t), S_2(t), \dots, S_n(t)\}$ is the systemic state vector of all V2G network do-
 194 mains, where $S_i(t)$ is the number of sessions being served in the i -th V2G network domain at time t , and
 195 $S_i(t) \geq 0$ ($i = 1, 2, \dots, n$, n is the number of V2G network domains in a federated-IoT-enabled V2G net-
 196 work environment, $t = 0, 1, 2, \dots$). Here, $MS = \{ms_{ij}(t)\}_{n \times n}$ is a matrix of migrated sessions, and $ms_{ij}(t)$
 197 ($0 \leq ms_{ij}(t) \leq 1$, $i, j = 1, 2, \dots, n$, $t = 0, 1, 2, \dots$) is the probability of a session migrating from the i -th
 198 V2G network domain to the j -th one, which can be calculated by the ratio of the number of migrated
 199 sessions to the total number of sessions served by the i -th V2G network domain. Note that data about
 200 migrated sessions, including their mobility and session characteristics, will be periodically collected by the
 201 *CA* deployed in each V2G network domain and used to generate the matrix MS at the current moment.
 202 The vector of terminated sessions is $\vec{T}S = \{ts_1(t), ts_2(t), \dots, ts_n(t)\}$ in all V2G network domains at time
 203 t , where $ts_i(t)$ ($0 \leq ts_i(t) \leq 1$, $i = 1, 2, \dots, n$, $t = 0, 1, 2, \dots$) denotes the probability of a session being

204 terminated in the i -th V2G network domain. That value can also be calculated using the ratio of the num-
 205 ber of terminated sessions to the total number of sessions served by the i -th V2G network domain. The
 206 vector $\vec{N}_{admissible} = \{N_1(t), N_2(t), \dots, N_n(t)\}$ represents the ideal number of newly initiated access requests
 207 admissible by all the V2G network domains at time t , and $N_i(t)$ ($N_i(t) \geq 0$) is the factor that determines
 208 whether new access requests are admitted.

209 Based on the above definitions, at time $t + \varepsilon$, the number of sessions being served in the i -th V2G network
 210 domain can be deduced using the Markov model as shown in Eq. (1):

$$S_i(t + \varepsilon) = S_i(t) - S_i(t) \cdot ts_i(t) - \sum_{\substack{j=1 \\ j \neq i}}^n ms_{ij}(t) \cdot S_i(t) + N_i(t) + \sum_{\substack{j=1 \\ j \neq i}}^n ms_{ji}(t) \cdot S_j(t). \quad (1)$$

211 For convenience, we assume that $\sum_{\substack{j=1 \\ j \neq i}}^n ms_{ij}(t) + ts_i(t) = 1$; therefore, Eq.(1) can be simplified to Eq. (2):
 212

$$S_i(t + \varepsilon) = \sum_{\substack{j=1 \\ j \neq i}}^n ms_{ji}(t) \cdot S_j(t) + N_i(t). \quad (2)$$

213 Given the system's state \vec{S} at time t , if an $\vec{N}_{admissible}$ obtained according to MS could enable the
 214 systemic state at time $t + \varepsilon$ to approach the near-ideal one represented by \vec{S}^* , that is the final $\vec{N}_{admissible}$
 215 we expect. When the near-ideal state \vec{S}^* is obtained, the left side of Eq. (2) can be replaced by \vec{S}^* , and
 216 sequentially, $\vec{N}_{admissible}$ could be obtained as in Eq. (3).

$$\vec{N}_{admissible} = \vec{S}^* - \vec{S} \cdot MS. \quad (3)$$

217 Because the number of served sessions has a positive impact on the overall benefit of a V2G network
 218 domain, in the near-ideal state \vec{S}^* , the number of admissible sessions must be maximized within the afore-
 219 mentioned capacity limit. Accordingly, as shown in (4), we can deduce a formula to solve \vec{S}^* . Where
 220 $\vec{S}^* \geq \vec{S} \cdot MS$ is configured in terms of Eq. (3) to ensure $\vec{N}_{admissible} \geq 0$ in the near-ideal system state,
 221 $0 \leq S_i^* \leq N_i^{capacity}$ is introduced to constrain the number of served sessions to fewer than the capacity lim-
 222 it, and $p(S_i^*) \leq p_i^{overload}$ is introduced to constrain the current overload probability represented by $p(S_i^*)$
 223 to a value no greater than the threshold $p_i^{overload}$.

$$\begin{aligned} & \max \sum_{i=1}^n S_i^* \\ & \text{s.t. } 0 \leq S_i^* \leq N_i^{capacity} \\ & \quad \vec{S}^* \geq \vec{S} \cdot MS \\ & \quad p(S_i^*) \leq p_i^{overload}. \end{aligned} \quad (4)$$

224 As shown in (4), to solve \vec{S}^* , $p(S_i^*)$ must first be determined. Here, we partially refer to the method
 225 proposed in [30]. For the i -th V2G network domain, we assume that there are S_i^* served sessions at time
 226 t and that the arrival rate of newly initiated access requests follows a Poisson distribution with parameter
 227 λ_i and is represented by $p(N_i^{arrival} = k) = (\lambda_i^k / k!) \cdot e^{-\lambda_i}$. Additionally, at the end of time t , for each V2G
 228 network domain, the served sessions attached to the original V2G network domain but migrating to another
 229 V2G network domain all are independent events, and their properties correspond to a binomial distribution.
 230 Therefore, we assume that, following a binomial distribution, as shown in Eq. (5), the probability of served

231 sessions attached to the i -th V2G network domain is represented by $B(d_i, S_i^*, ms_{ii}(t))$, where $d_i = S_i^* \cdot$
232 $ms_{ii}(t)$ is the number of attached served sessions. Similarly, the probability of sessions served by the i -th V2G
233 network domain migrating to the j -th ($j \neq i$) V2G network domain is represented by $B(m_i, S_i^*, ms_{ij}(t))$,
234 where $m_i = S_i^* \cdot ms_{ij}(t)$, and the probability of sessions served by the j -th V2G network domain migrating to
235 the i -th V2G network domain is represented by $B(m_j, S_j^*, ms_{ji}(t))$, where $m_j = S_j^* \cdot ms_{ji}(t)$. Accordingly,
236 at the end of time t , there will be $N_i^{served} = d_i + k + \sum_{j=1, j \neq i}^n m_j$ sessions served by the i -th V2G network
237 domain, and the probability distribution of the number of served sessions, denoted as $p(N_i^{served})$, can be
238 represented by the convolution summation of $B(d_i, S_i^*, ms_{ii}(t))$, $p(N_i^{arrival} = k)$ and all $B(m_j, S_j^*, ms_{ji}(t))$.
239 According to the *central – limit theorem*, it is acceptable that $p(N_i^{served})$ can be further approximated by
240 the normal distribution as shown in (6).

