Efficient and Anonymous Authentication With Succinct Multi-Subscription Credential in SAGVN

Dongxiao Liu, *Member, IEEE*, Huaqing Wu, *Member, IEEE*, Jianbing Ni, *Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—In this paper, we propose an efficient and anonymous authentication protocol with a succinct multi-subscription credential (AnMsc) in Space-air-ground integrated vehicular networks (SAGVN). First, we adopt a subscription-based service model in SAGVN. Specifically, vehicular users (VEs) can subscribe to network services and conduct direct mutual authentication with subscribed access points (APs) to avoid message exchanges with VEs' home network. Early application data can also be transmitted with authentication messages to improve communication efficiency. Second, we carefully tailor the design of the redactable signature and propose an efficient credential management mechanism in SAGVN. Multiple service subscriptions can be embedded into a succinct (constant-size) credential. With the credential, VEs can anonymously access any subscribed AP without revealing other subscription information. Thorough security analysis and comprehensive performance evaluation demonstrate that AnMsc can guarantee key-exchange security, VE anonymity, and service fairness while ensuring credential management and authentication efficiency.**

***Index Terms*—Space-air-ground integrated vehicular networks (SAGVN), authentication, communication efficiency, anonymity, succinct credential.**

I. Introduction

With the developments of communication technologies and smart vehicles, vehicular networks are playing an increasingly critical role in the modern transportation system. By the integration of current cellular networks [1] and device-to-device communications, vehicular networks enable vehicles to exchange information with nearby vehicles, roadside infrastructures, and the Internet for a wide range of vehicular services, including safety message broadcasting, on-board entertainment, and high-definition map downloading [2]. However, due to the limited wireless coverage in rural areas [3] and air spectrum contention in urban areas, it has become a challenging issue to enable seamless, reliable, and high-quality connections for vehicular users. To address the issue, it is promising to integrate emerging satellite and unmanned aerial vehicles (UAV) communication technologies in vehicular networks. First, the satellite networks, e.g., Starlink, can provide globally ubiquitous communications. Second, the UAV networks can be dynamically and flexibly deployed to confront the burst of network traffic or temporary shutdown of ground networks. Therefore, space-air-ground integrated vehicular networks (SAGVN) [4] have gained extensive attention recently from both the academia and the industry.

In SAGVN, since all messages are transmitted through the air, it is essential to establish secure communications between vehicular users (VEs) and heterogenous space/air/ground access points (APs). Specifically, authentication protocols are used by VEs and APs to: (1) mutually authenticate each other, and (2) securely negotiate a session encryption key for their communications [5]. In SAGVN, there are unique challenges on designing the authentication protocol.

A. Authentication Efficiency

VEs are fast-moving objects that can travel across coverage areas of different APs, which is very common for a low-earth-orbit (LEO) satellite with a limited coverage time [2] and the ultra-dense base stations. As a result, frequent AP switches [6] can happen in SAGVN. Moreover, communications between VEs and satellite APs suffer from long propagation delays [7]. To this end, an efficient authentication protocol with low handover cost and less communication overhead is desirable to achieve the full potential of SAGVN.

B. Authentication Anonymity

If VE identity information is transmitted through the air in an authentication protocol without proper protections, significant VE identity and location privacy can be leaked [8]. For example, an attacker can easily intercept transmitted handshake messages in wireless channels to break VE's anonymity. Therefore, the strong guarantee of VE anonymity should be achieved in SAGVN [9].

In ground (cellular) networks, authentication protocols are based on pre-stored VE information at its Home Network (HN) [5], [10]. Therefore, when a VE accesses a serving AP, the AP must consult the HN or a network control center [11] to authenticate the VE, which can lead to rounds of communications to finish the authentication. Due to frequent handovers and long transmission delays [7], the *authentication efficiency* in SAGVN may be affected. Therefore, direct mutual

Manuscript received February 27, 2021; revised November 2, 2021 and December 7, 2021; accepted January 19, 2022. Date of publication February 8, 2022; date of current version March 9, 2022. This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The Associate Editor for this article was T. Han. *(Corresponding author: Dongxiao Liu.)*

Dongxiao Liu and Xuemin Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: dongxiao.liu@uwaterloo.ca; sshen@uwaterloo.ca).

Huaqing Wu is with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4L8, Canada (e-mail: wu482@mcmaster.ca).

Jianbing Ni is with the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON K7L 3N6, Canada (e-mail: jianbing.ni@queensu.ca).

Digital Object Identifier 10.1109/TITS.2022.3147354

authentication between VEs and APs can be considered for SAGVN [12]. Specifically, VEs can be assigned with an identity credential from HN, such as an X509 certificate, to be authenticated by APs. Since we aim at eliminating communications with HN, the identity credential should also embed service subscription information of VEs. Otherwise, a serving AP can only check VE identity but cannot determine if the VE can access its service without consulting HN. As a result, VEs need to require multiple credentials for directly authenticating themselves to multiple serving APs in SAGVN, which may increase credential management costs at both VEs and HN. The credential management issue becomes more challenging if *VE anonymity* [13], [14] is considered. A strategy to address the issue is to let VEs frequently change identity credentials, such as a pseudonym-based certificate, to guarantee VE anonymity. Another strategy is to utilize group signature-based anonymous credential [8] to guarantee VE identity privacy to reduce the credential management cost. To this end, how to embed specific VE subscription information in the credential needs extra research attention.

In this paper, we design, analyze, and evaluate an efficient and anonymous authentication protocol in SAGVN, named AnMsc. We introduce a subscription-based service model, where VEs can first obtain a multi-subscription credential for direct mutual authentication with APs. Furthermore, we carefully tailor the designs of the redactable multi-signature technique, and propose an efficient credential management mechanism. The main contributions of this paper are summarized as follows:

- AnMsc enables VEs to obtain an all-in-one credential that embeds identities and subscribed network services. Moreover, AnMsc empowers VEs to directly conduct authentications with APs and transmit application data in early handshake messages without relying on HN.
- AnMsc ensures that a VE can anonymously prove its valid identity and service subscriptions at different authentication instances without the fear of revealing true identities. Moreover, At the same time, VE true identities can be recovered by CM if necessary.
- We conduct thorough security analysis to demonstrate AnMsc ensures key-exchange security, VE anonymity, and service fairness. Comprehensive evaluation results show that AnMsc is an efficient authentication protocol with succinct credential management overhead.

The remainder of this paper is organized as follows. We discuss state-of-the-art works on authentication protocols in cellular and SAG networks in Section II. We formulate the system and security models of AnMsc with design goals in Section III. Building blocks, including cryptographic notations, zero-knowledge proof technique, and redactable PS signature, are discussed in Section IV. We present the details of AnMsc in Section V. We give security analysis of AnMsc in Section VI and evaluate the performance of AnMsc in Section VII. Finally, we conclude this paper in Section VIII.

II. Related Work

In this section, we review the state-of-the-art research on authentication protocols in 5G and SAG networks, to emphasize the unique design challenges of an authentication protocol for SAGVN.

A. Authentication in Cellular Networks

3rd Generation Partnership Project (3GPP) proposed to standardize authentication protocols in cellular networks [5], [15]. 5G-AKA and EAP-AKA are two primary authentication methods to set up secure sessions between user equipments (UEs) and a Serving Network (SN). Both of the authentication protocols inherited main features of 4G AKA protocols based on Universal Subscriber Identity Module (USIM), which requires a pre-shared key between UEs and HN [10], where USIM in 5G can conduct more crypto operations than that in 4G. For example, subscriber identity is encrypted using public keys of HN, which increases the protection of subscriber privacy in 5G [16]. Another type of authentication protocol for 5G cellular network is the EAP-TLS [5], [17], that can be used to access non-3GPP private access points based on chain of certificates. For other use scenarios in 5G, such as massive machine communications, a light-weight authentication protocol was proposed based on the aggregated MAC [18]. For service-oriented authentication protocols, fine-grained authentication mechanism was designed. Specifically, in a software-defined network architecture, authentication protocols can be conducted with different network functions or a service function chain [19]. For SAGVN, if HN is often required to authenticate VE identity and service subscription, additional communication rounds may occur that reduces the authentication efficiency.