$$B(d_i, S_i^*, ms_{ii}(t)) = C_{S_i^*}^{d_i} \cdot ms_{ii}(t)^{d_i} \cdot (1 - ms_{ii}(t))^{S_i^* - d_i} \quad (5)$$

$$p(N_i^{served}) \sim N \left(d_i + k + \sum_{j=1, j \neq i}^n m_j, \sqrt{d_i \cdot (1 - ms_{ii}(t)) + k + \sum_{j=1, j \neq i}^n m_j \cdot (1 - ms_{ji}(t))} \right) \quad (6)$$

$$\begin{aligned} p(S_i^*) &= \prod_{N_i^{served}=N_i^{capacity}+1}^{\infty} P(N_i^{served}) = 1 - \prod_{N_i^{served}=0}^{N_i^{capacity}} P(N_i^{served}) \\ &= 1 - \Phi \left(\frac{\left(N_i^{capacity} - (d_i + k + \sum_{j=1, j \neq i}^n m_j) \right)}{\sqrt{d_i \cdot (1 - ms_{ii}(t)) + k + \sum_{j=1, j \neq i}^n m_j \cdot (1 - ms_{ji}(t))}} \right) \end{aligned} \quad (7)$$

$$\begin{aligned} p(S_i^*) \leq p_i^{overload} &\Leftrightarrow p(S_i^*) - p_i^{overload} \leq 0 \\ \Leftrightarrow 1 - \Phi \left(\frac{\left(N_i^{capacity} - (d_i + k + \sum_{j=1, j \neq i}^n m_j) \right)}{\sqrt{d_i \cdot (1 - ms_{ii}(t)) + k + \sum_{j=1, j \neq i}^n m_j \cdot (1 - ms_{ji}(t))}} \right) &- (1 - \Phi(\beta_i)) \\ \Leftrightarrow \Phi(\beta_i) - \Phi \left(\frac{\left(N_i^{capacity} - (d_i + k + \sum_{j=1, j \neq i}^n m_j) \right)}{\sqrt{d_i \cdot (1 - ms_{ii}(t)) + k + \sum_{j=1, j \neq i}^n m_j \cdot (1 - ms_{ji}(t))}} \right) & \\ \Leftrightarrow \beta_i \cdot \sqrt{d_i \cdot (1 - ms_{ii}(t)) + k + \sum_{j=1, j \neq i}^n m_j \cdot (1 - ms_{ji}(t))} + \left(d_i + k + \sum_{j=1, j \neq i}^n m_j \right) - N_i^{capacity} &\leq 0 \end{aligned} \quad (8)$$

241 Accordingly, the current overload probability of the i -th V2G network domain can be defined in Eq. (7),
242 and it is further defined according to *Laplace's theorem*, where $\Phi(x) = \int_{-\infty}^x \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$. Note that,
243 without loss of generality, for the i -th V2G network domain, there will be only one given threshold $p_i^{overload}$
244 and $\exists \beta_i$, $p_i^{overload} = 1 - \Phi(\beta_i)$. Hence, as shown in (8), the configured constraint of $p(S_i^*) \leq p_i^{overload}$ can
245 be represented in another way.

246 Now, based on the finally defined $p(S_i^*)$, we can further obtain \vec{S}^* by solving (4) and, finally, obtain
247 the $\vec{N}_{admissible}$ through Eq. (3). By introducing the Metropolis rule of simulated annealing algorithm into
248 the particle swarm algorithm (SA-PSO), we can use the SA-PSO (which was developed in our previous

work [31]) to solve the optimization problem defined in (4). The specific implementation of the SA-PSO is available in [31]. For each V2G network domain, the elements in $\vec{N}_{admissible}$ are used as the basis for determining whether to admit a newly initiated access request at the current moment. As a reminder, after updating the MS in the next moment, the corresponding $\vec{N}_{admissible}$ must be recalculated to satisfy the new requirements of mobility and session triggered by the EV s and to maximize the entire systemic benefit under the constraints of capacity and overload probability.

3.2. Authentication Model

Based on this developed capacity-based active access admission control scheme, to maintain access security and conditional privacy in V2G networks when a new access request is admissible, a high-level authentication model is developed as shown in Fig. 1. In practice, in a federated-IoT-enabled V2G network environment, the certified EV s may consist of multiple groups with corresponding group attributes [32]. Specifically, the number of certified EV s in each group may be different, but these grouped EV s with distinctive (or identical) session characteristics are likely to have correlated mobility. To collectively provide access authentication for EV s in the same group, the existing authentication mechanisms (e.g., one-to-one authentication) have been shown to not only fail to fully use the group characteristics but also to cause significant system overhead and large (even unacceptable) authentication delay. Therefore, a secure and efficient group-based authentication mechanism must be employed in the developed authentication model.

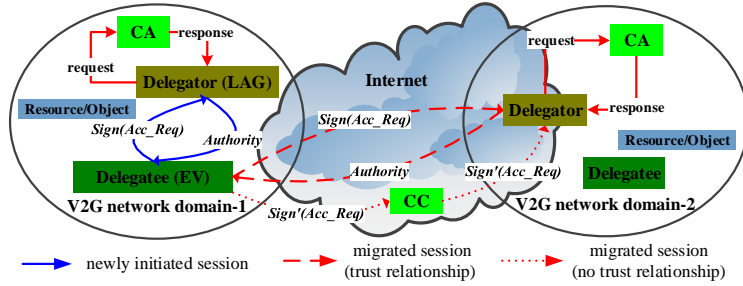


Figure 1: A high-level authentication model in a federated-IoT-enabled V2G network environment.

As shown in Fig. 1, a *Delegator(LAG)* is a delegation decision-making entity and a *Delegatee(EV)* is a delegation requestor entity. In the implementation of authority delegation for a newly initiated access request of EV , an access request from a *Delegatee* located in its default V2G network domain will be signed using a specific group-based signature scheme, e.g., a forward secure revocable group signature (FSR-GS), and forwarded directly to the default *Delegator*. Upon receiving the access request, the *Delegator* will validate the signature and evaluate the access request based on the combination of available rules and policies provided by the CA to determine whether to grant some or all of its authority to the *Delegatee*. If the verification result is positive, a corresponding response with the requested authority would be returned to the *Delegatee*; otherwise, an error message or a rejection decision would be returned.

In contrast, in the implementation of authority delegation for a migrating EV session, we will consider two different scenarios based on whether a trust relationship between the two relevant V2G network domains has been established. When a trust relationship between two V2G network domains has already been established through some mutual authentication scheme, the *Delegatee* located in V2G network domain-1 would sign the access request using FSR-GS and forward it directly to the *Delegator* in V2G network domain-2. Subsequently, the operations for authority delegation in this scenario would be the same as those performed for a newly initiated access request. When no prior trust relationship between the two V2G network domains exists, unlike the approach used for the first scenario, the signed access request would be forwarded to the *Delegator* through the CC , which is the only entity trusted by all other entities. Detailed explanations for the implementations of considered authority delegation are provided below.

3.3. Authentication Procedures

As stated above, FSR-GS will be employed as an important means for signing the access request in this work; therefore, we first review the definition of FSR-GS. As described in [33, 34], an FSR-GS is composed of several important probabilistic polynomial-time algorithms and an interactive mechanism, and it can be represented by a six-tuple $(G.Kg, G.Enroll, G.Revoke, G.Sign, G.Ver, G.Open)$. The concrete definitions and implementations of these tuples can be found in [33, 34]. Additionally, the entities participating in FSR-GS include a group manager, a group member and a verifier. For the considered scenarios of authority delegation in this work, the CC acts as the global group manager, and the CA in each V2G network domain acts as a local group manager; the former has a global master key pair (mPK_{CC}, mSK_{CC}) , and the latter has a local master key pair (mPK_{CA}, mSK_{CA}) . The certified $LAGs$ in each V2G network act as verifiers or *Delegators*. The two types of group managers and each LAG have signing and verification key pairs, respectively, represented by (PK_{CC}, SK_{CC}) , (PK_{CA}, SK_{CA}) and (PK_{LAG}, SK_{LAG}) and generated by a conventional digital signature scheme (e.g., the Elliptic Curve Digital Signature Algorithm (ECDSA)). Correspondingly, using $G.Kg$, the generated initial information of the group members (also called “signers”) managed by the global group manager and local group manager are represented by $\Omega_{CC} = (c_g, \mu_g)$ and $\Omega_{CA} = (c_l, \mu_l)$, respectively, where c_g and c_l are initialized to ‘ g_1 ’ and μ_g and μ_l are initialized to ‘1.’

During the setup phase of the federated-IoT-enabled V2G network environment, the CC announces its global master public key mPK_{CC} to all its group members, including the certified CAs , $LAGs$ and EVs , and the CA in each V2G network domain announces its local master public key mPK_{CA} to all its group members, including the certified $LAGs$ and EVs . In each V2G network domain, the ID_{CA} and PK_{CA} of the CA and the ID_{LAG} and PK_{LAG} of each LAG are publicly known to all the authorized accessors and to the EVs and CA in the other V2G network domains using an already established trust relationship. Additionally, each LAG shares a session key $Shared_Key(sess.)$ with its managing CA .

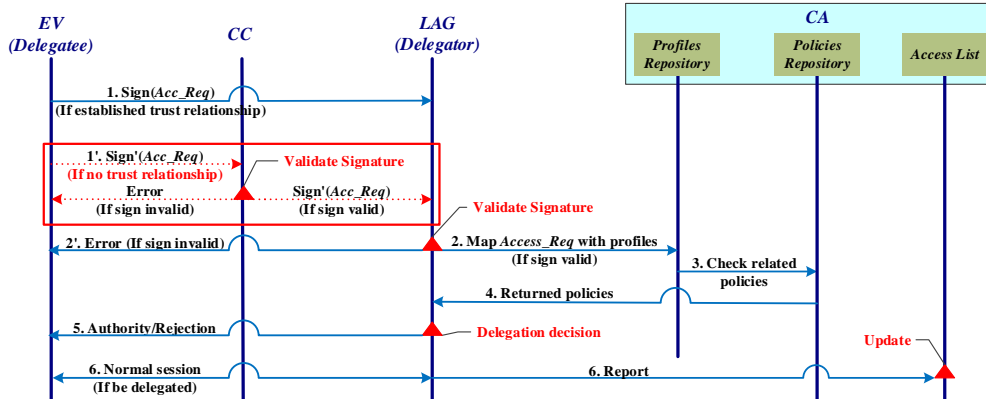


Figure 2: The overall framework for implementing considered authority authentication.

During the authentication phase of a new access request, the three scenarios, namely, i) authentication for a newly initiated access request, ii) authentication for a migrated session with established trust relationship, and iii) authentication for a migrated session without established trust relationship, will be discussed separately. The overall framework for implementing considered authority authentication is shown in Fig. 2.

i) When $Delegatee(i)$ makes a new access request, it must authenticate itself to the default CA through a direct interaction. The default CA will execute $G.Enroll$ to generate a signing key, $Key_i(sig.)$, a (public) membership key, $Key_i(mem.)$, and a revocation key, $Key_i(rev.)$, for $Delegatee(i)$. All these generated keys and PK_{CA} are sent to $Delegatee(i)$ using a secure transmission protocol. Upon receiving this required knowledge, $Delegatee(i)$ first chooses a random number ξ and a temporary identity $alias(VID)$ and then generates a group signature σ_i as shown in Eq. (9), where T is a timestamp added to defend against *replay* attacks, VID is defined as a tetrad $(ID, Profile, Context, Policy)$, ID is the unique identifier of the $Delegatee(i)$, $Profile$ refers to the $Delegatee(i)$'s profile (e.g., attributes and personal information), $Context$ refers to the

320 security contexts (e.g., trust level and authentication level) and other context considerations (e.g., battery
 321 status, working mode), and *Policy* is a set of policies associated with *Delegatee(i)*'s preferences or access
 322 permissions. Subsequently, by using the public key PK_{LAG} of the default *LAG*, *Delegatee(i)* encrypts
 323 the message $\{alias(VID), g^\xi, \sigma_i, T\}$ to produce an access request $AR_i = (alias(VID), g^\xi, \sigma_i, T)_{PK_{LAG}}$ and
 324 sends AR_i to the default *LAG*.

325 ii) When *Delegatee(i)* needs to migrate a session and the trust relationship between the two relevant
 326 V2G network domains has already been established, *Delegatee(i)* generates a group signature σ_i , as shown
 327 in Eq. (9), using the necessary knowledge provided by the target *CA* from the other V2G network domain,
 328 and subsequently produces an access request $AR_i = (alias(VID), g^\xi, \sigma_i, T)_{PK_{LAG}}$ using the target *LAG*'s
 329 public key PK_{LAG} . Then, it sends AR_i to the target *LAG*.

$$\sigma_i = G.Sign(mPK_{CA}, Key_i(sig.), Key_i(mem.), Key_i(rev.), \Omega_{CA}, alias(VID) || g^\xi || T) \quad (9)$$

330 iii) When *Delegatee(i)* needs to migrate a session and no trust relationship between the two relevant V2G
 331 network domains exists, *Delegatee(i)* must authenticate itself to the *CC* by a direct interaction. The *CC* will
 332 execute *G.Enroll* to generate $Key'_i(sig.)$, $Key'_i(mem.)$ and $Key'_i(rev.)$ for *Delegatee(i)*. All these generated
 333 keys and PK_{CC} are then sent to *Delegatee(i)* using a secure transmission protocol. Upon receiving this
 334 required knowledge, *Delegatee(i)* first chooses a random number ξ and a temporary identity, $alias(VID)$
 335 and then generates a group signature, σ_i , as shown in Eq. (10). Subsequently, by using the *CC*'s master
 336 public key, mPK_{CC} , *Delegatee(i)* encrypts the message $\{alias(VID), g^\xi, \sigma_i, T\}$ to produce an access request
 337 $AR_i = (alias(VID), g^\xi, \sigma_i, T)_{mPK_{CC}}$ and sends AR_i to the *CC*. Upon receiving the request AR_i , the *CC*
 338 uses its master private key mSK_{CC} to decrypt the request to obtain the secret message $\{alias(VID), g^\xi, \sigma_i, T\}$
 339 and executes *G.Ver* to check the validity of the group signature σ_i . If the message is invalid, the *CC* rejects
 340 the access request; otherwise, the *CC* uses the target *LAG*'s public key PK_{LAG} to re-encrypt the message
 341 $\{alias(VID), g^\xi, \sigma_i, T\}$, producing a new access request $AR'_i = (alias(VID), g^\xi, \sigma_i, T)_{PK_{LAG}}$. Finally, it
 342 sends AR'_i to the target *LAG*.