B. Authentication in SAG Networks

Different from existing authentication protocols in cellular networks, there were also extensive research efforts on authentication for air networks, such as UAV communications [20], and the space information network [21]. A mutual authentication protocol for space information network considering roaming was proposed in [8], where the group signature was utilized for UE privacy preservation. Group key agreement of UAVs was studied in [20] to support handover authentications. A blockchain-based architecture was designed in [20] to deal with the cross-domain authentication transparency. Authentication protocols were also designed based on novel crypto assumptions, such as lattice-based cryptography [22]. For vehicular networks, a security credential management architecture was proposed in [23], [24]. Vehicles can be assigned with pseudonym-based identity certificates to communicate with the environment. At the same time, considering the mobility of vehicles, frequent changes of certificates may be required for privacy protections. This requirement can be more strict in SAGVN. Since there are heterogeneous APs in SAGVN, subscriber anonymity [25] should also be carefully considered with novel authentication protocol designs without introducing additional credential management cost for subscribers.

III. Problem Formulation

A. System Model

In Figure 1, we show an illustrative system model of SAGVN, where a vehicle travels in an area with heterogenous

TABLE I
NOTATIONS

CM	Credential manager
AP	Access points
VE	Vehicular user
TSAP	Terrestrial satellite access point
λ	Security parameter
$\mathbb{G}$	Bilinear groups
e	Bilinear pairing
H	Hash function
$\mathcal{I}$	A set of n messages
$\mathcal{S}$	A subset of messages
$\mathcal{I}_A$	A set of APs
$\mathcal{S}_A$	A set of subscribed APs
Cer_v	Subscription credential

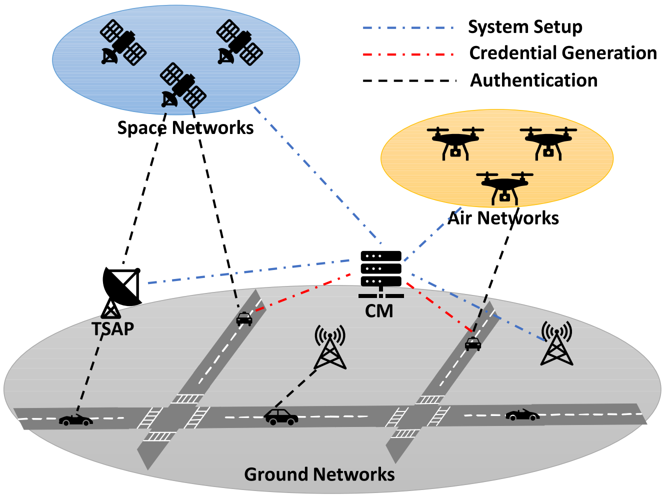


Fig. 1. System model.

APs. The traveling vehicle can switch to different APs to enjoy flexible, ubiquitous, and seamless network connections [2]. In urban areas, the vehicle can utilize the ground networks or the air networks when the ground network capacity is insufficient. In rural areas without ground/air network coverage, the vehicle can use the space networks. While vehicles can establish direct communications with different APs, they can also utilize a terrestrial satellite access point (TSAP) as a relay node between VEs and the satellite APs, that helps amplify and repeat the transmission signals.

In SAGVN, VEs can access different APs for various network services. More specifically, VEs connect to the Internet via satellite APs in rural areas. VEs also accesses specialized services provided directly by APs. For example, an autonomous vehicle can connect to roadside edge servers (APs) to retrieve high-definition maps at the edge servers' local storage without connecting to the Internet.

VEs and APs run an authentication protocol to authenticate each other and negotiate secure session keys. Under the system model, we consider three entities for authentications in SAGVN: AP, VE, and credential manager (CM).

- CM: CM is a trusted authority, such as a centralized authentication, authorization, and accounting (AAA) server. It is responsible for setting up public system parameters and issuing anonymous credentials for VEs to access different APs in SAGVN.
- VE: VEs are smart vehicles equipped with on-board units and multiple transceivers, that can operate in low frequency band for ground APs and high frequency band for air/space APs. VEs also have secure local storages with sufficient computing capability.
- AP: APs include ground stations, drones, and satellites to provide wireless connections for VEs. APs are differentiated by network providers, coverage areas, service types, and QoS guarantees.

The proposed AnMsc works with three phases: (1) System Initialization: CM sets up public parameters of the system, including a security parameter, cryptographic parameters, and public keys of APs; (2) Credential Generation: Each VE registers at CM to subscribe to multiple services of different APs according to the VE's traveling area and service requirements. CM generates an anonymous credential for the VE to conduct anonymous authentication at subscribed APs. More importantly, the anonymous credential should be succinct (constant-size) regardless of the number of subscribed APs; (3) Anonymous Authentication: With the anonymous credential, each VE can conduct an authentication protocol to set up a secure session key with a subscribed AP while guaranteeing VE anonymity.

B. Security Model

CM is trusted in AnMsc, since it is audited by governmental offices to provide secure system setup and credential management for VEs. APs in AnMsc are heterogenous entities that do not collude with each other. VEs are rational users that do not collude with each other to share secret keys. We consider an attacker with bounded computational power in SAGVN, that can intercept or modify authentication messages transmitted in wireless channels. Under the security model, AnMsc achieves the following security goals:

Key-Exchange Security [26] – It protects the confidentiality and correctness of session keys with three requirements: (1) If an authentication instance completes at uncorrupted AP and VE (with a valid service subscription), a correct session key is established between the AP and the VE; (2) An adversary cannot correctly compute a session key of uncorrupted AP and VE from intercepted authentication messages; (3) An adversary cannot impersonate an uncorrupted AP or VE, if their long-term secrets and secret keys are not leaked.

VE Anonymity – An adversary cannot recover an uncorrupted VE's true identity (the identity information when the VE register themselves at CM) from intercepted authentication messages. It should be noted that cross-layer, side-channel or other leakages of VE information are not considered in AnMsc.

Service Fairness – (1) VEs can only access subscribed SAG services; (2) True identity of VEs can be recovered from valid anonymous signatures in case of any dispute.

C. Design Goals

AnMsc achieves the following design goals:

- For frequent AP switches in SAGVN, AnMsc should reduce communication rounds between APs and VEs to achieve authentication efficiency.
- For multiple AP subscriptions in SAGVN, AnMsc should achieve efficient credential management.
- For security, anonymity, and fairness guarantees in SAGVN, AnMsc should achieve all mentioned security goals under the security model.

IV. Preliminaries

In this section, we discuss building blocks of AnMsc, including cryptographic notations, zero-knowledge proof technique, and redactable PS signature.

A. Cryptographic Notations

λ is a security parameter and is often taken as inputs implicitly. A set of multiplicative groups over elliptic curves [27] is defined as $\mathbb{G} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T\}$, with a Type III asymmetric paring $e : (\mathbb{G}_1, \mathbb{G}_2) \to \mathbb{G}_T$ and a prime order p. A ring of integers is denoted as $\mathbb{Z}_p$. We use g to denote a generator from $\mathbb{G}_1$, and $\tilde{g}$ to denote a generator from $\mathbb{G}_2$. A hash function is denoted as $H : (0, 1)^* \to \mathbb{Z}_p$.

B. Zero-Knowledge Proof

There are two parties in a Zero-knowledge proof (ZKP) [28] protocol: prover and verifier. The prover wants to demonstrate the knowledge of a secret from $\mathbb{Z}_p$ for a public relation to the verifier. In AnMsc, we consider algebraic relations with single discrete logarithm. A typical ZKP protocol can be written as follows:

$$ZKP\{(x_1, x_2) : Y = g_1^{x_1} g_2^{x_2}\}. \tag{1}$$

$x_1, x_2 \in \mathbb{Z}_p^2$ are secrets, and $Y, g_1, g_2 \in \mathbb{G}_1^3$ are public parameters.

In a non-interactive Sigma protocol [29], the prover first chooses two random numbers $r_1, r_2 \in \mathbb{Z}_p^2$ and computes $T = g_1^{r_1} g_2^{r_2}$. Then, the prover computes $c = H(Y||T)$, $ck_1 = r_1 - c \times x_1$, $ck_2 = r_2 - c \times x_2$, and sends a proof $\pi = (Y, T, ck_1, ck_2)$ to the verifier. The verifier computes $c' = H(Y||T)$ and checks the following equation:

$$Y^{c'} g_1^{ck_1} g_2^{ck_2} \stackrel{?}{=} T. \tag{2}$$

ZKP has three basic security properties [28]: *Completeness* ensures that an honest verifier accepts the correct proof; *Soundness* ensures that an efficient prover cannot forge a proof that passes ZKP verification; *Zero knowledge* ensures that the verifier learns nothing about the secrets other than if the secrets satisfy the public relation.

C. Redactable PS Signature

A redactable PS (RPS) [30], [31] signature scheme enables a signer to sign on a set of messages $\mathcal{I} = (m_1, m_2, \ldots, m_n) \in \mathbb{Z}_p^n$ and obtain a succinct signature π. Later, a signature owner can extract a valid signature on any subset $\mathcal{S} \in \mathcal{I}$. Given two generators $g \in \mathbb{G}_1$ and $\tilde{g} \in \mathbb{G}_2$, the RPS signature consists of four algorithms [31]:

- $RPS.Setup(\lambda, n) \to (x_*, y_*, \widetilde{X}, \widetilde{\mathcal{Y}}, \mathcal{Y})$ – Denote n as the number of messages in $\mathcal{I}$. Choose two random numbers $x_*, y_* \in \mathbb{Z}_p^2$ as secret keys and compute public keys:

$$\begin{aligned} \widetilde{X} &= \tilde{g}^{x_*}, \widetilde{Y}_i = \tilde{g}^{{y_*}^i}, \quad i \in [1, n], \\ Y_i &= g^{{y_*}^i}, \quad i \in [1, 2n] \setminus (n+1). \end{aligned} \tag{3}$$

  Set $\widetilde{\mathcal{Y}} = \{\widetilde{Y}_i\}_{i \in [1,n]}$ and $\mathcal{Y} = \{Y_i\}_{i \in [1,2n] \setminus (n+1)}$.
- $RPS.Sign(x_*, y_*, \mathcal{I}) \to \pi = (\pi_1, \pi_2)$ – Given a set of n messages $\mathcal{I} = (m_1, m_2, \ldots, m_n) \in \mathbb{Z}_p^n$, compute a signature $\pi = (\pi_1, \pi_2)$ as follows:

$$\pi_1 \neq 1_{\mathbb{G}_1} \in_R \mathbb{G}_1, \quad \pi_2 = \pi_1^{\sum_{i=1}^n m_i {y_*}^i + x_*}, \tag{4}$$

  where π_1 is a non-identity random generator in $\mathbb{G}_1$.
- $RPS.Extract(\tilde{\mathcal{Y}}, \mathcal{Y}, \pi, \mathcal{S}) \to \pi' = (\pi'_1, \pi'_2, \tilde{\pi}', \pi'_s)$ – $\mathcal{S} \in \mathcal{I}$ is a subset of $\mathcal{I}$ with k messages. Choose two random numbers $r_1, r_2 \in \mathbb{Z}_p^2$ and compute:

$$\pi'_1 = \pi_1^{r_1}, \pi'_2 = \pi_2^{r_1} \pi_1'^{r_2}. \tag{5}$$

  For messages $m_i \in \mathcal{I} \setminus \mathcal{S}$, compute the following:

$$\tilde{\pi}' = (\prod_{m_i \in \mathcal{I} \setminus \mathcal{S}} \widetilde{Y}_i^{m_i}) \tilde{g}^{r_2}. \tag{6}$$

  For messages $m_i \in \mathcal{S}$, compute a redacted signature:

$$\begin{aligned} \pi'_s &= \prod_{m_i \in \mathcal{S}} (Y_{n+1-i}^{r_2} \prod_{m_j \in \mathcal{I} \setminus \mathcal{S}} Y_{n+j+1-i}^{m_j})^{c_i}, \\ c_i &= H(\mathcal{S}||i||\pi'_1||\pi'_2||\tilde{\pi}')_{m_i \in \mathcal{S}}, \end{aligned} \tag{7}$$

  where c_i is the digest of messages and randomized signatures. Set $\pi' = (\pi'_1, \pi'_2, \tilde{\pi}', \pi'_s)$.
- $RPS.Check(\mathcal{S}, \widetilde{X}, \widetilde{\mathcal{Y}}, \mathcal{Y}, \pi') \to (0, 1)$ – For each message $m_i \in \mathcal{S}$, compute $c_i = H(\mathcal{S}||i||\pi'_1||\pi'_2||\tilde{\pi}')$. Check the following equations:

$$\begin{aligned} &\pi'_1 \neq 1_{\mathbb{G}_1}, \quad e(\pi'_2, \tilde{g}) = e(\pi'_1, \tilde{\pi}' \widetilde{X} \prod_{m_i \in S} \widetilde{Y}_i^{m_i}), \\ &e(\pi'_s, \tilde{g}) = e(\prod_{m_i \in S} Y_{n+1-i}^{c_i}, \tilde{\pi}'). \end{aligned} \tag{8}$$

  If all checks pass, return 1; Otherwise, return 0.

The security properties of the redactable PS signature include *unforgeability* and *unlinkability*. The first property ensures that an efficient adversary cannot forge a valid signature without knowledge of the secret keys [31]. The second property ensures that the verification of a subset of $\mathcal{I}$ does not leak other messages of $\mathcal{I}$ in the original signature.

V. Proposed AnMsc

In this section, we present AnMsc that supports credential-based mutual authentication [5], [17] between APs and VEs with 0 round-trip (0-RTT) mode. Our starting technique is the mutual authentication protocol [26], [32], [33]. Then, we adopt the RPS signature [31] to generate an anonymous credential for VEs with subscriptions to multiple network services. During an authentication instance, VEs can reveal any individual service subscription at a corresponding AP with high anonymity guarantees. Moreover, VE subscriptions can expire overtime in SAGVN and VE true identities can also be recovered by CM when it is necessary.

In the following, we present detailed constructions of AnMsc, including System Initialization, Credential Generation, Anonymous Authentication and Revocation. For illustrative simplicity, we assume that secure and authenticated out-of-band channels have been set up between VE/AP and CM during System Initialization and Credential Generation.

A. System Initialization

CM sets a security parameter λ, e.g., 128-bit security level. CM chooses a set of multiplicative groups $\mathbb{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ with a prime order p and a type III bilinear pairing e. CM chooses two random generators $(g, \tilde{g}) \in \mathbb{G}_1 * \mathbb{G}_2$. CM sets hash functions $H : (0, 1)^* \rightarrow \mathbb{Z}_p$. CM sets n as the number of APs in the system. CM runs $RPS.Setup(\lambda, n)$ to get system master secret keys $msk = (x_*, y_*)$ and system public keys $mpk = (\widetilde{X}, \widetilde{\mathcal{Y}}, \mathcal{Y})$.