$$\sigma_i = G.Sign(mPK_{CC}, Key'_i(sig.), Key'_i(mem.), Key'_i(rev.), \Omega_{CC}, alias(VID) || g^\xi || T) \quad (10)$$

343 Upon receiving AR_i or AR'_i , the default/target *LAG* first decrypts the message using its private key
 344 SK_{LAG} to obtain the secret message $\{alias(VID), g^\xi, \sigma_i, T\}$. Then, it checks to ensure that the time-stamp
 345 T falls within the allowable time-scope by comparing it with the current time. When T is legitimate, it
 346 executes *G.Ver* to check the validity of the group signature σ_i . If the validation fails, the *LAG* replies with
 347 an error message rejecting the access request, either directly to *Delegatee(i)* or through the *CC*; otherwise,
 348 upon validation success, the *LAG* sends the message $\{alias(VID), g^\xi, \sigma_i, T\}$, encrypted by the defined
 349 shared session key $Shared_Key(sess.)$, to the managing *CA*. After receiving the message, the *CA* obtains
 350 the identity of AR_i by executing *G.Open*, which indicates that the *CA* can provide conditional privacy. Then,
 351 it invokes the deployed *Profiles Repository* to map the profiles of *Delegatee(i)* with VID . The mapped
 352 profiles of VID , together with the *Context*, are then sent to the *Policies Repository* to obtain the relevant
 353 disclosed policies, which are, finally, sent back to the *LAG*. After receiving the relevant policies, the *LAG* will
 354 combine them and decide whether to approve the authority authentication. When the decision is positive,
 355 the *LAG* chooses another random number ξ' , generates $\lambda' = ECDSA.Sign(SK_{LAG}, alias(VID) || g^\xi || g^{\xi'})$
 356 and then sends a message $\{g^{\xi'}, \lambda'\}$ to *Delegatee(i)* while, in parallel, it computes a session key, $Key(sess.) =$
 357 $(g^\xi)^{\xi'}$. Subsequently, it erases ξ' from its memory; otherwise, the access request would be rejected.

358 Upon receiving the message $\{g^{\xi'}, \lambda'\}$, *Delegatee(i)* will execute $ECDSA.Ver(PK_{LAG}, alias(VID) || g^\xi || g^{\xi'}, \lambda')$
 359 to verify the validity of λ' . If the result is '1', *Delegatee(i)* generates another session key $Key'(sess.) = (g^{\xi'})^\xi$

360 corresponding to $Key(sess.)$ and erases ξ from its memory. Subsequently, $Delegatee(i)$ will produce a ses-
 361 sion $S_i = (alias(VID)\|g^\xi\|g^{\xi'})_{Key'(sess.)}$ through symmetric encryption, which is then sent to the LAG .
 362 Upon receiving the message, the LAG will decrypt it using $Key(sess.)$ and check its validity. If it is valid,
 363 the LAG concludes that $Delegatee(i)$ has established a session key and proceeds with a normal session;
 364 otherwise, the access request is rejected. Finally, when the access request is accepted, a report is sen-
 365 t to the CA to update the *Access List*. The membership information of the CA should be updated as
 366 $\Omega_{CA} = (c_l^{Key_i(mem.)}, \mu_l \cdot Key_i(mem.))$.

$$\Omega_{CA} = \left(c_l^{\left(\prod_{j=k}^n Key_j(rev.) \right) / Key_i(rev.)}, \mu_l \cdot \left(\prod_{j=k}^n Key_j(rev.) \right) / Key_i(rev.) \right) \quad (11)$$

367 3.4. Discussions of Session Revocation and Recovery

368 In a real world application, within a period of time after the delegation, the sessions of some EVs may
 369 expire or some EVs may want to suspend their session services for some amount of time according to plans
 370 made in advance.

371 For the former case, because the expiration time of the session for an accessed $Delegatee(i)$ is registered
 372 in the *Access List* of the serving CA , after the registered expiration time of $Delegatee(i)$ has elapsed, the
 373 assigned signing key $Key_i(sig.)$ is invalidated from then on. The serving CA should remove $Delegatee(i)$
 374 and execute $G.Revoke(mPK_{CA}, Key_i(rev.), \Omega_{CA})$ to update the membership information. The updated
 375 membership information is denoted as $\Omega_{CA} = (c_l^{Key_i(rev.)}, \mu_l \cdot Key_i(rev.))$. Note that in *AccessAuth*, to
 376 ensure forward security for session revocation, the anonymity of the revoked session's protocol must be
 377 executed before the revocation such that eavesdroppers or adversaries cannot correlate the revoked session
 378 and derive previous or subsequent interrogations.

379 For the latter case, when $Delegatee(i)$ wishes to reactivate a suspended session, the registering CA is
 380 generally required to execute $G.Enroll$ to generate new keys (e.g., $Key'_i(sig.)$, $Key'_i(mem.)$ and $Key'_i(rev.)$)
 381 for $Delegatee(i)$ and then re-invoke the authentication procedure described above. Obviously, this approach
 382 imposes additional authentication overhead and greatly increases the authentication delay. To overcome
 383 the shortcomings of this inconvenient approach, *AccessAuth* still uses the previously assigned keys. We as-
 384 sume that, at the time when $Delegatee(i)$ wishes to reactivate its session service, the session represented by
 385 $\{S_k, \dots, S_n\}$ (the session for $Delegatee(i)$, $S_i \in \{S_k, \dots, S_n\}$) has been revoked, and the current membership in-
 386 formation is represented by $\Omega_{CA} = \left(c_l^{\prod_{j=k}^n Key_j(rev.)}, \mu_l \cdot \prod_{j=k}^n Key_j(rev.) \right)$. Therefore, when $Delegatee(i)$
 387 wishes to recover its session service, we need only update the membership information as shown in Eq. (11).
 388 In this way, $Delegatee(i)$ can automatically reactivate its previous session.

389 4. Performance-Security Trade-off

390 4.1. Proofs of Security & Privacy Requirements

391 This section analyzes *AccessAuth* with respect to the critical security and privacy preservation require-
 392 ments listed in Section 2.

393 1) Mutual authentication, verification and their defense against attacks. Regardless of whether a trust
 394 relationship has been established between two relevant V2G networks, the authentication procedures in
 395 *AccessAuth* allow only a legitimate EV in the networks to generate a valid group signature based on the
 396 keys generated by $G.Enroll$ and the membership information Ω . Subsequently, authentication of the target
 397 LAG is achieved by responding with the message $\{g^{\xi'}, ECDSA.Sign(SK_{LAG}, VID\|g^\xi\|g^{\xi'})\}$. Using that
 398 message, the EV can determine the identity of the target LAG and proceed with a normal session. Therefore,
 399 *AccessAuth* satisfies the requirement of mutual authentication.

400 Additionally, during the setup phase of the federated-IoT-enabled V2G network environment, only the
 401 *CA* can generate valid certificates—including ID_{LAG} and PK_{LAG} —for the target *LAG*. Consequently,
 402 other *LAGs* or illegal entities cannot eavesdrop using different *IDs* and public keys. Therefore, we can
 403 conclude that *AccessAuth* also satisfies the verification requirement.

404 Moreover, *AccessAuth* can prevent various types of well-known security attacks. For example, the
 405 temporary identity *alias* introduced for *EV* and the generated shared secret authentication and session keys
 406 efficiently defeat *impersonation* and *repudiation* attacks. Similarly, because adversaries cannot decrypt
 407 encrypted messages with the private key owned only by the certified entity in the communication, *Man –*
 408 *In – The – Middle(MITM)* attacks can also be defeated. Because the shared secret keys for ongoing
 409 sessions are different and are regenerated for newly initiated sessions, the well-known key attacks can also
 410 be prevented. Finally, the timestamp T added to the generated group signature during the authentication
 411 procedure can defeat *replay* and *injection* attacks, and because the *CA* maintains conditional privacy, the
 412 identity and location of an *EV* can be verified to resist *redirection* attacks.

413 2) Session key establishment. Session keys (e.g., $Key(sess.)$ and $Key'(sess.)$) generated by challenge-
 414 response ($g^\xi, g^{\xi'}$) are used as shared secret keys for each authority between the *EV* and *LAG* within the
 415 whole expiry period. Thus, data confidentiality and integrity in the sessions can be ensured.

416 3) Strong anonymity and untraceability of *EVs*. In the authentication procedures described for *AccessAuth*,
 417 the *EV* creates a temporary identity *alias*, and the FSR-GS is used to sign the access request with the *alias*.
 418 Thus, during an ongoing authentication and session, the *EVs* private information is effectively protected,
 419 even for revoked sessions. Because an *EV* will apply for the next session using a new *alias(VID)*, eavesdrop-
 420 pers or adversaries will be unable to correlate the sessions and derive previous or subsequent interrogations,
 421 as described in detail for FSR-GS in [33, 34].

422 4) Conditional privacy preservation. In an emergency, the identities and locations of *EVs* must be able
 423 to be interrogated. In the authentication procedures described for *AccessAuth*, only the *CA* can obtain this
 424 private information by executing *G.Open*, indicating that conditional privacy can be preserved.

425 5) Anonymity for *CAs* and the *CC*. In the authentication procedures described for *AccessAuth*, an
 426 access request triggered by an *EV* is encrypted by the PK_{LAG} of the target *LAG*. Only the target *LAG*
 427 can use its SK_{LAG} to decrypt and obtain either the secret message or the identity of the registering *CA*
 428 or *CC*; consequently, the identity of the registering *CA* or *CC* is hidden from all legal and illegal entities
 429 except the visited *LAG*. Thus, the anonymity of both the *CAs* and the *CC* can be guaranteed.

430 4.2. Performance Analysis and Evaluation

431 To numerically analyze and evaluate the performance of *AccessAuth*, we consider a federated-IoT-enabled
 432 V2G network environment including four V2G network domains. First, to evaluate the capacity-based active
 433 access admission control scheme, we conducted a simulation using the MATLAB 2012a platform. The
 434 relevant performance characteristics of the executing host were as follows: a 64-bit Windows 7 operating
 435 system and an Intel(R) Core(TM) i5-3450 CPU running at 3.10 GHz with 4 GB of RAM. In the simulations,
 436 the initial number of served sessions in each V2G network domains was set to 100, the capacity limit of
 437 each V2G network domain was set to $N_i^{capacity} = 200$ ($i = 1, 2, 3, 4$), the time period ε was set to $\varepsilon = 60s$,
 438 and the session migration probability matrix during the time period was assumed to consist of three cases:

$$439 \text{ Case 1: } MS = \begin{bmatrix} 0.6 & 0.15 & 0.05 & 0 \\ 0.15 & 0.6 & 0.15 & 0.05 \\ 0 & 0.15 & 0.65 & 0.15 \\ 0.05 & 0.15 & 0.6 & 0.15 \end{bmatrix}; \text{ Case 2: } MS = \begin{bmatrix} 0.8 & 0.05 & 0.1 & 0 \\ 0.05 & 0.75 & 0.05 & 0.05 \\ 0 & 0.05 & 0.8 & 0.1 \\ 0.05 & 0.05 & 0.7 & 0.1 \end{bmatrix}; \text{ and Case 3:}$$

$$440 MS = \begin{bmatrix} 0.6 & 0.05 & 0.1 & 0 \\ 0.05 & 0.6 & 0.05 & 0.05 \\ 0.1 & 0.05 & 0.6 & 0.05 \\ 0 & 0.7 & 0.05 & 0.05 \end{bmatrix}. \text{ The corresponding vectors of session termination probability during}$$

441 the time period were $\vec{TS} = \{0.2, 0.05, 0.05, 0.05\}$, $\vec{TS} = \{0.05, 0.1, 0.05, 0.1\}$ and $\vec{TS} = \{0.25, 0.25, 0.2, 0.2\}$,
 442 respectively. Note that the configurations for the three cases were chosen randomly, but the session migration
 443 probability and the session termination probability vary considerably across the different scenarios.

444 Fig. 3 shows the impact of overload probability on the average ideal number of admissible sessions in
 445 the V2G network environment. We can clearly see that the ideal number of admissible sessions gradually
 446 increases as the overload probability limit increases. Nevertheless, even when using the same overload prob-
 447 ability limit for different cases of MS , the ideal number of admissible sessions will be different. Concretely,
 448 in Case 1, the average probability of session migration is greater; therefore, the ideal number of admissible
 449 sessions must be reduced to avoid migrated and newly initiated sessions arriving in great numbers in the
 450 V2G network, causing the overload probability to increase beyond the given limit. In Case 3, the average
 451 probability of session termination is greater, which means those session durations are relatively short. There-
 452 fore, the ideal number of admissible sessions can be increased—without negatively impacting the overload
 453 probability. In Case 2, because the average probabilities of session migration and termination fall between
 454 the preceding two cases, the ideal number of admissible sessions at the same overload probability limit lies
 455 in the middle as well.

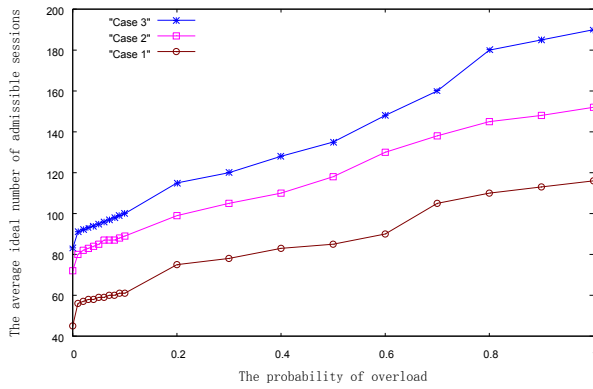


Figure 3: The impact of overload probability on the average ideal number of admissible sessions in the V2G network environment.