CM initializes s secure signature scheme, such as ECDSA [34] or certificate-based signatures with two algorithms: (1) $Sign(m, sk) \rightarrow \pi$, and (2) $Verify(\pi, m, pk) \rightarrow (0, 1)$. Intuitively, (pk, sk) is a public/private key pair (corresponding to a trusted certificate), m is a message, and π is the generated signature. CM also initializes an authenticated encryption scheme [35], e.g., a symmetric encryption with a message authentication code. In the encryption scheme, key is an encryption key, and $Enc(m, key)$ is an authenticated encryption of a message m.

APs can register themselves at CM. CM verifies the eligibility of APs and assigns each AP with a set of RPS public key $(\widetilde{Y}_i, Y_i)$. There are n APs in the system denoted as $\mathcal{I}_A = (AP_1, AP_2, \ldots, AP_n)$. Each AP_i also obtains a public/private key pair (pk_i, sk_i) for the signature scheme. $\widetilde{Y}_i, Y_i$, and pk_i are bound to AP_i by a certificate signed by CM. Finally, CM publishes the system public parameters as follows:

$$Para = \{\lambda, \mathbb{G}, p, e, g, \tilde{g}, \mathcal{I}_A, n, mpk, H\}. \tag{9}$$

B. Credential Generation

Any VE can register itself at CM with its true and authenticated identity ID. Based on its locations, trip plans, and service requirements, the VE first subscribes a set of APs, where k subscribed APs are denoted as $\mathcal{S}_A$. The VE can pre-pay the subscription fee of $\mathcal{S}_A$ to CM. To generate a subscription credential, the VE and CM conduct the following operations as shown in Figure 2:

(1) The VE chooses a secret key sk_v and constructs a set of n messages $\mathcal{I} = \{m_i\}_{i \in [1,n]}$ as follows:

$$\begin{aligned} m_i &= sk_v, \quad if\ AP_i \in S_A, \\ m_i &= 0, \quad if\ AP_i \notin S_A. \end{aligned} \tag{10}$$

The VE uses sk_v to compute:

$$\begin{aligned} &V_1 = g^{sk_v}, \quad \tilde{V}_2 = \tilde{g}^{sk_v}, \\ &\pi_V = ZKP\{(sk_v) : V_1 = g^{sk_v} \wedge \tilde{V}_2 = \tilde{g}^{sk_v}\}. \end{aligned} \tag{11}$$

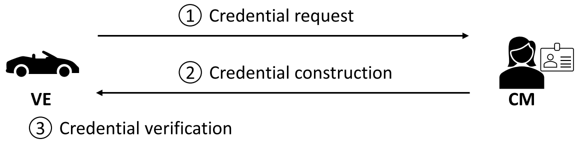


Fig. 2. Credential generation.

π_V is to prove the knowledge of sk_v in V_1 and $\tilde{V}_2$. The VE sends $(ID, \mathcal{S}_A, V_1, \tilde{V}_2, \pi_V)$ and pays the service subscription fee to CM via a secure channel.

(2) Upon receiving $(ID, \mathcal{S}_A, V_1, \tilde{V}_2, \pi_V)$, CM first checks $V_1, \tilde{V}_2$ are non-identity element, π_V is correct, and there are no registered $V_1, \tilde{V}_2$. If the check passes and the subscription fee is correctly received, CM stores $(\mathcal{S}_A, \tilde{V}_2)$ at its storage and generates a PS signature on V_1 using its secret keys (x_*, y_*) as follows:

$$\begin{aligned} C_1 &= g^{r_v}, \quad r_v \in_R \mathbb{Z}_p, \\ C_2 &= (g^{x_*}(V_1)^{\sum_{AP_i \in \mathcal{S}_A} y_*{}^i})^{r_v} \\ &= (g^{r_v})^{x_*}(g^{r_v})^{sk_v \sum_{AP_i \in \mathcal{S}_A} y_*{}^i}. \end{aligned} \tag{12}$$

This is a multi-message PS signature on the message set $\mathcal{I}$ in Equ. 10, where the randomness r_v serves the purpose of obtaining a random generator C_1. CM sets $Cer_v = (C_1, C_2)$ and sends Cer_v to the VE via a secure channel.

(3) Upon receiving Cer_v, VE checks the correctness of Cer_v:

$$C_1 \neq 1_{\mathbb{G}_1}, \quad e(C_2, \tilde{g}) = e(C_1, \widetilde{X} \prod_{AP_i \in \mathcal{S}_A} \widetilde{Y}_i^{sk_v}). \tag{13}$$

Note that, since Cer_v is not extracted here, the verification is similar to the first line of Equ. 8. If the check passes, the VE stores sk_v and Cer_v in its secure storage.

Discussions: VEs can utilize secure hardware technologies, such as Intel SGX or specialized hardware designs. With the secure hardware in VEs, the generated credential can be securely transmitted to VEs by establishing an authenticated channel between VEs and CM [36]. Later on, the credential can also be used in the secure hardware. Moreover, a blockchain-based provenance architecture can be used to audit behaviors of CM [37]. Secret information of APs and CM should also be well generated and stored.

C. Anonymous Authentication

After obtaining Cer_v, the VE can access SAG services in $\mathcal{S}_A$ by running an authentication protocol with any subscribed AP. The VE must detect nearby APs, i.e., a service discovery process is required. [33]. For a discovered AP_i, the VE has the following authenticated information:

$$pp_A = (bid, ID_A, pk_i, g^s). \tag{14}$$

bid is a broadcast id of the SAG service provided by AP_i. ID_A is an authenticated id of AP_i. To verify the authenticity of AP_i, a public signature verification key pk_i of AP_i is also obtained by the VE. Moreover, a semi-static and authenticated DH share g^s is sent to the VE for transmissions of early application data.

We omit details of the discovery process, but hint two potential mechanisms: (1) VEs can pre-store pp_A at the subscription phase. This is reasonable especially for SAG services in rural areas, where available APs can be pre-determined. However, the broadcast id and the semi-static DH share should be refreshed frequently for security guarantees. (2) There can be a broadcasting channel, where APs sign and broadcast their services and pp_A to nearby VEs. Moreover, a CM-signed certificate of APs may also need to be sent to VEs.

After obtaining pp_A, the VE can conduct an anonymous authentication protocol to access AP_i as follows:

(1) The VE constructs a handshake message m_h:

$$m_h = (bid, ssid, ID_A, T_p, T_c, g^s, g^x). \tag{15}$$

bid is the broadcast id of AP_i; ID_A is the identity of AP_i; $ssid$ is a unique and random session ID; $x \in \mathbb{Z}_p$ is a VE-chosen DH secret and g^x is the DH share; T_p is an identifier of a subscription period. The subscription period can depend on specific applications, e.g., a one-hour subscription period, "3-4 pm, Jan 6, 2021", can be represented by "151601062021". Note that, subscription time can be removed if APs determine subscription information from T_c; T_c is a current time stamp.

The VE proves the valid subscription to AP_i from Cer_v. By setting a message set $\mathcal{S}$ with only one message ($m_i = sk_v$) for AP_i, the VE extracts a signature from Cer_v as follows:

$$RPS.Extract(\tilde{\mathcal{Y}}, \mathcal{Y}, Cer_v, \mathcal{S}) \rightarrow Cer_v' = (\pi_1', \pi_2', \tilde{\pi}', \pi_s'). \tag{16}$$

The VE computes an anonymous signature π_{ssid} on m_h:

$$\pi_{ssid} = ZKP\{(sk_v) : e(\pi_2', \tilde{g}) = e(\pi_1', \tilde{\pi}'\widetilde{X}\widetilde{Y}_i^{sk_v})\}. \tag{17}$$

π_{ssid} proves that the valid subscription to AP_i and sk_v is consistent across Cer_v'. π_{ssid} can be achieved by using the ZKP technique with slight modifications [31] and including m_h in computing a challenge in the ZKP.