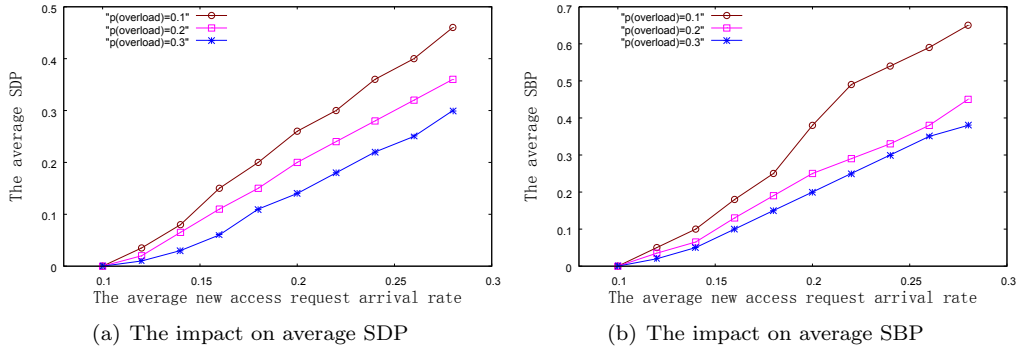


Figure 4: The impact of overload probability on average SDP and SBP in the V2G network environment.

456 Using Case 2 (the intermediate-level performance case) as an example, but with a different average new
 457 access request arrival rate, Fig. 4 shows the impact of overload probability on the average migrated session-
 458 dropping probability (SDP) and average newly initiated session-blocking probability (SBP) by the averaged
 459 results over 500 time periods of ϵ . When the overload probability limit is fixed, when the average new
 460 access request arrival rate increases, both the average SDP and average SBP gradually increase because of
 461 the limited number of admissible new access requests. However, as the overload probability limit increases,
 462 the ideal number of admissible newly initiated access requests, $N_i^{admissible}$, computed by Eq. (3) will also
 463 increase. Consequently, the number of admissible new access requests in the V2G network environment will
 464 increase as well. Thus, the average SDP and average SBP are gradually reduced. Note that the performance

465 penalty for dropping an ongoing session is more serious than that for blocking a newly initiated session;
 466 therefore, higher admission priorities are assigned to migrated sessions than to newly initiated sessions, and
 467 the reduction in average SDP is greater.

468 Using Case 2 as an example with the same configuration as in the former experiment and a fixed overload
 469 probability $p(\text{overload}) = 0.2$, Fig. 5 shows the performance of system utilization in terms of the average
 470 number of sessions served in the created federated-IoT-enabled V2G network environment. The NOA-GM
 471 that we proposed in [35] and the method proposed in [36] were selected for comparison. The method in [36]
 472 was developed based on MIR (Mobile IP Reservation Protocol), in which, if the network load is lower
 473 than a pre-defined threshold, both migrated sessions and newly initiated access requests are admissible;
 474 otherwise, newly initiated access requests would be blocked. The NOA-GM first periodically evaluates the
 475 load status of the access networks using the proposed dynamic weighted load evaluation algorithm to identify
 476 candidate underloaded access networks. Then, it achieves the optimal results by evaluating the candidates
 477 using normalized models of objective and subjective metrics. From Fig. 5, in the proposed method, as the
 478 average new access request arrival rate increases, the average number of served sessions in the proposed work
 479 experiences a steady increase based on the previously demonstrated performance concerning the average ideal
 480 number of admissible sessions, the average SDP, and the average SBP. In the NOA-GM and the method
 481 in [36], when the average new access request arrival rate is relatively low, the average SBP and SDP in
 482 some time periods of ε may be low due to the fixed pre-defined threshold; therefore, the average number
 483 of served sessions gradually increases. However, as the average new access request arrival rate increases,
 484 the average SBP and SDP may be high due to the fixed pre-defined threshold, which adversely affects the
 485 average number of served sessions.

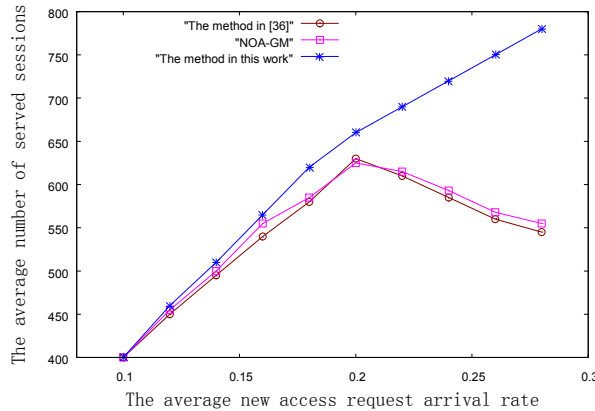


Figure 5: The performance of system utilization.

486 In addition, the performance of the authentication procedure of *AccessAuth* is analyzed and evaluated
 487 using two performance metrics: computational load and communication overhead. The scheme proposed
 488 in [19], the scheme named P^2 in [23], and the scheme in [28] are selected for comparisons. To achieve fair
 489 comparisons, all the compared schemes use the same experiment configuration. Concretely, the relevant
 490 performance parameters of entities involved in the V2G network environment, e.g., *EV*, *LAG*, *CA* and
 491 *CC*, are shown in Table 1, and the time costs of the primitive cryptographic operations conducted on these
 492 entities (obtained by the *OpenSSL* library) are shown in Table 2. For the sake of convenience, the time
 493 costs of highly efficient operations such as hash functions, symmetric encryption/decryption, Auth.code
 494 (HMAC), and point addition are omitted because their contributions to the overall computational load are
 495 insignificant. In this comparison, n *EV*s simultaneously trigger access requests (in 40% of these triggered
 496 access requests, no prior trust relationship exists between the relevant V2G network domains). Comparisons
 497 of the computational loads and the communications overhead are shown in Table 3 and Table 4, respectively.

498 In Table 3, T_{EV} , T_{LAG} , T_{CA} and T_{CC} represent the computational load on a *EV*, *LAG*, *CA* and
 499 the *CC*, respectively. As Table 3 shows, when using *AccessAuth*, if a trust relationship exists between the

Table 1: The relevant performance parameters of involved entities.

Entity	CPU	RAM	OS
<i>EV</i>	Qualcomm(R) Octa-core 1.5 GHz	2 GB	Android 4.2.2
<i>LAG</i>	Intel(R) Dual-core 3.1 GHz	4 GB	64-bit Win-7
<i>CA</i>	Intel(R) Hexa-core 1.6 GHz	16 GB	Win server 2012
<i>CC</i>	Intel(R) Hexa-core 1.6 GHz	16 GB	Win server 2012

Table 2: The time costs of the involved primitive cryptographic operations.

Entity	T_{SM} (ms)	T_{IO} (ms)	T_{EO} (ms)	T_{PO} (ms)
<i>EV</i>	0.54	0.33	0.5	16.6
<i>LAG</i>	0.36	0.33	0.38	11.5
<i>CA</i>	0.3	0.26	0.31	8.6
<i>CC</i>	0.3	0.26	0.31	8.6

T_{SM} : the time for a scalar multiplication operation;

T_{IO} : the time for an inverse operation;

T_{EO} : the time for a exponentiation operation;

T_{PO} : the time for a pairing operation;

relevant V2G network domains, the primitive cryptographic operations for a successful access authentication are conducted on the entities *EV*, *LAG* and *CA*; otherwise, a successful access authentication requires additional cryptographic operations on the *CC*. Overall, pairing operations are required in the compared schemes; however, *AccessAuth* instead takes greater advantage of scalar multiplication operations, which are much more efficient than pairing operations and result in much less computational load. Therefore, *AccessAuth* is more efficient than the compared schemes.

With respect to the communication overhead, a *CA* deployed in a V2G network domain is generally remotely connected with various *LAGs*; thus, we treat the communication overhead for transmitting an authentication message between a *LAG* and the *CA* as one unit and use it as a reference and criterion. The communication overhead between an *EV* and a *LAG* is assumed to be η ($0 < \eta < 1$). Similarly, because the *CC* is often located in a remote location in a V2G network environment, the communication overhead between the *CC* and a *EV* or a *LAG* can also be treated as one unit. In *AccessAuth*, when no prior trust relationship exists between relevant V2G network domains, the signed access request will be forwarded through the *CC*, which causes the total communication overhead to be $\eta + 5$ for a successful authentication; otherwise, the authentication request will be forwarded directly to the *LAG*, and a successful authentication requires a total communication overhead of $2\eta + 3$. Overall, as shown in Table 4, *AccessAuth* outperforms the compared schemes with respect to communication overhead. Because it achieves both computation and communication efficiency, *AccessAuth* has a more acceptable authentication delay; therefore, it is more suitable for practical application requirements.

Table 3: Comparisons of computational load.

Schemes	Computational load (ms)
scheme in [19]	$n \times (T_{EV} + T_{LAG} + T_{CA}) = n \times ((T_{PO} + 3T_{EO}) + (T_{PO} + 5T_{EO} + 6T_{SM}) + (3T_{EO} + 2T_{SM})) = n \times 35.19$
P^2 in [23]	$n \times (T_{EV} + T_{LAG} + T_{CA}) = n \times ((4T_{PO} + 9T_{EO} + 10T_{SM}) + (6T_{PO} + 6T_{EO} + T_{SM}) + (4T_{EO} + 5T_{SM})) = n \times 183.84$
scheme in [28]	$n \times (T_{EV} + T_{LAG} + T_{CA}) = n \times ((4T_{PO} + 9T_{EO} + 8T_{SM}) + (6T_{PO} + 2T_{EO} + T_{SM}) + (4T_{EO} + 3T_{SM})) = n \times 180.64$
<i>AccessAuth</i>	$0.4 \times n \times (T_{EV} + T_{CC} + T_{LAG} + T_{CA}) + 0.6 \times n \times (T_{EV} + T_{LAG} + T_{CA}) = 0.4 \times n \times ((3T_{SM} + 8T_{EO} + T_{IO}) + (T_{SM}) + (T_{IO} + 18T_{SM}) + (3T_{EO})) + 0.6 \times n \times ((3T_{SM} + 8T_{EO} + T_{IO}) + (T_{IO} + 18T_{SM}) + (3T_{EO})) = n \times 13.81$

Table 4: Comparisons of communication overhead.

Schemes	Communication overhead
scheme in [19]	$n \times (6\eta + 4)$
P^2 in [23]	$n \times (3\eta + 4)$
scheme in [28]	$n \times (4\eta + 5)$
<i>AccessAuth</i>	$0.4 \times n \times (\eta + 5) + 0.6 \times n \times (2\eta + 3)$

5. Conclusion

This paper addresses the security and privacy requirements for access authentication in a federated-IoT-enabled V2G network environment and proposes *AccessAuth* as a lightweight protocol for capacity-based security access authentication. The implemented capacity-based active access admission control scheme in *AccessAuth* was demonstrated to efficiently reduce the SDP for migrated sessions while maintaining a low SBP for newly initiated access requests. Moreover, the designed authentication model, which includes specific authentication procedures that consider whether prior trust relationships exist between the relevant V2G network domains, was shown to efficiently satisfy the critical security and privacy preservation requirements. Finally, analytical and evaluation results were used to demonstrate the performance of *AccessAuth* with regard to computational load and communication overhead. The results indicate that *AccessAuth* is more suitable for practical applications requirements than are previous approaches.

In the future, we plan to implement this protocol as middleware architecture in a federated-IoT-enabled V2G network environment to enhance its operating efficiency. Additionally, continuously improving this protocol to cope with emerging security and privacy concerns and some other open issues are directions we hope to explore further in future work.

Acknowledgments

This work is supported in part by the National Natural Science Fund, China (Grant No. 61300198); the Guangdong University Scientific Innovation Project (Nos. 2013KJJCX0177 & 2014KTSCX188); the outstanding young teacher training program of the Education Department of Guangdong Province (YQ2015158); Guangdong Provincial Science & Technology Plan Projects (No. 2016A010101035); and JSPS KAKENHI (Grant Nos. JP16K00117 and JP15K15976), KDDI Foundation.

References

- [1] S. Habib, M. Kamran, U. Rashid, Impact analysis of vehicle-to-grid technology and charging strategies of electric vehicles on distribution networks-A review, *J. Power Sources* 277 (3) (2015) 205–214.
- [2] M. Yilmaz, P. T. Krein, Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces, *IEEE Trans. Power Electron.* 28 (12) (2012) 5673–5689.
- [3] D. Q. Xu, J. Géza, M. Lévesque, M. Maier, Integrated V2G, G2V, and renewable energy sources coordination over a converged fiber-wireless broadband access network, *IEEE Trans. Smart Grid* 4 (3) (2013) 1381–1390.
- [4] M. Tao, K. Ota, M. Dong, Foud: Integrating fog and cloud for 5G-enabled V2G networks, *IEEE Netw.* 31 (2) (2017) 8–13.
- [5] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. T. Yang, M. Guizani, Securing vehicle-to-grid communications in the smart grid, *IEEE Wirel. Commun.* 20 (6) (2013) 66–73.
- [6] A. Mainetti, L. Palano, L. Patrono, M. Stefanizzi, R. Vergallo, P. Chu, R. Gadh, A new vehicle-to-grid system for battery charging exploiting IoT protocols, in: *IEEE International Conference on Industrial Technology (ICIT)*, IEEE, 2015, pp. 2154–2159.
- [7] N. Bui, A. P. Castellani, P. Casari, M. Zorzi, The internet of energy: A web-enabled smart grid system, *IEEE Netw.* 26 (4) (2012) 39–45.
- [8] H. Ning, H. Liu, J. Ma, L. T. Yang, R. Huang, Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology, *Future Gener. Comput. Syst.* 56 (2016) 504–522.
- [9] A. Rajhans, A. Bhave, I. Ruchkin, B. H. Krogh, D. Garlan, A. Platzer, B. Schmerl, Supporting heterogeneity in cyber-physical systems architectures, *IEEE Trans. Autom. Control* 59 (12) (2014) 3178–3193.
- [10] D. He, C. Chen, J. Bu, C. Sammy, Y. Zhang, M. Guizani, Secure service provision in smart grid communications, *IEEE Commun. Mag.* 50 (8) (2012) 53–61.