The VE derives a handshake key htk using the HMAC-based Key Derivation Function (HKDF) [38]. Specifically, HKDF is a function that takes DH shares to output multiple keys for the authenticated encryption scheme Enc, including handshake keys htk, htk', an early application-data key edk, and a session key ssk. htk, htk', edk are derived from g^x, g^s, g^{sx} [33]. The VE sets

$$m_e = (ID_A, T_p, T_c, \pi_{ssid}, Cer_v'), \tag{18}$$

and encrypts m_e using htk as $Enc(m_e, htk)$ [26], [33]. The VE can also include some early application data $EData$ as $Enc(EData, edk)$.

Finally, the VE sends the following message to AP_i via a wireless channel:

$$\{bid, ssid, g^x, Enc(m_e, htk), Enc(EData, edk)\}. \tag{19}$$

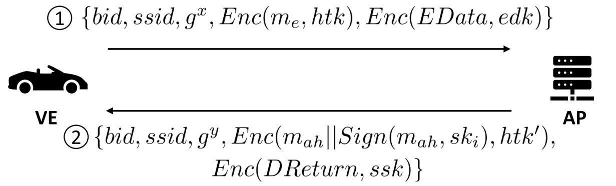

① $\{bid, ssid, g^x, Enc(m_e, htk), Enc(EData, edk)\}$
VE
AP
② $\{bid, ssid, g^y, Enc(m_{ah}||Sign(m_{ah}, sk_i), htk'),$
$Enc(DReturn, ssk)\}$

Fig. 3. Anonymous authentication.

(2) Upon receiving the message from the VE, AP_i first checks the validity of bid and $ssid$. If the check passes, AP_i computes g^{xs} using g^x and the local semi-static secret s. AP_i derives htk, htk', edk from g^x, g^s, g^{xs} using the HKDF. AP_i tries to decrypt $Enc(m_e, htk)$ using htk. If the decryption or the integrity verification fails, AP_i aborts the message. Otherwise, AP_i obtains $m_e = (ID_A, T_p, T_c, \pi_{ssid}, Cer_v')$. AP_i can maintain a list of received authentication instances at its storage.

AP_i checks the validity of ID_A, T_p, T_c. Note that, T_p is pre-determined. Then, AP_i verifies the correctness of π_{ssid} and $Cer_v' = (\pi_1', \pi_2', \tilde{\pi}', \pi_s')$ as follows:

$$e(\pi_s', \tilde{g}) = e(Y_{n+1-i}^{c_i}, \tilde{\pi}'), e(\pi_1', \tilde{\pi}'\tilde{X}) \neq e(\pi_2', \tilde{g}), \quad Check\ \pi_{ssid}\ using\ ZKP. \tag{20}$$

i is the index of the AP and c_i is calculated similar in Equ. 7. The second equation ensures that sk_v is not 0, where 0 indicates the service is not subscribed. The third equation ensures that π_{ssid} is correct, such that the VE has the knowledge of a valid sk_v for AP_i.

If the above check fails, AP_i aborts; Otherwise, AP_i chooses another secret $y \in_R \mathbb{Z}_p$ and computes g^y and g^{xy}. AP_i derives a secure session key ssk using HKDF from $g^s, g^x, g^y, g^{sx}, g^{xy}$. AP_i sets a message m_{ah} as follows:

$$m_{ah} = (bid, ssid, ID_A, T_r, g^s, g^x, g^y), \tag{21}$$

where T_r is a new time stamp. AP_i computes a signature on m_{ah} as $Sign(m_{ah}, sk_i)$ using its authenticated signing key. AP_i computes $Enc(m_{ah}||Sign(m_{ah}, sk_i), htk')$. AP_i can also include some application date $DReturn$ in the message by computing $Enc(DReturn, ssk)$. AP_i sends the following message to the VE:

$$\{bid, ssid, g^y, Enc(m_{ah}||Sign(m_{ah}, sk_i), htk'), Enc(DReturn, ssk)\}. \tag{22}$$

(3) Upon receiving the above message, the VE first checks $bid, ssid$. If the check passes, the VE uses g^y and the local secret x to compute g^{xy}. The VE decrypts the message to obtain m_{ah} and $Sign(m_{ah}, sk_i)$ using htk', and verifies the correctness of $Sign(m_{ah}, sk_i)$ using the public key pk_i of AP_i. If all checks pass, the VE computes ssk using $g^s, g^x, g^y, g^{sx}, g^{xy}$ based on HKDF. The VE can decrypt the application data $Enc(DReturn, ssk)$ and communicate with AP_i using the secure session key ssk.

A description of the authentication protocol is shown in Figure 3. The protocol can support different modes for specific use cases: For ground APs, more flexible authentication can be implemented without relying on the pre-shared semi-static DH share, g^s. This is because ground APs usually have less communication delay and non-0-RTT authentication protocol can be supported. For space/air APs, a pre-shared semi-static g^s is required to enable early data transmissions with handshake messages. To further reduce communication overhead between VEs and space/air APs, we can use a trusted

TSAP as a relaying node on the ground. VEs can first send handshake messages to the TSAP, taht sends the messages to space/air APs via a reserved channel. Forward security can be considered with the integration of puncturable encryption scheme [39] and the 0-RTT authentication protocol. However, this may increase the computation and communication costs for both VEs and APs in an authentication instance.

D. Revocation

For multi-subscription anonymous credentials, we can adopt a time-bounded revocation strategy [31] in SAGVN.

There are APs where subscriptions can only be valid for a certain period of time due to the following reasons: (1) Air APs, e.g, UAVs are temporarily deployed at areas with bursting network requirements; and (2) Satellite APs can serve a certain area with limited time while moving at their orbits, e.g., a few minutes for an LEO satellite. Therefore, the revocation strategy for such APs is to assign VEs with time-bounded credentials [40], [41]. Specifically, a time-bounded credential is only valid at certain time periods, which can be achieved by expanding corresponding public keys of the AP to a set of public keys for different subscription periods [31]. For example, CM can extend AP_i's public keys into $(AP_{i,1}, AP_{i,2}, \ldots)$, where each $AP_{i,j}$ indicates a subscription period. VEs register at CM with fine-grained subscriptions of each period and CM can generate a credential on subscribed service windows.

When a cheating VE is found, such as an attempt to access an unsubscribed service, the true identity of the VE should be recovered from a valid anonymous signature. Given a valid Cer_v' for AP_i, CM can check all $\tilde{V}_2 = \tilde{g}^{sk_v}$ in its storage with the following equation until a match is found:

$$e(\pi_1', V_2) = (e(\pi_2', \tilde{g})e(\pi_1', \tilde{X}\tilde{\pi}')^{-1})^{y_*^{-i}}. \tag{23}$$

After finding the corresponding $\tilde{V}_2$, CM can output the VE's true identity from its storage. Counter-measures can be taken to enforce accountability against the misbehaving VE based on CM's service agreement.

After the VE's identity is recovered by CM, the VE is considered revoked in the system. In this case, a revocation list can be set up. For a VE with subscriptions at AP_i that have not expired, CM computes the following equation based on its master secret key y_* and the submitted $\tilde{V}_2 = \tilde{g}^{sk_v}$ of the VE:

$$R_v = (\tilde{g}^{sk_v})^{y_*^{i}}. \tag{24}$$

CM sends R_v to AP_i. AP_i can further check if a valid received signature is within a revocation list using the following equation:

$$e(\pi_1', R_v)e(\pi_1', \tilde{X}\tilde{\pi}') = e(\pi_2', \tilde{g}). \tag{25}$$

Note that, the above equation is derived from the verification equation of RPS signature in Equ. 8. Moreover, the revocation list is used after a VE's identity is recovered by CM and CM will not share the recovered identity with APs or other entities in AnMsc. However, after the opening, the VE is not considered as anonymous in AnMsc.

VI. Security Analysis

In this section, we demonstrate the security properties of AnMsc in terms of key-exchange security, VE anonymity, and service fairness.

A. Key-Exchange Security

As discussed in [33], the first two requirements of the key-exchange security require that the strong DH assumption, the Hash DH assumption [33], the underlying RPS signature [31], the digital signature scheme used by APs, the authentication encryption scheme, and the HKDF [26] are secure. Moreover, the adversary cannot compromise long-term secrets of other entities in SAGVN. Compared with the protocol [26], [33], the main difference in AnMsc is the adoption of a signature scheme based on anonymous credentials. As a result, the authenticity of VEs in AnMsc is from valid service subscriptions. At the same time, the property required for the signature scheme of VEs is still the *unforgeability* which cannot be compromised by an efficient adversary.

For the third requirement of key-exchange security, the adversary can only impersonate an uncorrupted AP or VE if the adversary can break the security of the RPS signature or the digital signature scheme used by APs. For the RPS signature, there are two processes: credential generation and proof of knowledge of a signature. For the first process, without the system master secret keys, the adversary cannot issue a valid subscription credential unless it can break the *unforgeability* of the RPS signature [31]. For the second process, without a valid subscription credential, Cer_v, the adversary cannot generate a correct proof, π_{ssid}, to demonstrate the knowledge of sk_v, unless it can break the *soundness* property of the ZKP protocol. The signature scheme used by APs is also unforgeable under different secure instantiations.

Discussions on 0-RTT security: First, it is required that the (semi-static) secrets of APs not to be leaked or APs frequently update bid and g^s. An alternative solution is to use the puncturable encryption scheme for the 0-RTT mode [39]. Moreover, an expiration time of the semi-static secret should be authenticated by APs [33]. Second, 0-RTT mode may need detailed design considerations when combining with application layer protocols [42], [43] in different SAG services, which is out of scope of this paper.

B. VE Anonymity

In the authentication protocol of AnMsc, a VE with a valid subscription credential first extracts a signature for an intended AP, and then proves the knowledge of sk_v in the extracted signature with the ZKP technique.

VE anonymity can be reduced to the security of RPS signature and ZKP protocol. The extracted signature does not leak the original signature or other signed messages in the credential Cer_v since VEs can choose two random numbers to randomize the original signature [31]. The extracted signature is verified with the $RPS.Verify$ function, which can be made zero-knowledge (for sk_v) by the ZKP technique. Specifically, for verifications that require the input of sk_v, VE chooses a random number to replace sk_v and constructs a non-interactive

ZKP proof π_{ssid}. By doing so, the adversary can only obtain sk_v from π_{ssid} if the adversary can (1) break the *anonymity* of the RPS signature [31], or (2) break the *zero knowledge* of the ZKP protocol.

Discussions: An interesting issue in anonymous signature-based authentication protocols is to provide message linkability within each individual session [44]. That is, AP cannot determine a true identity of a VE but can know that messages are from the same VE in one session. A potential solution is to introduce a basename [45], [46] for controlled linkability, and require VEs to prove knowledge of sk_v on the basename. However, how to specifically set the basename for different sessions in SAGVN may need more attentions, especially when revocation list or signature derivation is used with a basename-based linkability [47].

C. Service Fairness

Service fairness includes two aspects. First, VEs should only be able to access subscribed services. CM is trusted and uncompromised in AnMsc, and is in charge of credential issuance. An adversary can only forge a valid subscription credential if it can break the *unforgeability* of RPS signature. To prevent VEs from arbitrarily sharing the credentials with others is not considered in AnMsc. A potential solution is to use secure hardware to transmit and store the credential or design subscription strategy that requires VEs' master secret to be embedded into the credential.

Second, VEs are required to be revoked for certain services, which can be done when the subscription credential expires for APs. In case of VE misbehavior, VE anonymity should be removed to reveal its true identity. This can be reduced to the *traceability* and *non-frameability* of the RPS signature, which ensures that valid anonymous signature can be securely opened by CM. After the opening, by adding the opened VE to a revocation list, AnMsc achieves fine-grained service-level VE revocation.

VII. Performance Evaluation

In this section, we evaluate the computation, communication, and storage overhead of AnMsc. We mainly consider cryptographic operations, including exponentiations in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, and pairing operations, that are denoted as E_1, E_2, E_T and P, respectively. $|\mathbb{G}_1|, |\mathbb{G}_2|$ and, $|\mathbb{G}_T|$ are denoted as the size of corresponding group elements. The signature scheme for APs in our experiments is ECDSA as adopted in [33], with S_g and S_v as the computation cost of generation and verification of a signature, respectively. We denote n as the number of total SAG services in $\mathcal{I}$ and k as the number of subscribed services in $\mathcal{S}_A$.

We simulate AnMsc on a laptop with an Intel Core i5 2.3 GHz processor and 8 GB memory over a Type III BN curve in Miracl library [48]. For the ECDSA signature, we simulate the *sign* and *verify* algorithms with a 256-bit order. E_1, E_2, E_t and P are tested without pro-pressing. The size of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, and $\mathbb{Z}_p$ in the BN curve is 512 bit, 1024 bit, 3072 bit, and 256 bit, respectively. The evaluation results are shown in the following sections, including credential generation, anonymous authentication, and revocation.

TABLE II

Complexity Analysis of Credential Generation

	Computation	Storage
CM	$5E_1 + 2E_2$	$\lvert\mathbb{G}_2\rvert + \lvert S_A\rvert$
VE	$2E_1 + 3E_2 + 2P$	$(2k+3)\lvert\mathbb{G}_1\rvert +$ $(k+1)\lvert\mathbb{G}_2\rvert + \lvert\mathbb{Z}_p\rvert$

A. Credential Generation

The credential generation mainly involves interactions between CM and VEs. For VEs, they set messages to be signed for subscribed services as sk_v. For non-subscribed services, VEs set messages as 0. As a result, VEs only need to conduct one E_2 and two pairings in verifying the signature. For CM, it verifies the correctness of proof π_V and generates an RPS signature on g^{sk_v}. More specifically, the computation overhead is 15.75 ms for CM and 60.8 ms for VEs to negotiate a credential as shown in Table II, which is feasible in real-world applications.

For the communication overhead, VEs essentially send commitments of sk_v with the proof π_V and a subscription list $\mathcal{S}_A$ to the CM. The CM returns a succinct credential Cer_v. Specifically, one-round communication is conducted in the credential generation phase and the communication overhead is mainly affected by k.

For the storage overhead at CM, it stores a tracing token $\tilde{g}^{sk_v}$ and a subscription list $\mathcal{S}_A$ for each VE, which results in a linearly increasing storage overhead with the number of VEs in the system. However, this is still significant storage savings compared with pseudonym-based credentials or traditional anonymous credentials, where credentials may need to be changed for each subscribed service at different subscription periods.

For the storage overhead at an individual VE, the size of its credential is not affected by the number of subscribed services, which is very important in SAGVN since storing a credential $(sk_v, Cer_v) \in \mathbb{Z}_p * \mathbb{G}_1^2$ securely is expensive compared with that of storing public parameters related to the credential. At the same time, the VE needs to store public parameters of subscribed services to be used when deriving credentials for an intended service. Specifically, the VE stores two public generators $g, \tilde{g}$. Since the VE sets all messages to be signed in Cer_v as sk_v and other messages as 0, the VE needs to only store $k|\mathbb{G}_2|$ and $2k|\mathbb{G}_1|$ by pre-computing $\prod \tilde{Y}_i$ and $\prod Y_{n+j+1-i}$. Finally, the total storage overhead of a VE's credential and related public parameters is $(2k+3)|\mathbb{G}_1| + (k+1)|\mathbb{G}_2| + |\mathbb{Z}_p|$.

We plot the storage overhead in bits in Figure 4. We denote the storage of $|AP_i|$ in S_A as a 32-bit word. Although the storage overhead increases at VEs due to the public parameters, the credential size for an individual VE remains succinct. If the VE would like to enable 0-RTT mode of the authentication protocol, it needs to additionally store a semi-static DH share g^s and a public key for the ECDSA scheme of the subscribed AP in S_A.