- 561 [11] C. Bekara, Security issues and challenges for the IoT-based smart grid, *Procedia Comput. Sci.* 34 (2014) 532–537.
- 562 [12] T. H. Yuen, C. Zhang, S. S. Chou, S. M. Yiu, Related randomness attacks for public key cryptosystems, in: *ACM*
563 *Symposium on Information, Computer and Communications Security*, ACM, 2015, pp. 215–223.
- 564 [13] Z. Hao, S. Zhong, N. Yu, A privacy-preserving remote data integrity checking protocol with data dynamics and public
565 verifiability, *IEEE Trans. Knowl. Data Eng.* 23 (9) (2011) 1432–1437.
- 566 [14] B. Li, R. Lu, W. Wang, K.-K. R. Choo, Distributed host-based collaborative detection for false data injection attacks in
567 smart grid cyber-physical system, *J. Parallel Distrib. Comput.* 103 (2017) 32–41.
- 568 [15] H. Liu, H. Ning, Y. Zhang, M. Guizani, Battery status-aware authentication scheme for V2G networks in smart grid,
569 *IEEE Trans. Smart Grid* 4 (1) (2013) 99–110.
- 570 [16] H. Liu, H. Ning, Y. Zhang, Q. Xiong, L. T. Yang, Role-dependent privacy preservation for secure V2G networks in the
571 smart grid, *IEEE Trans. Inf. Forensics Secur.* 9 (2) (2014) 208–220.
- 572 [17] J. Wu, M. Dong, K. Ota, Z. Zhou, D. Bin, Towards fault-tolerant fine-grained data access control for smart grid, *Wirel.*
573 *Pers. Commun.* 75 (3) (2014) 1787–1808.
- 574 [18] G. Xu, Y. Ren, G. Zhang, B. Liu, X. Li, Z. Feng, HyCPK: Securing identity authentication in ubiquitous computing, in:
575 *IEEE 12th International Conference on Ubiquitous Intelligence and Computing and IEEE 12th International Conference on*
576 *Autonomic and Trusted Computing and IEEE 15th International Conference on Scalable Computing and Communications*
577 *and Its Associated Workshops (UIC-ATC-ScalCom)*, IEEE, 2015, pp. 239–246.
- 578 [19] N. Saxena, B. J. Choi, Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks,
579 *IEEE Trans. Inf. Forensics Secur.* 11 (7) (2016) 1438–1452.
- 580 [20] H. Liu, H. Ning, Y. Zhang, L. T. Yang, Aggregated-proofs based privacy-preserving authentication for V2G networks in
581 the smart grid, *IEEE Trans. Smart Grid* 3 (4) (2012) 1722–1733.
- 582 [21] L. Guo, M. Dong, K. Ota, J. Wu, J. Li, Event-oriented dynamic security service for demand response in smart grid
583 employing mobile networks, *China Commun.* 12 (12) (2015) 63–75.
- 584 [22] H. Guo, Y. Wu, F. Bao, H. Chen, M. Ma, UBAPV2G: A unique batch authentication protocol for vehicle-to-grid commu-
585 nications, *IEEE Trans. Smart Grid* 2 (4) (2011) 707–714.
- 586 [23] Z. Yang, S. Yu, W. Lou, C. Liu, P^2 : Privacy-preserving communication and precise reward architecture for V2G networks
587 in smart grid, *IEEE Trans. Smart Grid* 2 (4) (2011) 697–706.
- 588 [24] H. Wang, B. Qin, Q. Wu, L. Xu, J. Domingo-Ferrer, TPP: Traceable privacy-preserving communication and precise reward
589 for vehicle-to-grid networks in smart grids, *IEEE Trans. Inf. Forensics Secur.* 10 (11) (2015) 2340–2351.
- 590 [25] M. He, K. Zhang, X. Shen, PMQC: A privacy-preserving multi-quality charging scheme in V2G network, in: *IEEE Global*
591 *Communications Conference (GLOBECOM)*, IEEE, 2014, pp. 675–680.
- 592 [26] A. Abdallah, X. Shen, Lightweight security and privacy-preserving scheme for V2G connection, in: *IEEE Global Commu-*
593 *nications Conference (GLOBECOM)*, IEEE, 2015, pp. 1–7.
- 594 [27] B. Vaidya, D. Makrakis, H. T. Mouftah, Security and privacy-preserving mechanism for aggregator based vehicle-to-grid
595 network, *Ad Hoc Netw.* 140 (2014) 75–85.
- 596 [28] H. R. Tseng, A secure and privacy-preserving communication protocol for V2G networks, in: *IEEE Wireless Communi-*
597 *cations and Networking Conference (WCNC)*, IEEE, 2012, pp. 2706–2711.
- 598 [29] B. Vaidya, D. Makrakis, H. T. Mouftah, Multi-domain public key infrastructure for vehicle-to-grid network, in: *IEEE*
599 *Military Communications Conference (MILCOM)*, IEEE, 2015, pp. 1572–1577.
- 600 [30] M. Naghshineh, M. Schwartz, Distributed call admission control in mobile/wireless networks, *IEEE J. Sel. Areas Commun.*
601 14 (4) (1996) 711–717.
- 602 [31] M. Tao, S. Huang, Y. Li, M. Yan, Y. Zhou, SA-PSO based optimizing reader deployment in large-scale RFID systems, *J.*
603 *Netw. Comput. Appl.* 52 (2015) 90–100.
- 604 [32] X. Zhou, B. Wu, Q. Jin, User role identification based on social behavior and networking analysis for information dissem-
605 ination, *Future Gener. Comput. Syst.* doi: 10.1016/j.future.2017.04.043.
- 606 [33] H. Jin, D. S. Wong, Y. Xu, Efficient group signature with forward secure revocation, in: *IEEE International Conference*
607 *on Security Technology (SecTech)*, IEEE, 2009, pp. 124–131.
- 608 [34] D. He, J. Bu, S. Chan, C. Chen, Handauth: Efficient handover authentication with conditional privacy for wireless
609 networks, *IEEE Trans. Comput.* 62 (3) (2012) 616–622.
- 610 [35] M. Tao, M. Dong, K. Ota, Z. He, Multiobjective network opportunistic access for group mobility in mobile Internet, *IEEE*
611 *Syst. J.* doi: 10.1109/JSYST.2016.2569568.
- 612 [36] U. M. Mir, A. H. Mir, A. Bashir, M. A. Chishti, DiffServ-aware multi protocol label switching based quality of service in
613 next generation networks, in: *IEEE International Advance Computing Conference (IACC)*, IEEE, 2014, pp. 233–238.