B. Anonymous Authentication

The anonymous authentication protocol involves APs and VEs. For an individual VE with a credential Cer_v of k

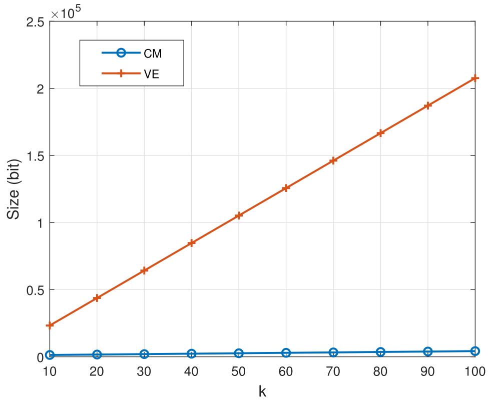
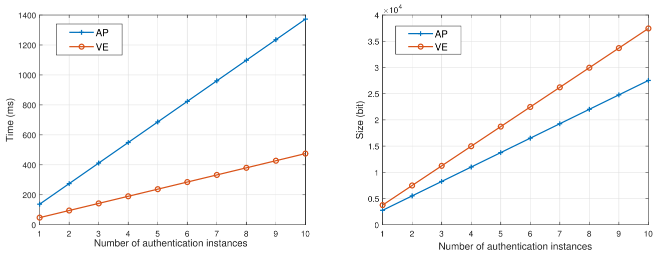


Fig. 4. Storage cost of credential generation.



(a) Computation Cost (b) Communication Cost

Fig. 5. Authentication efficiency.

subscribed services, the VE can prove the knowledge of one service subscription at each subscribed AP. The dominant computation overhead for the VE is the extraction function when generating a redacted credential Cer'_v. This seems to result in a linearly increasing computation overhead with $(n-1)$ exponentiations. However, since messages signed in Cer_v are all sk_v, only limited exponentiation operations need to be conducted for non-redacted messages when extracting signatures using Equ. 6 and Equ. 7. We consider VE computations of DH shares, extracting a valid signature from Cer_v, proving knowledge of sk_v in π_{ssid}, and verifying ECDSA signatures. The simulation results of VE computations in the authentication are shown in Figure 5a. From the results, we can see that it only costs a few milliseconds for one VE to finish computations in the handshake messages.

The computation overhead for APs mainly consists of the verification of Cer'_v, π_{ssid}, computing new DH shares, and generating an ECDSA signature. In Figure 5a, we can see that the computation cost is a few milliseconds for APs in an authentication instance.

For the communication overhead, we mainly consider the size of handshake messages without the early application data and session data. We denote each of $bid, ssid, ID_A, T_p, T_c$ and T_r as a 32-bit word. More importantly, the additional overhead introduced by the anonymous signature in the authentication protocol is constant regardless of the size of public parameters. As shown in Figure 5b, a single round of an authentication instance only incurs a few bytes for handshake messages. It should be noted that if we implement the authenticated encryption with a symmetric encryption and message authentication code (MAC), a digest of each message in a single authentication instance is added compared with that in Figure 5b.

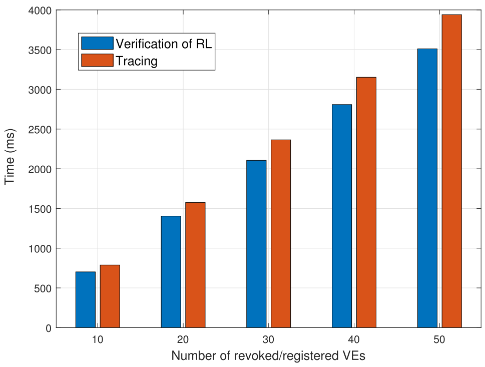


Fig. 6. Computation cost of revocation/tracing.

TABLE III
COMPLEXITY ANALYSIS OF REVOCATION

Verification of RL	Tracing	RL Storage
$n_r 3P$	$n_s(3P + E_t)$	$n_r \lvert \mathbb{G}_2 \rvert$

C. Revocation

There are two revocation methods in AnMsc. The first strategy eliminates the use of a revocation list, but increases the size of public parameters. The impact of the first strategy on the credential generation and the authentication protocol can be seen in Section V-D. The second strategy adds a revocation token for each service subscription at a revocation list (RL). In Table III, the verification cost of a revoked user and the RL storage size grow with the number of VEs in the RL, denoted as n_r. At the same time, the computation cost of the tracing operation increases with the number of registered VEs for the service, denoted as n_s. In the worst case, CM may need to search all registered VEs until a match is found. In Figure 6, we can see that the computation cost of verifying the RL is a few seconds as n_r increases.

In summary, AnMsc significantly reduces credential management cost for both CM and VEs while ensuring the strong anonymity guarantees. The storage cost of VE credential remains constant regardless of the number of subscribed services and the requirements of the identity anonymity. Authentication efficiency is also achieved with only one-round communication between VEs and APs, the limited size of handshake messages, and a few milliseconds in computational overhead. More importantly, early application data are enabled with transmissions of handshake messages, which is essential for SAGVN due to the long propagation delays of space/air networks.

VIII. CONCLUSION

In this paper, we have proposed an efficient and anonymous authentication protocol with succinct multi-subscription credential (AnMsc) for SAGVN. AnMsc enables mutual authentication with efficient communication overhead. Moreover, AnMsc guarantees strong VE anonymity and service fairness in SAGVN while preserving credential management efficiency.

We have conducted thorough security analysis and comprehensive performance evaluation to demonstrate the security and efficiency of AnMsc. The in-depth analysis of authentication requirements in future wireless networks and the design, analysis, and evaluation of AnMsc may shed light on the research and practices for securing diversified services in SAGVN. In the future, we will further explore distributed credential management issue for SAGVN, where a blockchain-based credential manager can be designed to promote transparent collaboration among heterogenous SAG service providers.

References

[1] S. Chen *et al.*, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, Jun. 2017.

[2] H. Wu *et al.*, "Resource management in space-air-ground integrated vehicular networks: SDN control and AI algorithm design," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 52–60, Dec. 2020.

[3] W. Shi, H. Zhou, J. Li, W. Xu, N. Zhang, and X. Shen, "Drone assisted vehicular networks: Architecture, challenges and opportunities," *IEEE Netw.*, vol. 32, no. 3, pp. 130–137, Jan. 2018.

[4] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, Jul. 2017.

[5] *Security Architecture and Procedures for 5G System*, document Ts 33.501, v0.8.0, 3GPP, 2018.

[6] C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, and J. Lee, "ReHand: Secure region-based fast handover with user anonymity for small cell networks in mobile communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 927–942, 2020.

[7] K. Xue, W. Meng, H. Zhou, D. S. L. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 3673–3684, Jun. 2020.

[8] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "AnFRA: Anonymous and fast roaming authentication for space information network," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 486–497, Jul. 2018.

[9] D. He, D. Wang, Q. Xie, and K. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Sci. China Inf. Sci.*, vol. 60, no. 5, May 2017, Art. no. 052104.

[10] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM CCS*, 2018, pp. 1383–1396.

[11] B. Zhao, P. Liu, X. Wang, and I. You, "Toward efficient authentication for space-air-ground integrated Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 7, Jul. 2019, Art. no. 155014771986039.

[12] S. Yao, J. Guan, Y. Wu, K. Xu, and M. Xu, "Toward secure and lightweight access authentication in SAGINs," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 75–81, Dec. 2020.

[13] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.

[14] G. Neven, G. Baldini, J. Camenisch, and R. Neisse, "Privacy-preserving attribute-based credentials in cooperative intelligent transport systems," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 131–138.

[15] A. Braeken, "Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability," *Comput. Netw.*, vol. 181, Nov. 2020, Art. no. 107424.

[16] A. Koutsos, "The 5G-AKA authentication protocol privacy," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Jun. 2019, pp. 464–479.

[17] J. Zhang, Q. Wang, L. Yang, and T. Feng, "Formal verification of 5G-EAP-TLS authentication protocol," in *Proc. IEEE Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2019, pp. 503–509.

[18] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: A lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5329–5344, Jun. 2020.

[19] J. Ni, X. Lin, and X. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.

[20] K. Gai, Y. Wu, L. Zhu, K.-K.-R. Choo, and B. Xiao, "Blockchain-enabled trustworthy group communications in UAV networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4118–4130, Jul. 2021.

[21] C. Huang, Z. Zhang, M. Li, L. Zhu, Z. Zhu, and X. Yang, "A mutual authentication and key update protocol in satellite communication network," *Automatika*, vol. 61, no. 3, pp. 334–344, Jul. 2020.

[22] R. Ma, J. Cao, D. Feng, and H. Li, "LAA: Lattice-based access authentication scheme for IoT in space information networks," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2791–2805, Apr. 2020.

[23] B. Brecht and T. Hehn, "A security credential management system for V2X communications," in *Connected Vehicles*. Cham, Switzerland: Springer, 2019, pp. 83–115.

[24] *Proximity-Based Services (Prose); Security Aspects*, document Ts 33.303, v14.1.0, 3GPP, 2017.

[25] M. Li, Y. Chen, S. Zheng, D. Hu, C. Lal, and M. Conti, "Privacy-preserving navigation supporting similar queries in vehicular networks," *IEEE Trans. Dependable Secure Comput.*, early access, Aug. 18, 2020, doi: 10.1109/TDSC.2020.3017534.

[26] H. Krawczyk and H. Wee, "The OPTLS protocol and TLS 1.3," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Mar. 2016, pp. 81–96.

[27] J.-N. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin, "Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 247–257, Jan. 2020.

[28] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proc. CRYPTO*. Berlin, Germany: Springer, 1997, pp. 410–424.

[29] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. CRYPTO*. Berlin, Germany: Springer, 1986, pp. 186–194.

[30] O. Sanders, "Efficient redactable signature and application to anonymous credentials," in *Proc. IACR Int. Conf. Public-Key Cryptogr.* Cham, Switzerland: Springer, 2020, pp. 628–656.

[31] O. Sanders, "Improving revocation for group signature with redactable signature," in *Proc. IACR Int. Conf. Public-Key Cryptography*. Cham, Switzerland: Springer, 2021, pp. 301–330.

[32] H. Krawczyk, "SIGMA: The 'SIGn- and-MAc'approach to authenticated Diffie-Hellman and its use in the IKE protocols," in *Proc. CRYPTO*. Berlin, Germany: Springer, 2003, pp. 400–425.

[33] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the Internet of Things," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2016, pp. 301–319.

[34] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[35] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2000, pp. 531–545.

[36] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," in *Proc. 2nd Int. Workshop Hardw. Architectural Support Secur. privacy*, vol. 13, 2013, p. 7.

[37] D. Liu, J. Ni, C. Huang, X. Lin, and X. Shen, "Secure and efficient distributed network provenance for IoT: A blockchain-based approach," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7564–7574, Aug. 2020.

[38] H. Krawczyk and P. Eronen, "HMAC-based extract- and-expand key derivation function (HKDF)," Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. RFC 5869, May 2010.

[39] F. Günther, B. Hale, T. Jager, and S. Lauer, "0-RTT key exchange with full forward secrecy," in *Proc. EUROCRYPT*. Cham, Switzerland: Springer, 2017, pp. 519–548.

[40] J. K. Liu, C.-K. Chu, S. S. M. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 178–189, Jan. 2014.

[41] K. Emura and T. Hayashi, "Road-to-Vehicle communications with time-dependent anonymity: A lightweight construction and its experimental results," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1582–1597, Feb. 2018.

[42] M. Fischlin and F. Gunther, "Replay attacks on zero round-trip time: The case of the TLS 1.3 handshake candidates," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 60–75.

[43] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, "A comprehensive symbolic analysis of TLS 1.3," in *Proc. ACM CCS*, 2017, pp. 1773–1788.

[44] J. Y. Hwang, S. Eom, K.-Y. Chang, P. J. Lee, and D. Nyang, "Anonymity-based authenticated key agreement with full binding property," in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, 2012, pp. 177–191.

[45] J. Camenisch, M. Drijvers, and A. Lehmann, "Anonymous attestation using the strong Diffie Hellman assumption revisited," in *Proc. Int. Conf. Trust Trustworthy Comput.* Cham, Switzerland: Springer, 2016, pp. 1–20.

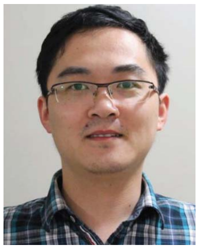
[46] J. Camenisch, M. Drijvers, and A. Lehmann, "Universally composable direct anonymous attestation," in *Public-Key Cryptography*. Berlin, Germany: Springer, 2016, pp. 234–264.

[47] J. Blömer, F. Eidens, and J. Juhnke, "Practical, anonymous, and publicly linkable universally-composable reputation systems," in *Proc. CT-RSA*. Cham, Switzerland: Springer, 2018, pp. 470–490.

[48] *Miracl Crypto SDK*. Accessed: Jan. 2021. [Online]. Available: https://libraries.docs.miracl.com/

Dongxiao Liu (Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2020. He is currently a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include security and privacy in intelligent transportation systems, blockchain, and mobile networks.

Huaqing Wu (Member, IEEE) received the B.E. and M.E. degrees from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014 and 2017, respectively, and the Ph.D. degree from the University of Waterloo, ON, Canada, in 2021. She is currently a Post-Doctoral Research Fellow with McMaster University, ON, Canada. Her current research interests include vehicular networks with emphasis on edge caching, wireless resource management, space-air-ground integrated networks, and application of artificial intelligence (AI) for wireless networks. She received the Prestigious Natural Sciences and Engineering Research Council of Canada (NSERC) Post-Doctoral Fellowship Award in 2021.



Jianbing Ni (Member, IEEE) received the B.E. and M.S. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2018. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering and the Ingenuity Labs Research Institute, Queen's University, Kingston, ON, Canada. His current research interests include applied cryptography and network security, with a focus on cloud computing, smart grid, mobile crowdsensing, and the Internet of Things.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990.

He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include network resource management, wireless network security, the Internet of Things, 5G and beyond, and vehicular *ad hoc* and sensor networks. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, a Chinese Academy of Engineering Foreign Member, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He received the Canadian Award for Telecommunications Research from the Canadian Society of Information Theory (CSIT) in 2021; the R.A. Fessenden Award from IEEE, Canada, in 2019; the Award of Merit from the Federation of Chinese Canadian Professionals (Ontario) in 2019; the James Evans Avant Garde Award from the IEEE Vehicular Technology Society in 2018; the Joseph LoCicero Award in 2015 and Education Award in 2017 from the IEEE Communications Society; and the Technical Recognition Award from Wireless Communications Technical Committee (2019) and AHSN Technical Committee (2013). He has also received the Excellent Graduate Supervision Award from the University of Waterloo in 2006 and the Premier's Research Excellence Award (PREA) from the Province of Ontario, Canada, in 2003. He served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom' 16, IEEE Infocom'14, IEEE VTC'10 Fall, and IEEE Globecom'07. He served as the Chair for the IEEE Communications Society Technical Committee on Wireless Communications. He is the President of the IEEE Communications Society. He was the Vice President for Technical and Educational Activities, the Vice President for Publications, a Member-at-Large on the Board of Governors, the Chair of the Distinguished Lecturer Selection Committee, and a member of IEEE Fellow Selection Committee of the ComSoc. He served as the Editor-in-Chief for the IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, and *IET Communications*.